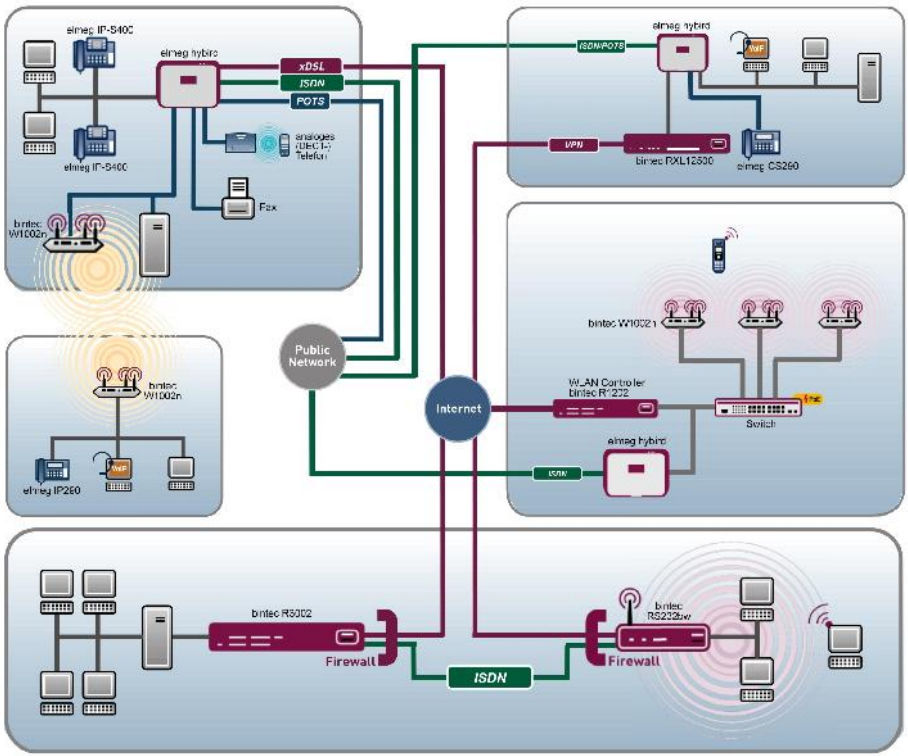


Benutzerhandbuch
elmeg hybird 120 / hybird 130

Rechtlicher Hinweis

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

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

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

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

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

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

Copyright

Richtlinien und Normen

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

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

Inhaltsverzeichnis

Kapitel 1 Einleitung

Die **hybird 120** und **hybird 130** sind komfortable Kommunikationssysteme, welche Ihr Sprachnetz mit dem Datennetz verbinden.

Die Geräte sind geeignet für die Anschaltung an einen ISDN-Amtsanschluss (vorkonfiguriert ist ein ISDN-Mehrgeräteanschluss). Für Telefonie über das Internet kann die **hybird 120** / **hybird 130** auch an einem analogen oder IP-basierten Anschluss angeschlossen bzw. können optional weitere SIP-Provider eingetragen werden.

In der Werkseinstellung können bis zu 10 Endgeräte angeschlossen werden, über eine Lizenz kann die Anzahl auf 20 (**hybird 120**) bzw. 30 (**hybird 130**) erhöht werden.

SIP-Telefone und PC-basierte SIP-Telefone sind als SIP-Endgeräte möglich. Die SIP-Endgeräte müssen über eine eigenständige Stromversorgung verfügen. Vier Geräte können direkt angeschlossen werden und werden automatisch mit den vorkonfigurierten Internrufnummern *30*, *31*, *32* und *33* belegt.

Hinweis

Zum Anschluss weiterer SIP-Endgeräte können nicht genutzte Analog- oder ISDN-Teilnehmer aus der Standardkonfiguration gelöscht werden. Durch Verwendung von Terminal-Lizenzen kann die Anzahl der Endgeräte auf 20 (**hybird 120**) bzw. 30 (**hybird 130**) erweitert werden. Die maximale Anzahl gleichzeitiger SIP-Gespräche kann über eine Lizenze von zwei auf sieben (**hybird 120**) bzw. zwölf (**hybird 130**) erhöht werden.

Neben den SIP-Endgeräten können auch konventionelle ISDN- bzw. Analogapparate und Fax-Geräte genutzt werden, mit denen Sie optional ebenfalls über einen VoIP-Provider telefonieren können.

Das Gerät verfügt über analoge Nebenstellen (über zwei RJ12-Buchsen und zwei bzw. drei interne Anschlussklemmen) und ISDN-(BRI)-Anschlüsse (RJ45), die sowohl für den internen Anschluss von ISDN-Endgeräten als auch für einen ISDN-Amtsanschluss, zusätzlich zum VoIP-Anschluss, genutzt werden können. Im Auslieferzustand ist ein ISDN (BRI) intern und ein ISDN (BRI) extern (also für die Verbindung mit dem ISDN-Anschluss des Providers) voreingestellt.

Hinweis

Bei einem IP-basierten Anschluss ist kein weiterer analoger oder ISDN-Amtsanschluss vorhanden.

Drei analoge Telefone mit den Internrufnummern *10*, *11* und *12* und ein analoges Fax bzw. Kombigerät mit der Internrufnummer *13* sind vorkonfiguriert und können direkt angeschlossen werden. Die Anschlüsse für die analogen Endgeräte sind fest für das MFV-Wahlverfahren eingerichtet. Daher müssen die analogen Endgeräte nach dem MFV-Wahlverfahren wählen und eine Flash-Taste besitzen. Endgeräte, die nach dem IWV-Wahlverfahren wählen, können zwar angerufen werden, aber keine Funktionen oder Kennziffern nutzen.

Einer der integrierten ISDN-Anschlüsse ist als **ISDN intern** vorkonfiguriert. Damit steht ein interner ISDN-Bus als Mehrgeräteanschluss für den Betrieb von ISDN- und Systemtelefonen zur Verfügung. Zwei ISDN-Endgeräte mit den Internrufnummern *20* und *21* sind vorkonfiguriert und können direkt angeschlossen werden. Darüber hinaus kann er für den Anschluss von Up0-Telefonen umkonfiguriert werden (siehe *Konfiguration der ISDN-Anschlüsse* auf Seite 32).

hybird 130 stellt zusätzlich zwei fest als Up0-Anschlüsse konfigurierte Schnittstellen bereit. Der Anschluss erfolgt über den Klemmblock unter der Oberschale des Geräts.

Hinweis

Beachten Sie, dass einige der in dieser Bedienungsanleitung beschriebenen Leistungsmerkmale beim Netzbetreiber beauftragt werden müssen.

Einen Internetzugang bauen Sie über das integrierte ADSL-Modem (ADSL1/ADSL2/ADSL2+) auf. Das Modem unterstützt den überwiegend in Deutschland eingesetzten ADSL-Standard Annex B (ADSL over ISDN) nach ITU G992.1 und ist kompatibel zum U-R2 Anschluss der Deutschen Telekom. Zusätzlich unterstützt das Modem auch den ADSL-Standard Annex J für den Anschluss an IP-basierte Anschlüsse. Darüber hinaus existiert eine gesonderte Produktvariante zur Unterstützung des Annex-A-Standards (die Varianten unterscheiden sich ausschließlich in der Art der ADSL-Unterstützung und sind am Typenschild auf der Geräterückseite zu erkennen). So ist Ihr Gerät in der Lage, Ihre verschiedenen Unternehmensnetze miteinander zu verbinden. Weiterer Vorteil: Ihre Mitarbeiter können auch außerhalb des Unternehmens sicher und zuverlässig auf das System zugreifen. Hierfür stehen Ihnen grundlegende Funktionen eines IP-Access-Routers zur Verfügung, wie z. B. NAT, SIF, VPN und IPSec.

Das Gerät verfügt über vier Gigabit-Ethernet-Ports, an die die SIP-Telefone und Computer im lokalen Netzwerk angeschlossen werden.

Für den Einsatz einer SD-Karte ist ein Slot vorgesehen. Damit werden Voice-Anwendungen (z. B. Wartemusik, automatische Ansagen) und Voice-Mail unterstützt. Außerdem können Systeminformationen (z. B. Konfigurationsdateien) auf die SD-Karte gesichert werden.

Hinweis

Verwenden Sie von der bintec elmeg GmbH freigegebene Karten (siehe *SD-Karte* auf Seite 41)!

Sicherheitshinweise

Was Sie im Umgang mit dem Gerät beachten müssen, erfahren Sie im Kapitel *Sicherheitshinweise* auf Seite 3.

Installation

Wie Sie das Gerät anschließen, erfahren Sie im Kapitel *Inbetriebnahme* auf Seite 10.

Konfiguration

Im Kapitel *Grundkonfiguration* auf Seite 49 zeigen wir Ihnen, wie Sie von einem PC aus auf die Konfigurationsoberfläche zugreifen, um die Grundkonfiguration und weiterführende Einstellungen vorzunehmen.

1.1 Sicherheitshinweise

Achtung

Wichtige Sicherheitshinweise zur Handhabung des Geräts!

Beachten Sie bitte zu Ihrer Sicherheit und zum Schutz des Geräts folgende Sicherheitshinweise:

- Vorsicht: Alle Bereiche, die sich nur mit Werkzeug öffnen lassen, sind Gefahrenbereiche. Durch unbefugtes Öffnen können Gefahren für den Benutzer entstehen.
- Zur Vermeidung eines Elektroschocks ist Vorsicht beim Anschließen von Telekommunikationsnetzen (TNV-Stromkreisen) geboten. LAN-Ports verwenden ebenfalls RJ-Steckverbinder.
- Um einen störungsfreien Betrieb zu gewährleisten, muss die **hybird 120** / **hybird 130** aufrecht an einer Wand montiert sein.
- Die Belüftungsöffnungen müssen frei bleiben. Halten Sie die Abstände entsprechend der Bohrschablone ein. Decken Sie das Gerät nicht mit Vorhängen, Tüchern usw. ab.
- Das Gerät darf keiner direkten Sonneneinstrahlung oder anderen Wärmequellen ausgesetzt sein.
- Das Gerät und die internen Anschlüsse dürfen nur innerhalb von Gebäuden montiert und

verlegt werden! Verlegen Sie die Leitungen bitte so, dass niemand darauf treten oder stolpern kann.

- Das Gerät darf nur mit dem mitgelieferten zugelassenen Steckernetzgerät betrieben werden.
- Beachten Sie, dass nur CE-zertifizierte Endgeräte an das Gerät angeschlossen werden.
- Für die Dauer eines Stromausfalls ist das Gerät über den externen ISDN-Anschluss oder einen IP-basierten Anschluss nicht erreichbar. Sie können aber durch Umstecken eines ISDN-Telefons weiter erreichbar bleiben (siehe dazu *Notbetrieb* auf Seite 13).
- Es dürfen keine Flüssigkeiten in das Geräteinnere oder das Steckernetzgerät gelangen können.
- Aktivieren und ändern Sie das System-Passwort des Konfigurationszugangs, wenn Sie verhindern wollen, dass andere Personen außer Ihnen Änderungen und Einstellungen vornehmen können.
- Bevor Sie das Gerät zu einer eventuellen Reparatur abgeben oder verkaufen, sollten Sie alle Daten speichern und die Telefonanlage anschließend in den Auslieferungszustand zurückversetzen (siehe *Reset* auf Seite 36).

1.2 Reinigen

Wischen Sie das Gerät bei Bedarf mit einem etwas angefeuchteten Tuch oder mit einem Antistatiktuch ab. Vermeiden Sie trockene oder nasse Tücher! Vermeiden Sie den Einsatz von Lösungs-, Putz- und Scheuermitteln! Sie schaden damit dem Gerät.

1.3 Konformitätserklärung und CE-Zeichen

Dieses Gerät erfüllt die Anforderungen der R&TTE-Richtlinie 1999/5/EG: "Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität". Weitere Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter *www.bintec-elmeg.com* .

CE

Abb. 2: CE-Zeichen

1.4 Entsorgung

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.

1.5 Open Source Software in diesem Produkt

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

1.6 GEMA

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

1.7 Zum Handbuch

Dieses Handbuch beschreibt, wie Sie als Anlagenbetreuer/in das Gerät Ihren Anforderungen anpassen können.

Dieses Dokument ist gültig für **elmeg**-Geräte mit einer System-Software ab Software-Version 9.1.7.

Das Handbuch enthält folgende Kapitel:

Benutzerhandbuch - Referenz

Kapitel	Beschreibung
Kurzanleitung	Diese enthält Anweisungen, wie Sie Ihr Gerät aufstellen, anschließen und in wenigen Minuten in Betrieb nehmen. Außerdem wird Ihnen der Weg zu weiterführenden Einstellungen beschrieben.

Kapitel	Beschreibung
Montage	Dieses Kapitel enthält die Beschreibung sämtlicher Anschlussmöglichkeiten Ihres Geräts.
Service-Zugang	Dieses Kapitel sagt Ihnen, wie Sie für die Grundkonfiguration und für erweiterte Konfigurationen den **elmeg**-Kundenservice kontaktieren und Ihr Gerät für Wartungs- und Konfigurationsarbeiten durch den Service vorbereiten.
Grundkonfiguration	Diese enthält Anweisungen, wie Sie Grundfunktionen Ihres Geräts konfigurieren.
Bedienung über das Telefon	Diese Kapitel enthalten alle Informationen über die Wechselwirkung zwischen Telefonen und Telefonanlage.
Zugang und Konfiguration	Hier werden die verschiedenen Zugangs- und Konfigurationsmöglichkeiten erläutert.
Reset	In diesem Kapitel wird das Zurücksetzen des Geräts in einen definierten Ausgangszustand beschrieben.
Technische Daten	Dieser Abschnitt enthält eine Beschreibung aller technischen Eigenschaften Ihres Geräts.
Assistenten **Systemverwaltung** **Physikalische Schnittstellen** **VoIP** **Nummerierung** **Endgeräte** **Anrufkontrolle** **Anwendungen** **LAN** **Wireless LAN Controller**	In diesen Kapiteln werden alle Optionen der Konfigurationsoberfläche beschrieben. Die Kapitel sind entsprechend der Navigationsstruktur angeordnet. In den einzelnen Kapiteln finden Sie auch generelle Erläuterungen zur jeweiligen Funktion.

Kapitel	Beschreibung
Netzwerk **Multicast** **WAN** **VPN** **Firewall** **Lokale Dienste** **Wartung** **Externe Berichterstellung** **Monitoring**	
Glossar	Das Glossar enthält eine Referenz der wichtigsten technischen Begriffe der Netzwerktechnik.
Index	Im Index sind wichtige Begriffe für die Bedienung des Geräts 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 Gefahren hin, die bei Nichtbeachten Sachschäden zur Folge haben können).
	Kennzeichnet Warnhinweise in der Gefahrenstufe **Warnung** (weist auf mögliche Gefahren hin, die bei Nichtbeachten Körperverletzung oder Tod zur Folge haben können).

Die folgenden 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 in der Konfigurationsoberfläche und in der Windows-Oberfläche.

`nicht-proportional (Courier),`
 	
`z. B. ping 192.168.1.253`
	Kennzeichnet Kommandos (z. B. in der Windows Eingabeaufforderung), die Sie wie dargestellt eingeben müssen.

fett, z. B. **Windows-Startmenü**	Kennzeichnet Tasten, Tastenkombinationen und Windows-Begriffe.
fett, z. B. **Anschlussart**	Kennzeichnet Felder in der Konfigurationsoberfläche.
kursiv, z. B. *`keiner`*	Kennzeichnet Werte, die Sie in der Konfigurationsoberfläche eintragen bzw. die eingestellt werden können.
Online: rot und kursiv, z. B. *http://www.bintec-elmeg.com*	Kennzeichnet Hyperlinks.

Kapitel 2 Kurzanleitung

2.1 Einleitung

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

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

Die mitgelieferte CD enthält das Handbuch Ihres Geräts sowie weitere Tools und Dokumentationen, die Sie für Konfiguration und Management verwenden können.

2.2 Inbetriebnahme

Die **hybird 120** / **hybird 130** ermöglicht Ihnen verschiedene Anschlussvarianten: Zum einen den Anschluss an einen ISDN-Amtsanschluss in Verbindung mit einem ADSL-Anschluss. Sie können dann sowohl IP-Telefonie als auch klassisches ISDN für Telefonverbindungen nutzen. Alternativ zum ISDN-Anschluss steht für diese Variante auch ein externer analoger Anschluss (FXO) bereit. Zum anderen können Sie die **hybird 120** / **hybird 130** an einem reinen IP-Anschluss betreiben. Sie telefonieren dann ausschließlich über VoIP, sind aber beim Anschluss Ihrer Endgeräte gegenüber der ersten Variante nicht eingeschränkt: Sie können SIP-, analoge und ISDN-Endgeräte und PCs anschließen.

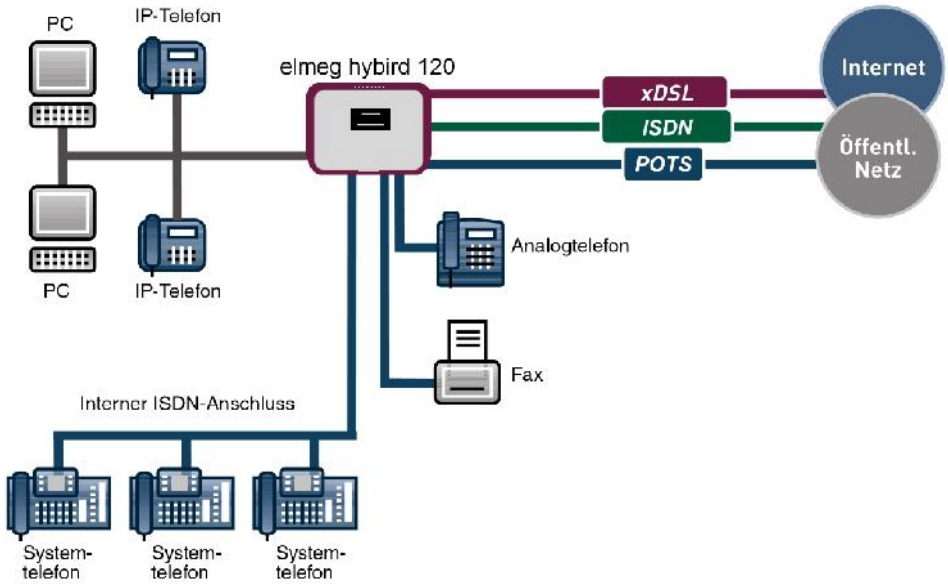


Abb. 3: Basisszenario **hybird 120** / **hybird 130**

Achtung

Vor Installation und Inbetriebnahme Ihres Geräts lesen Sie bitte aufmerksam die *Sicherheitshinweise* auf Seite 3.

2.2.1 Anschlüsse

Abb. 4: Anschlüsse

1	Buchse für das Steckernetzgerät
2	Externe Schnittstelle für analoge Endgeräte FXO 1
3	Interne Schnittstelle für analoge Endgeräte FXS 1 (Interne Rufnummer 10, Auslieferzustand)
4	Interne Schnittstelle für analoge Endgeräte FXS 2 (Interne Rufnummer 11, Auslieferzustand)
5	Schnittstelle für ISDN-BRI-Anschlüsse (ISDN S/U intern, Auslieferzustand, umsteckbar) (Interne Rufnummern 20 und 21, Auslieferzustand)
6	Schnittstelle für ISDN-BRI-Anschlüsse (ISDN S/U extern, Auslieferzustand, umsteckbar)
7	USB-Anschluss Typ B
8	10/100/1000 Base-T Ethernet-Schnittstelle (LAN 1)
9	10/100/1000 Base-T Ethernet-Schnittstelle (LAN 2)
10	10/100/1000 Base-T Ethernet-Schnittstelle (LAN 3)
11	10/100/1000 Base-T Ethernet-Schnittstelle (LAN 4)
12	ADSL2+-Schnittstelle

2.2.2 Anschlüsse (seitlich)

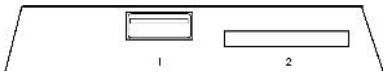


Abb. 5: Seitliche Anschlüsse

1	USB-Typ-A-Buchse (aktuell nicht in Betrieb)
2	SD-Card-Slot

2.2.3 Aufstellen und Anschließen

Achtung

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

Bei falscher Verkabelung der Telefon- und LAN-Schnittstelle kann es zum Defekt Ihres Geräts kommen! Verbinden Sie immer nur die LAN-Schnittstellen des Geräts mit der LAN-Schnittstelle des PCs und die externe ISDN-Schnittstelle des Geräts nur mit dem externen Telefonanschluss (also dem Anschluss des Providers).

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

(1) Montage: Im Betrieb muss das Gerät sicher an einer Wand montiert sein (lesen Sie bitte aufmerksam das Kapitel *Montage* auf Seite 21).

(2) LAN: Zur Konfiguration Ihres Geräts über Ethernet, verbinden Sie den Ethernet-Anschluss des PC mit einer der 10/100/1000 Base-T Ethernet-Schnittstellen (9-12) des Geräts über ein geeignetes Netzwerkkabel.

(3) Netzanschluss: Schließen Sie den Netzanschluss des Geräts (1) mit dem mitgelieferten Steckernetzgerät an eine 230 V~ Steckdose an.

Optionale Anschlüsse

- DSL: Wenn Sie das interne ADSL-Modem verwenden möchten, schliessen Sie die DSL-Schnittstelle des Geräts (13) mit dem mitgelieferten gelben Kabel an die DSL-Buchse des Splitters oder den entsprechenden Wandanschluss an.
- SIP-Telefone: Schliessen Sie Ihre SIP-Telefone an die 10/100/1000 Base-T Ethernet-Schnittstellen (9-12) an.
- Analoge Telefone/Fax: Verbinden Sie Ihre analogen Endgeräte mit den internen Schnittstellen für analoge Endgeräte (4-5). Verwenden Sie dazu das dem Endgerät beigefügte Kabel. Weitere analoge Endgeräte können im Gerät über Klemmen angeschlossen werden.
- ISDN-Telefone: Schließen Sie die ISDN-Telefone an den internen ISDN-Anschluss (6) an.
- Externer ISDN-Anschluss: Wenn Sie einen externen ISDN-Anschluss beauftragt haben, schließen Sie die Schnittstelle für externe Telefonleitungen des Geräts (7) mit dem mitgelieferten Kabel an Ihre Telefonanschlussdose an.
- Analoger Telefonanschluss: Wenn Sie über einen analogen Telefonanschluss verfügen, schließen Sie die FXO-Schnittstelle (2) über ein geeignetes Kabel an die Telefonanschlussdose an. Beachten Sie, dass die FXO-Buchse eine RJ12-Buchse ist.

Ihr Gerät ist nun einsatzbereit und für die weiterführende Konfiguration mit der Konfigurationsoberfläche vorbereitet.

2.2.4 Notbetrieb

Das Gerät verfügt über keinen eingerichteten Notbetrieb. Wenn Sie einen ISDN-Anschluss beauftragt haben, können Sie bei einem 230 V~ Netzausfall wie folgt vorgehen: Ziehen Sie das Anschlusskabel aus dem Netzabschlussgerät (ISDN-NTBA). Anschließend können Sie ein notspeisefähiges ISDN-Endgerät direkt in das Netzabschlussgerät stecken und wieder telefonieren. Nach Stromwiederkehr vergessen Sie nicht, diesen Vorgang rückgängig zu machen.

Hinweis

Beachten Sie die Einstellungen des notspeisefähigen Telefons: Es muss im Falle der Notspeisung für den aktuellen ISDN-Anschluss (Mehrgeräteanschluss oder Anlagenanschluss) eingestellt werden können.

Bei einem IP-basierten Anschluss ist ein Notbetrieb nicht möglich.

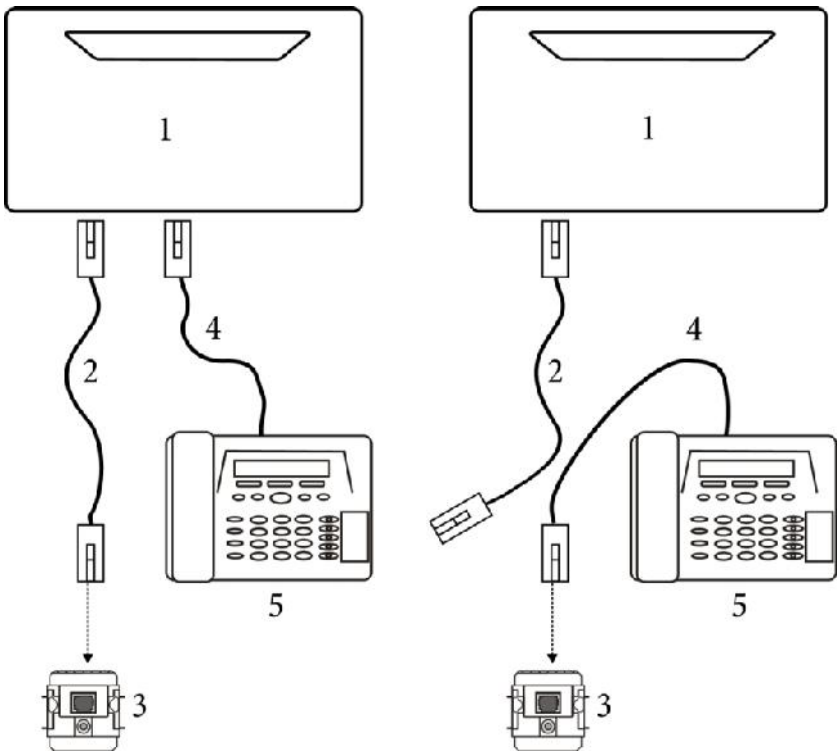


Abb. 6: Notbetrieb ISDN

1	**hybird 120** / **hybird 130**
2	Anschlusskabel RJ45-Stecker
3	ISDN-Anschluss des Netzabschlussgeräts
4	Anschlusskabel für das ISDN-Telefon mit RJ45-Stecker
5	Notspeisefähiges ISDN-Telefon

2.3 Voreinstellungen

Wenn Sie Ihr Gerät das erste Mal in Betrieb nehmen, sind einige Einstellungen bereits vorkonfiguriert, damit Sie in wenigen Schritten nach dem Aufstellen und Anschließen Ihr Gerät in Betrieb nehmen können.

Hinweis

Prüfen Sie anhand der Bedienungsanleitung Ihrer vorhandenen Endgeräte, wie und mit welchen Einstellungen Leistungsmerkmale genutzt werden können.

Die Voreinstellungen können Sie entsprechend Ihren persönlichen Erfordernissen und Anschlussbedingungen verändern.

Telefonie-Voreinstellungen

Analoge Anschlüsse	Als Telefon eingerichtet. Auf *Tonwahl (MFV)* nicht veränderbar eingestellt.
Anklopfen	Ist bei analogen Telefonen eingerichtet (für FXS 4 aber für den Anschluss eines Fax oder Kombigerätes deaktiveirt).
Anklopfende Anrufe	Sind am ISDN-Anschluss beide B-Kanäle belegt, werden anklopfende Anrufe abgewiesen.
Anrufvarianten manuell umschalten	Erlaubt
Wechselsprechen Empfangen	Erlaubt
Durchsage	Erlaubt
Net Direct (Keypad)	Erlaubt
TFE-Berechtigung	Erlaubt
TAPI	Erlaubt
Verbindungsdaten speichern	Eingerichtet
Amtsholung	Amtsholung über die *0* ist eingerichtet.
Internationaler Präfix	*00*
Länderkennzahl	*49*
Nationaler Präfix	*0*
Ortsnetzkennzahl	Nicht eingerichtet
Währung für Abrechnung	*EUR*
Berechtigung für die Endgeräte	Uneingeschränkt wahlberechtigt

Direktruf	Nicht eingerichtet
Eigene Telefonnummer	Wird zum Anrufenden übermittelt
Externe Anrufe	Werden an allen vorkonfigurierten Internrufnummern signalisiert (*Team Alle*).
Abgehende Telefonate	Für alle Internrufnummern über den voreingestellten externen ISDN-Anschluss (*ISDN Extern*).
Manuelle Bündelbelegung	Für alle Internrufnummern für den voreingestellten externen ISDN-Anschluss (*ISDN Extern*) eingerichtet.
Heranholen des Rufes	Eingerichtet
Interne Telefonnummern	Für den **ISDN (BRI) intern** am internen ISDN-Bus sind die internen Telefonnummern *20* und *21*, für die analogen Anschlüsse **FXS1** bis **FXS4** die internen Telefonnummern *10* bis *13*, für Systemtelefone die Telefonnummern *30* bis *33* vorgesehen.
Vorkonfigurierte Teams	Internrufnummer *40*: Team global (zugewiesene Internrufnummern: alle) Internrufnummer *41*: Team analog (zugewiesene Internrufnummern: *10*, *11*, *12*, *13*) Internrufnummer *42*: Team ISDN (zugewiesene Internrufnummern: *20*, *21*) Internrufnummer *43*: Team SysTel (zugewiesene Internrufnummern: *30*, *31*, *32*, *33*)
Abwurf bei Falschwahl	Auf Internrufnummer *40* (Team global)
Anrufweiterschaltung im Team	Erlaubt
Voice Mail System	Für alle Internrufnummern eingerichtet.

	Ohne PIN-Abfrage. (Nur wenn SD-Karte vorhanden).
Anzeige im Systemtelefonbuch	Für alle Internrufnummern eingerichtet
Besetztlampenfeld	Für alle Internrufnummern eingerichtet
Schaltzeiten (Kalender)	Nicht eingerichtet
Keypad-Funktion	Nicht eingerichtet
PIN 1	Nicht eingerichtet
PIN 2	*000000*
Telefonnummer des anrufenden Teilnehmers (CLIP)	Wird angezeigt
Telefonnummerübermittlung	Eingerichtet
ISDN-Mehrgeräteanschluss	Eingerichtet für den Anschluss ISDN 2
Mehrgeräteanschlussrufnummer	Keine eingetragen
Standard-MSN	*20 (#20)*
Uhrzeit am internen ISDN (BRI)	Die Uhrzeit ist nach Neustart immer auf *0:00* Uhr eingestellt.  **Hinweis** Überprüfen Sie nach einem Neustart immer die korrekte Systemzeit! Sofern Sie einen ISDN-Amtsanschluss beauftragt haben, wird die Zeit nach der ersten ausgehenden Verbindung aus dem ISDN bezogen. Wenn Sie über einen konfigurierten Internetzugang mit dem Internet verbunden sind,

	kann die Zeit von einem Zeitserver übernommen werden.
Gerät als interner Zeitserver	Eingerichtet
Wahlregeln	Eingerichtet für alle Internrufnummern, aber keine Rufnummern eingerichtet
Wahlkontrolle	Eingerichtet für alle Internrufnummern, aber keine Rufnummern eingerichtet
Vorrangrufnummern	Es sind keine Vorrangrufnummern konfiguriert. Übliche Nummern sind: Notruf *110* Notruf *112* Rettungswagen *19222*
Wartemusik 1	*MOH Intern 1* eingerichtet.
Zeit für Anrufweiterschaltung	Nach Zeit auf *15* Sekunden eingestellt.
Voreingestellte Feiertage	Es sind keine Feiertage konfiguriert. Übliche Feiertage sind: 01.01. Neujahr 06.01. Heilige Drei Könige 01.05. Tag der Arbeit 15.08. Mariä Himmelfahrt 03.10. Tag der deutschen Einheit 31.10. Reformationstag 01.11. Allerheiligen 25.12. 1. Weihnachtsfeiertag 26.11. 2. Weihnachtsfeiertag
IP-Adressvergabe an VoIP-Endgeräte und PCs im LAN	Über DHCP-Server mit IP-Adressbereich *192.168.0.10 - 192.168.0.30*

	Zeitserver: *192.168.0.250* DNS-Server: *192.168.0.250* Provisioning Server: *sdlp://192.168.0.250:18443*

Konfigurationsoberfläche

Die Konfigurationsoberfläche Ihres Geräts ist im Auslieferungszustand über einen der LAN-Anschlüsse unter folgender Adresse erreichbar:

- **IP-Adresse**: *192.168.0.250*
- **Netzmaske**: *255.255.255.0*

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration über die Konfigurationsoberfläche:

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

Hinweis

Nach dem ersten Login in das Gerät werden Sie aufgefordert, ein sicheres Passwort einzugeben. Beachten Sie hierzu die angezeigten Vorgaben für ein sicheres Passwort! Drücken Sie am Ende des Konfigurationsvorgangs die Schaltfläche **Konfiguration speichern**! Ansonsten geht auch das neue sichere Passwort nach einem Neustart verloren.

Software-Update

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Wie Sie den Softwarestand Ihres Geräts prüfen und ggf. eine Aktualisierung durchführen, wird im **Handbuch**-Kapitel „**Wartung**“ beschrieben (siehe auch Handbuch auf der mitgelieferten CD).

2.4 Support-Information

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

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

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

Kapitel 3 Montage

Warnung

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

Achtung

Um einen störungsfreien Betrieb zu gewährleisten, muss die **hybird 120** / **hybird 130** aufrecht an einer Wand montiert sein. Das Gerät darf keiner direkten Sonneneinstrahlung oder anderen Wärmequellen ausgesetzt sein. Beachten Sie auch die einzuhaltenden Abstände (siehe *Wandmontage* auf Seite 32).

Hinweis

Wenn Sie ein Endgerät mit einem TAE-Stecker anschließen wollen, können Sie einen TAE-auf-RJ12-Adapter verwenden, den Stecker am Kabel des Endgeräts entfernen und das Gerät an einem Klemmblock anschließen oder den Stecker des Endgerätekabels wechseln.

3.1 Anschlussvarianten

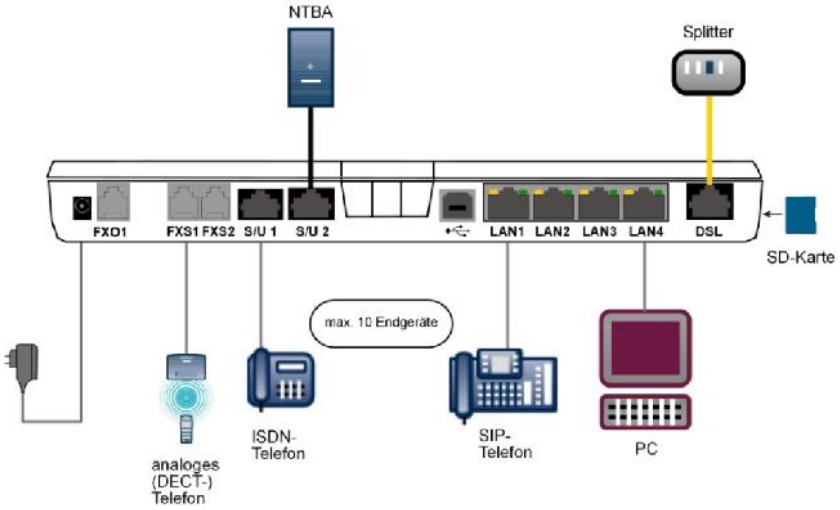


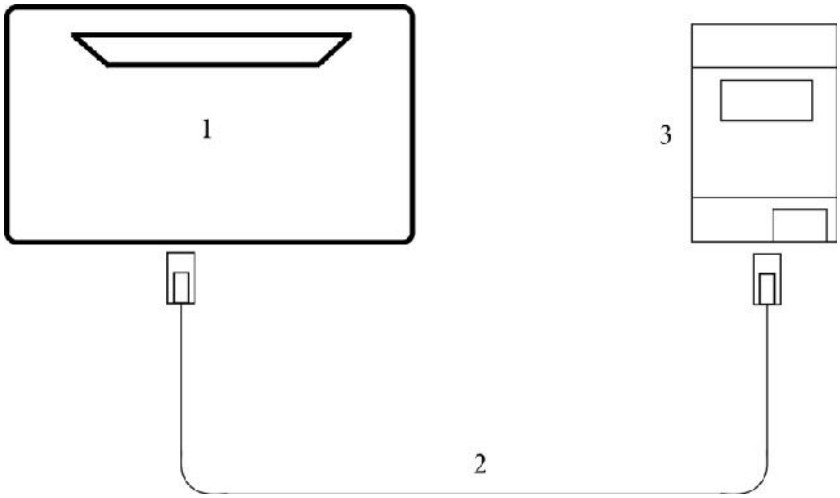
Abb. 7: Anschlüsse

3.1.1 Anschluss an das ISDN-Netz

Der zweite ISDN-Anschluss (ISDN 2 oder Klemmblock unten rechts) ist im Auslieferungszustand als externer S0-Anschluss (S0 TE) konfiguriert (zur Konfiguration der ISDN-Anschlüsse siehe *Konfiguration der ISDN-Anschlüsse* auf Seite 32). Abschlusswiderstände können Sie über Schalter bei der Konfiguration der ISDN-Anschlüsse ein- oder ausschalten. Im Auslieferungszustand sind alle Widerstände eingeschaltet.

3.1.1.1 Anschluss direkt am NTBA

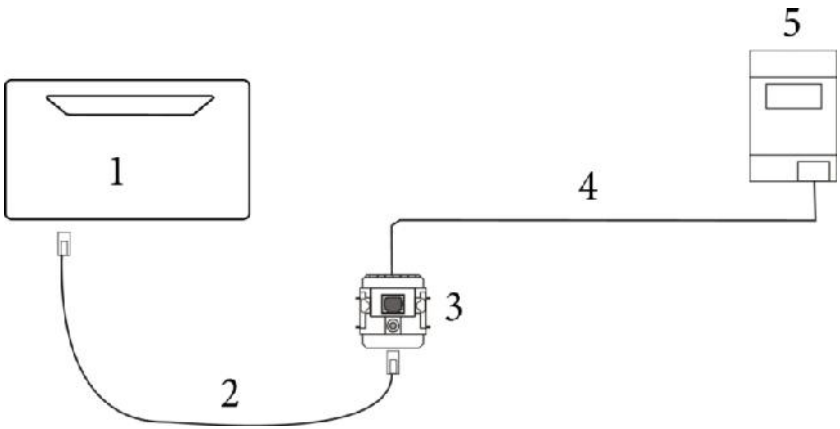
Beispiel 1: Das Gerät wird direkt an den ISDN-NTBA angeschlossen.



1	**hybird 120** / **hybird 130**
2	RJ45-Anschlusskabel für den ISDN-Anschluss
3	ISDN-NTBA mit eingeschalteten 2x 100 Ohm Abschlusswiderständen

3.1.1.2 Anschluss an einer Anschlussdose

Beispiel 2: Gerät und ISDN-NTBA sind weiter als ca. 2,5 Meter voneinander entfernt.

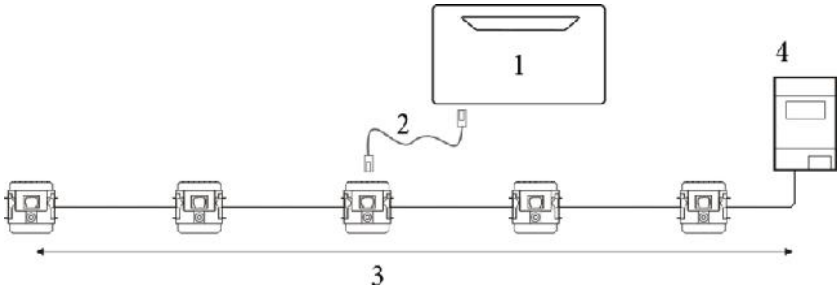


1	**hybird 120** / **hybird 130**
2	RJ45-Anschlusskabel für den ISDN-Anschluss
3	RJ45 Anschlussbuchse mit 2x 100 Ohm Abschlusswiderständen
4	Festes Verbindungskabel

5	ISDN-NTBA mit eingeschalteten 2x 100 Ohm Abschlusswiderständen

3.1.1.3 Anschluss an einem bestehenden ISDN-Bus

Beispiel 3: Das Gerät wird an einem bestehenden ISDN-Bus betrieben.



1	**hybird 120** / **hybird 130**
2	RJ45-Anschlusskabel für den ISDN-Anschluss
3	Bestehender ISDN-Bus beidseitig abgeschlossen
4	ISDN-NTBA mit eingeschalteten 2x 100 Ohm Abschlusswiderständen

Hinweis

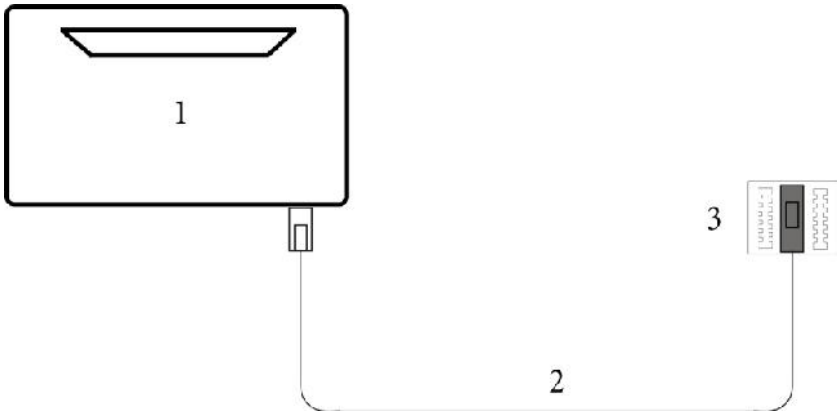
Der ISDN-Bus muss an beiden Enden mit 2x 100 Ohm Abschlusswiderständen abgeschlossen sein. In diesem Szenario müssen die integrierten Abschlusswiderstände der **hybird 120** / **hybird 130** geöffnet werden.

3.1.2 IP-basierter Anschluss

Bei einem rein IP-basierten Anschluss verbinden Sie die **hybird 120** / **hybird 130** wie in der Inbetriebnahme beschrieben zunächst mit dem Übergabepunkt des Netzbetreibers. Ein Splitter wird in diesem Fall in der Regel nicht verwendet, der Anschluss erfolgt direkt an der ersten Anschlussdose. Alternativ können Sie Ihr Gerät an ein bestehendes Modem (z. B. ein VDSL-Modem) anschließen.

3.1.2.1 ADSL-Anschluss

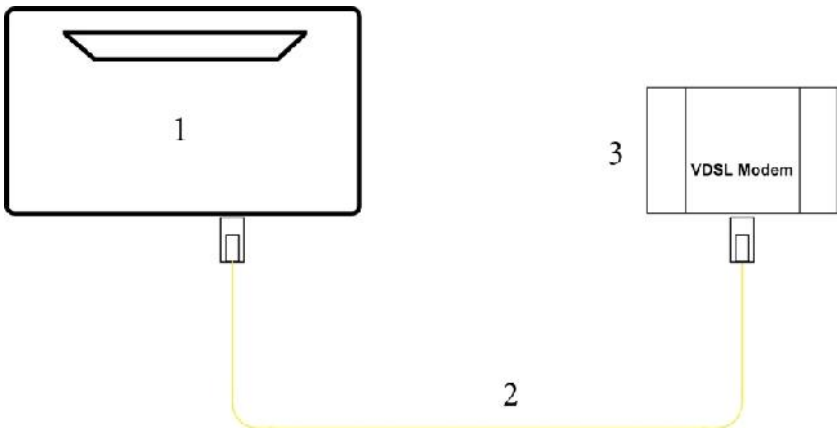
Beispiel 1: Die **hybird 120** / **hybird 130** wird direkt am ADSL-Anschluss betrieben: Hierzu müssen Sie Ihr Gerät lediglich mit der Wanddose des ADSL-Anschlusses verbinden und den Einrichtungsschritten folgen, die Sie dem Inbetriebnahmeposter oder dem Kapitel *Kurzanleitung* auf Seite 9 entnehmen können.



1	**hybird 120** / **hybird 130**
2	Anschlusskabel für die Verbindung zur ADSL-Buchse
3	ADSL-Anschlussdose

3.1.2.2 VDSL-Anschluss

Beispiel 2: Die **hybird 120** / **hybird 130** wird an einem vorhandenen VDSL-Modem betrieben: Auch bei dieser Anschlussvariante ist die Montage denkbar einfach. Schließen Sie Ihr Gerät mit dem mitgelieferten gelben Netzwerkkabel an das vorhandene VDSL-Modem an und befolgen Sie die auf dem Inbetriebnahmeposter oder im Kapitel *Kurzanleitung* auf Seite 9 beschriebenen Schritte.



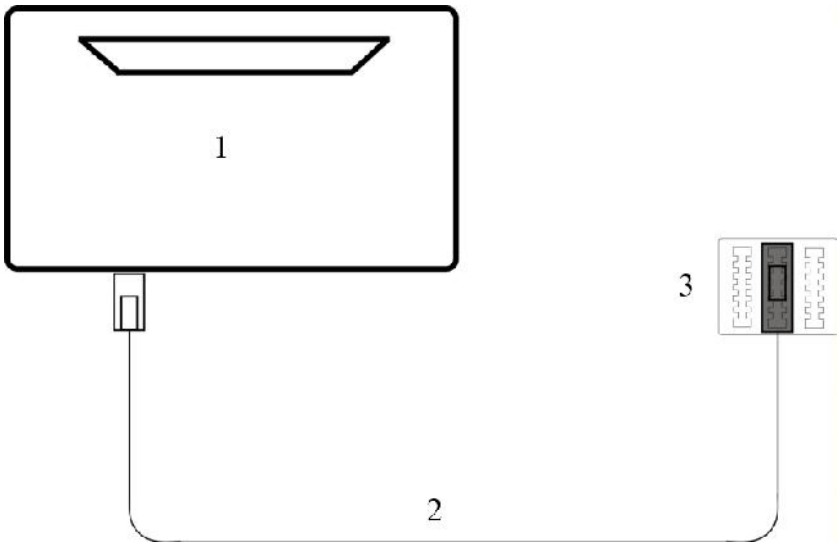
1	**hybird 120** / **hybird 130**
2	gelbes RJ45-Anschlusskabel für den Anschluss an das VDSL-Modem
3	VDSL-Modem

3.1.3 Anschluss an das analoge Telefonnetz

Zum Anschluss an das analoge Telefonnetz verbinden Sie die Anschlussdose Ihres Netzbetreibers mittels eines geeigneten Kabels mit der FXO-Schnittstelle Ihrer **hybird 120** oder **hybird 130**.

Hinweis

Beachten Sie, dass Sie ein Kabel benötigen, das die TAE-Anschlussdose mit der RJ12-Buchse Ihres Gerätes verbindet. Ein solches Kabel ist nicht im Lieferumfang enthalten.



1	**hybird 120** / **hybird 130**
2	Anschlusskabel für die Verbindung zur TAE-Dose (RJ12 auf TAE)
3	TAE-Anschlussdose

3.1.4 Anschluss von Endgeräten

3.1.4.1 Anschluss für analoge Endgeräte

An die analogen Anschlüsse sollten nur analoge Endgeräte mit Tonwahl (MFV-Wahlverfahren) angeschlossen werden. An die analogen Anschlüsse können analoge Telefone, Telefaxgeräte, Anrufbeantworter, Kombigeräte, Modems und Torstellen (Türfreisprecheinrichtung, TFE) angeschlossen werden.

Hinweis

Für den direkten Anschluss von zwei analogen Endgeräten sind zwei RJ12-Anschlussbuchsen (**FXS1** und **FXS2**) integriert. Diese Anschlüsse entsprechen den festen Anschlüssen an den Anschlussklemmen des oberen linken Klemmblocks.

Hinweis

Die festen Anschlüsse und die direkten Anschlüsse sind parallel verbunden. Sie können Endgeräte daher entweder am festen oder am direkten Anschluss betreiben.

Die R-Taste muss die Flash-Funktion (70 ms bis 310 ms) ausführen. Mit diesen Endgeräten sind die in der Bedienung und Konfiguration beschriebenen Funktionen ohne Einschränkungen zu nutzen. Die internen analogen Anschlüsse unterstützen die Clip- und die Clip-off-Hook-Funktion. Analoge Telefone mit dem Impulswahlverfahren (IWV) können nicht wählen. Ihr Gerät unterstützt bei den analogen Telefonen den Flash. Legen Sie daher den Hörer nie nur kurz auf oder betätigen Sie nie mit der Hand kurz den Gabelumschalter, sonst erkennt das Geräts einen Flash anstelle des Auflegens.

Kabelzuordnung an den Anschlussklemmen von TDO-Anschlussdosen

Die Leitungslänge vom Gerät bis zum Endgerät darf max. 1000 Meter betragen. Die Leitungslängen gelten für die Kabel J-Y (St) Y2x2x0,6.

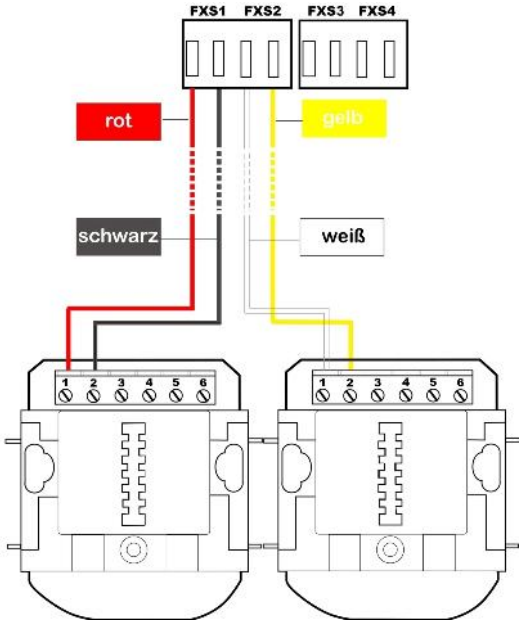


Abb. 8: Anschalten an einer TAE-Anschlussdose

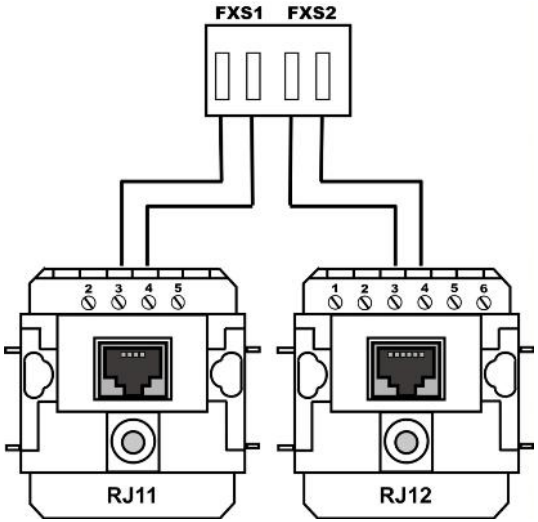


Abb. 9: Anschaltung an einer RJ11- oder RJ12-Dose

3.1.4.2 Interner ISDN-Anschluss

Der interne ISDN-Anschluss der **hybird 120** / **hybird 130** stellt an jedem internen ISDN-Anschluss 2,5 Watt Speiseleistung für den Anschluss von maximal zwei ungespeisten ISDN-Endgeräten zur Verfügung. Der interne ISDN-Anschluss ist im Auslieferungszustand als "Kurzer passiver Bus" ("S0-Bus") eingerichtet. Es ist die einfache Bus-Verkabelung eines ISDN-Systems mit einer Länge von bis zu 120 m.

Internen ISDN-Anschluss installieren

Ein Endgerät können Sie direkt in die Buchse **ISDN 1** (interner ISDN-Anschluss) stecken. Weitere ISDN-Endgeräte können Sie an einem fest installierten ISDN-Bus anschließen. An diesen Anschluss können Sie ein ISDN-Systemtelefon, ein ISDN-Telefon oder eine ISDN-Karte anschließen.

Der Anschluss weiterer ISDN-Endgeräte erfolgt über einen ISDN-Verteiler oder über eine feste Verkabelung an einem ISDN-Bus. Die Leitungslänge bis zu den ISDN-Anschlussdosen der Endgeräten kann bis zu 120 m, bei einem Drahtdurchmesser von 0,6 mm, betragen. Die Länge der ISDN-Anschlussleitungen von den ISDN-Anschlussdosen zu den ISDN-Endgeräten darf 10 Meter nicht überschreiten.

Die Leitungslängen gelten für die Kabel J-Y (St) Y2x2x0,6 (0,4). Mit anderen Kabeltypen sind auch größere Reichweiten möglich. Beachten Sie, dass die Ummantelung der Kabel nicht länger als nötig entfernt wird und die Adern bis zur Anschlussdose verdrillt oder verseilt bleiben.

Wichtig

In der letzten am ISDN-Bus installierten ISDN-Anschlussdose müssen die 100 Ohm Abschlusswiderstände angeschlossen werden.

3.1.5 Feste Anschlüsse

Hinweis

Beim Abnehmen des Deckels kann zunächst ein gewisser Kraftaufwand erforderlich sein. Halten Sie den Deckel an der Oberseite leicht angedrückt, während Sie mit Daumen und Zeigefinger die Lasche an der Unterseite lösen.

Für die festen Anschlüsse sind 4-polige Anschlussklemmen vorgesehen. Achten Sie darauf, dass die Adern bis an die Anschlussklemmen verdrillt bleiben. An jedem Anschluss können 2 Drähte gesteckt werden. Der Drahtdurchmesser kann 0,4 … 0,8 mm betragen.

Wenn Sie mit einem Schraubendreher auf die mit dem Pfeil gekennzeichnete Fläche der Anschlussklemme (Bild) drücken, können die Drähte mit leichtem Zug herausgezogen werden.

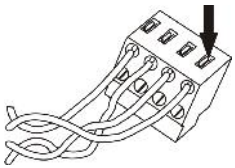


Abb. 10: Anschlussklemme

Für die Fixierung der Anschlusskabel sind Kabelfixierungen aus Kunststoff integriert. Sie sollten dennoch die Installationskabel vor dem Gerät z. B. durch Kabelschellen [D] gegen das Herausziehen sichern. Die Adern [B] der Anschlusskabel [A] sollten etwa 100 mm aus dem Kabelmantel herausstehen. Die Länge des Kabelmantels [C] ab den Kabelschellen sollte etwa 80 mm betragen. Die Enden der Adern müssen auf ca. 6-7 mm abisoliert werden.

Anschlussklemme	**Bezeichnung**	**Telefonnummern**
Klemme 1	**FXS1** und **FXS2**	*10* und *11*
Klemme 2	**FXS3** und **FXS4**	*12* und *13*
Klemme 3 (nur **hybird 130**)	**FXS 5** und **FXS 6**	
Klemme 4	**Schaltkontakt**	
Klemme 5	**ISDN 1 (konfigurierbar)**	*20, 21*
Klemme 6	**ISDN 2 (konfigurierbar)**	*extern*
Klemme 7 (nur **hybird 130**)	**Up0**	

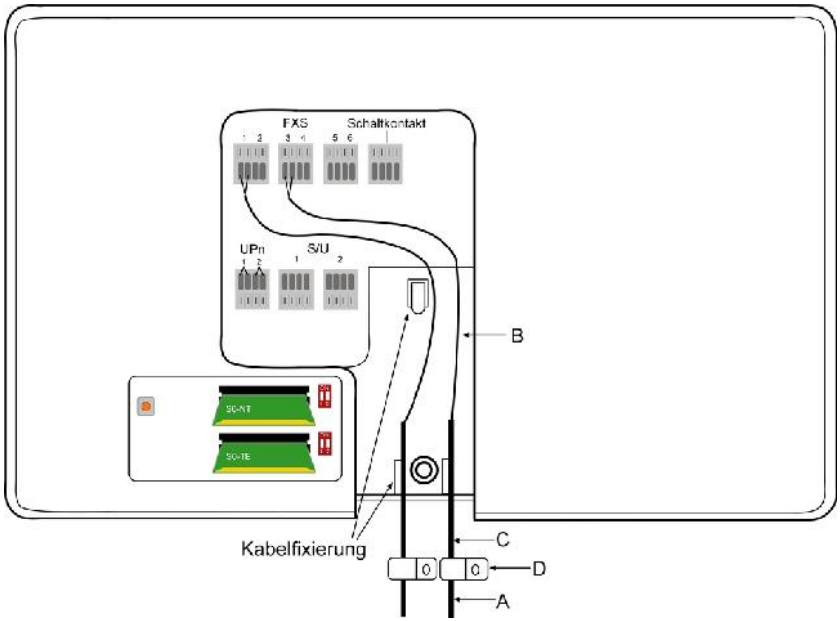


Abb. 11: Kabelfixierung

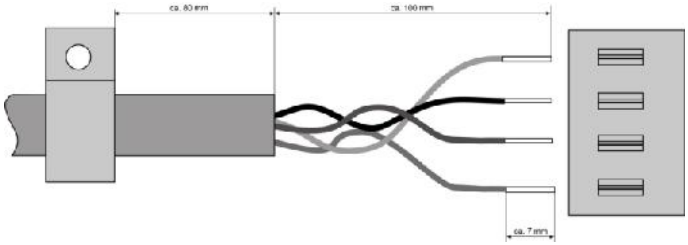


Abb. 12: Abisolieren

3.2 Konfiguration der ISDN-Anschlüsse

Die ISDN-Anschlüsse der **hybird 120** / **hybird 130** können variabel als S0 NT, S0 TE oder Up0 betrieben werden. Für die Umschaltung zwischen den einzelnen Betriebsarten finden Sie unter der abnehmbaren Oberschale und unter der darunter liegenden Klappe zwei Slots mit Mini-PCB:

Abb. 13: Mini-Module zur ISDN-Anschlusskonfiguration und Reset-Taster

Sie können die Betriebsart bestimmen, indem Sie für jeden Anschluss (ISDN 1 oben, ISDN 2 unten) das zugehörige Mini-Modul so stecken, dass bei der Aufsicht von oben die gewünschte Bezeichnung sichtbar ist (zur Orientierung: Die Anschlüsse des Gerätes befinden sich an der Unterseite).

Darüber hinaus finden Sie neben den Slots für die Umschaltung der Betriebsart zwei Schalterblöcke zum Ein- bzw. Ausschalten der Abschlusswiderstände. Im Auslieferungszustand sind die Widerstände für beide ISDN-Anschlüsse aktiv.

Achtung

Trennen Sie vor der Konfiguration der ISDN-Anschlüsse das Gerät von der Stromzufuhr. Ein Ziehen und/oder Stecken der Module im laufenden Betrieb führt zu Fehlern.

3.3 Reset Taster

Links neben den Slots zur Konfiguration der ISDN-Anschlüsse befindet sich der Reset-Taster, mit dem Sie einen Neustart des Geräts erzwingen oder den Auslieferungszustand wieder herstellen können (siehe *Konfiguration der ISDN-Anschlüsse* auf Seite 32).

3.4 Wandmontage

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

(1) Suchen Sie einen Montageort aus, der max. 1,5 Meter von einer 230 V ~ Netzsteck-

dose und 2,5 Meter vom Übergabepunkt des Netzbetreibers entfernt ist.

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

(3) Halten Sie die Abstände, wie auf dem Bild unten vorgegeben, ein.

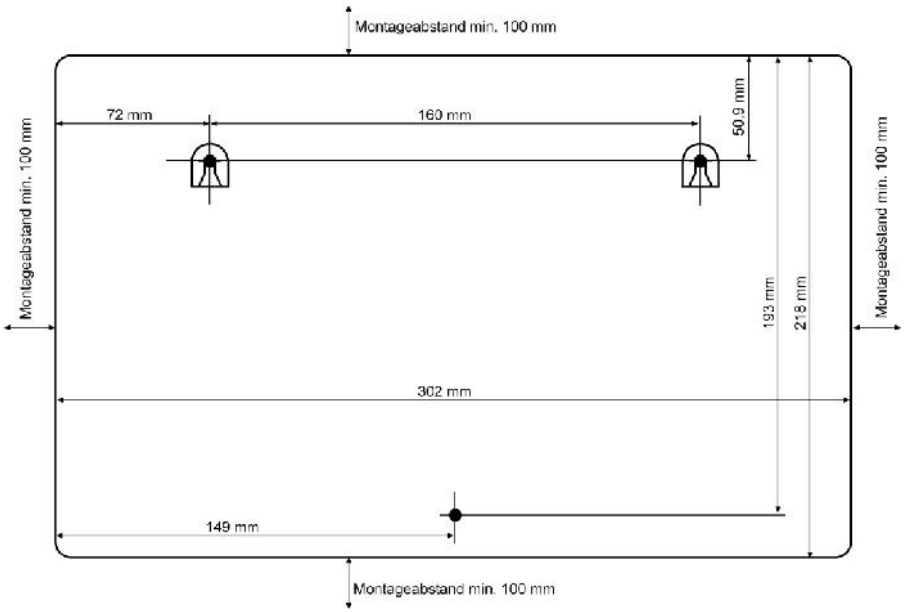


Abb. 14: Bohrschablone

(4) Markieren Sie die Bohrlöcher an der Wand.

(5) Überprüfen Sie die feste Auflage aller Befestigungspunkte der **hybird 120** / **hybird 130** an der Wand. Vergewissern Sie sich, dass im Bereich der markierten Bohrlöcher keine Versorgungsleitungen, Kabel o. ä. verlegt sind.

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

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

(8) Öffnen Sie das Gerät, indem Sie die Oberschale vorsichtig abnehmen.

(9) Hängen Sie die **hybird 120** / **hybird 130** mit den rückseitigen Halterungen von oben hinter den Schraubenköpfen ein.

(10) Schrauben Sie die untere Schraube durch das Gerät fest, damit dieses an der Wand fixiert ist.

(11) Installieren Sie, wenn erforderlich, die Anschlussdosen für die Endgeräte. Verbinden

Sie die Installation der Anschlussdosen mit der des Geräts. Die Anschlussdosen dienen der festen Installation, beispielsweise im Flur. Wenn diese installiert sind, werden die Anschlusskabel mit den Anschlüssen des Geräts verbunden.

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

(13) Verbinden Sie die **hybird 120** / **hybird 130** mit den externen Anschlüssen (ISDN und ADSL). Sie können dazu so verfahren, wie auf dem beigelegten Installationsposter beschrieben.

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

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

(16) Sie können das Gerät in Betrieb nehmen.

Kapitel 4 Service-Zugang

Wenn Montage und Verkabelung vollständig abgeschlossen sind und die Konfiguration nicht über einen lokalen PC stattfinden soll, kann die Konfiguration der **hybird 120** / **hybird 130** auch über ISDN vom **elmeg**-Kundenservice durchgeführt werden. Kontaktieren Sie dafür den Kundenservice und besprechen Sie die vorzunehmende Konfiguration.

Für die Grundkonfiguration ohne eigenen PC über ISDN gehen Sie vor wie folgt:

(1) Geben Sie an einem der angeschlossenen Telefone (analoges oder ISDN-Endgerät) die Tastenfolge **99* ein. Die **hybird 120** / **hybird 130** ist für 30 Minuten für die Service-Verbindung freigeschaltet.

(2) Daraufhin wird sich der **elmeg**-Kundendienst mit Ihrer **hybird 120** / **hybird 130** verbinden. Mit *#99* können Sie die Freigabe ggf. wieder beenden.

Kapitel 5 Reset

Der Reset wird über den Reset-Knopf im Gerät (siehe *Reset Taster* auf Seite 32) durchgeführt.

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

Drücken Sie die Reset-Taste für ca. 30 bis 40 Sekunden, führt das Gerät einen Factory Reset durch. Dies bedeutet, dass das Gerät in den Auslieferungszustand zurückversetzt wird. Die Verbindungsdaten werden dabei nicht gelöscht. Die Boot-Konfiguration wird gelöscht und alle Passwörter werden zurückgesetzt. Der Reset ist beendet, wenn sich das Gerät nach 30 bis 40 Sekunden im Betriebszustand befindet.

Hinweis

Wenn eine Konfiguration (boot) auf einer gesteckten SD-Karte gespeichert ist, ändert sich das Verhalten: Ein langer Tastendruck führt dann dazu, dass die auf dem Gerät selbst vorhandene Konfiguration gelöscht wird und das Gerät mit der auf der SD-Karte gespeicherten Konfiguration startet. Das Gerät startet ebenfalls mit einer auf der SD-Karte gespeicherten Konfiguration, wenn im Gerät selbst keine Konfiguration gespeichert ist.

Kapitel 6 Technische Daten

In diesem Kapitel sind die Hardware-Eigenschaften der **hybird 120** / **hybird 130** zusammengefasst.

6.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Produktname	Kabelsätze/Sonstiges	Software	Dokumentation
hybird 120 / **hybird 130**	Ethernet-Kabel (gelb) ISDN-BRI-Kabel (schwarz) Netzteil SD-Karte mit Voice Mail-Daten Schrauben und Dübel für die Wandmontage	Produkt-DVD	Kurzanleitung (de, en), Benutzerhandbuch (auf DVD)

6.2 Allgemeine Produktmerkmale

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

Allgemeine Produktmerkmale hybird 120 / hybird 130

Eigenschaft	
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	300 x 215 x 40 mm
Gewicht	ca. 900 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1400 g
Speicher	64 MB RAM, 16MB Flash ROM
Flash Card Slot	Unterstützt SD-Karten des SD-Standards Version 3. Siehe auch *SD-Karte* auf Seite 41.

Eigenschaft	
LEDs	Sieben bzw. neun Status-LEDs, je zwei LEDs pro Ethernet-Schnittstelle
Leistungsaufnahme Gerät	30 W 12 VDC
Spannungsversorgung	12 V DC 2,4 A
Umweltanforderungen:	
Lagertemperatur	-20 °C bis +70 °C
Betriebstemperatur	+5 °C bis +40 °C
Relative Luftfeuchtigkeit	max. 85 %
Raumklassifizierung	Nur in trockenen Räumen betreiben
Verfügbare Schnittstellen:	
ADSL-Schnittstelle	Internes ADSL2+-Modem für Annex B und für Annex J, bzw. für Annex A
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, auto-sensing, MDIX
ISDN-BRI	2 schaltbare ISDN-Schnitstellen, unterstützen S0 extern und intern, Up0 intern; ISDN-Terminierung mit 2x 100 Ohm, Speisespannung von 2 Watt, Anschluss über Buchse oder Klemmtechnik
FXS	4 FXS-Schnittstellen (**hybird 120**), Anschluss über Buchse und/oder Klemmtechnik 6 FXS-Schnittstellen (**hybird 130**), Anschluss über Buchse und/oder Klemmtechnik
FXO	1 FXO-Schnittstelle
Up0-Schnittstelle (nur **hybird 130**)	2x Up0-Schnittstelle
Schaltkontakt (nur **hybird 130**)	Klemmblock zum Anschluss z. B: von TFE-Adaptern
USB Console (Type B)	Baudraten: 1200 - 115200 Baud, Standard: 9600 Baud
USB (Type A)	derzeit nicht unterstützt
Vorhandene Buchsen:	

Eigenschaft	
USB Console	Standard USB-Type-B-Buchse
USB	Standard USB-Type-A-Buchse
Ethernet-Schnittstellen	RJ45-Buchse
ISDN-BRI-Schnittstelle	RJ45-Buchse
FXS-Schnittstelle	RJ12-Buchse
FXO-Schnittstelle	RJ12-Buchse
ADSL-Schnittstelle	RJ45-Buchse
Hohlsteckerbuchse für Stromversorgung	

6.3 LEDs

Die LEDs geben Aufschluss über Aktivitäten und Zustände des Geräts.

Die LEDs Ihrer **hybird 120** / **hybird 130** sind folgendermaßen angeordnet:

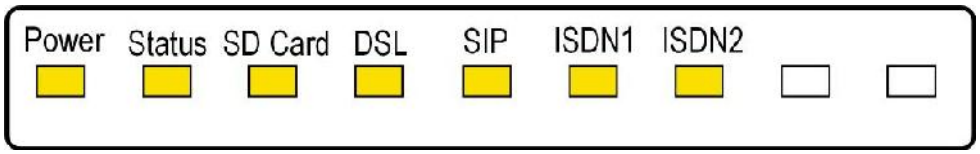


Abb. 15: LEDs **hybird 120**

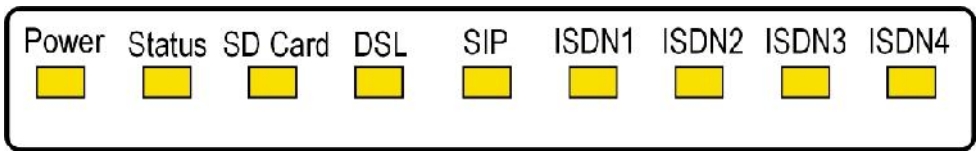


Abb. 16: LEDs **hybird 130**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
Power	Gelb	an	Stromversorgung angeschlossen

LED	Farbe	Status	Information
		aus	keine Stromversorgung
Status	Gelb	an	nach dem Einschalten: Gerät wird gestartet während des Betriebs: Fehler
		langsam blinkend	Gerät ist aktiv
SD Card	Gelb	an	SD-Karte gesteckt, keine Lese-/Schreibzugriffe
		aus	keine SD-Karte gesteckt
		flackernd	Lese-/ Schreibzugriff
DSL	Gelb	aus	keine Synchronisierung
		langsam blinkend	Synchronisation läuft
		an	Verbindung hergestellt
		flackernd	Datentransfer
SIP	Gelb	an	erfolgreich beim SIP-Provider registriert
		aus	keine SIP-Registrierung
ISDN1 bis ISDN 2	Gelb	an	Schicht 1 ist aktiv
		aus	Ruhezustand bzw. außer Betrieb
		langsam blinkend	ein B-Kanal ist aktiv
		schnell blinkend	zwei B-Kanäle sind aktiv
ISDN1 bis ISDN 4 (**hybird 130**)	Gelb	an	Schicht 1 ist aktiv

LED	Farbe	Status	Information
		aus	Ruhezustand bzw. außer Betrieb
		langsam blinkend	ein B-Kanal ist aktiv
		schnell blinkend	zwei B-Kanäle sind aktiv

Die LEDs der Ethernet-Buchsen zeigen folgende Statusinformationen an:

Ethernet-LEDs

LED	Farbe	Status	Information
ETH 1 bis 4	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
	grün	blinkend	Datenverkehr mit 1 Gbit/s.
	gelb	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
	gelb	blinkend	Datenverkehr mit 100 Mbit/s.
	grün und gelb	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und gelb	blinkend	Datenverkehr mit 10 Mbit/s.

6.4 SD-Karte

Die **hybird 120** / **hybird 130** unterstützt grundsätzlich SD-Karten des SD-Standards Version 3. Die bintec elmeg GmbH hat folgende Karten qualifiziert:

- SanDisk SDSDAA-001G - 1 GB
- SanDisk SDSDAA-002G - 2 GB

6.5 Pin-Belegungen

6.5.1 USB-Console-Schnittstelle

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

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

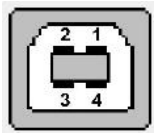


Abb. 17: USB-Type-B-Buchse

Die Pin-Belegung ist wie folgt:

Pin-Belegung der USB-Type-B-Buchse

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

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

6.5.2 Ethernet-Schnittstellen

Die Geräte verfügen über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4).

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

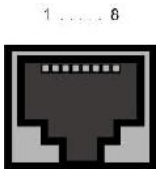


Abb. 18: Ethernet-10/100/1000 Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

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

6.5.3 ISDN-BRI-Schnittstelle

Der Anschluss erfolgt über eine RJ45-Buchse:

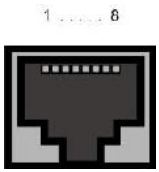


Abb. 19: ISDN-BRI-Schnittstelle (RJ45-Buchse)

Die Pin-Zuordnung für die ISDN-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

6.5.4 FXS-Schnittstellen

Die Endgeräte werden an die FXS-Schnittstellen (RJ12-Buchse) mit einem RJ11-Stecker angeschlossen.

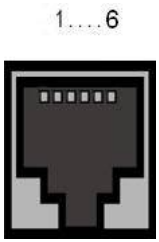


Abb. 20: FXS-Schnittstelle (RJ12)

Die Pin-Zuordnung für die FXS-Schnittstelle (RJ12-Buchse) ist wie folgt:

RJ12-Buchse für FXS-Anschluss

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	FXS
4	FXS
5	Nicht genutzt
6	Nicht genutzt

6.5.5 ADSL-Schnittstelle

Die **hybird 120** / **hybird 130** verfügt über eine ADSL-Schnittstelle.

Die ADSL-Schnittstelle wird mittels eines RJ45-Steckers angebunden.

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

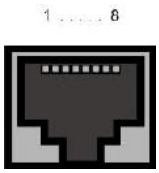


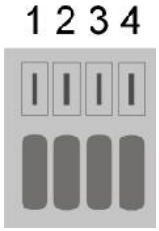
Abb. 21: ADSL-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ADSL-Anschluss

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

6.5.6 Klemmblöcke FXO

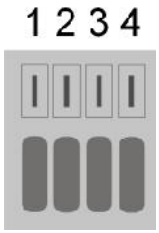


Pin-Belegung der FXO-Blöcke

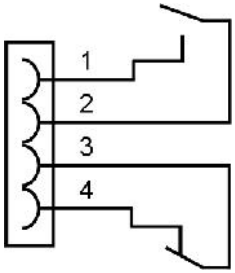
Pin	Funktion
1	a1
2	b1
3	a2
4	b2

Die Beschaltung der weiteren Blöcke ist analog (a/b3 bis a/b6).

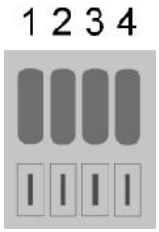
6.5.7 Klemmblock Schaltkontakt



Der Schaltkontakblock ist folgendermaßen belegt:



6.5.8 Klemmblöcke ISDN



Pin-Belegung der ISDN-Blöcke im TE-Modus

Pin	Funktion
1	RX+
2	RX-
3	TX+
4	TX-

Pin-Belegung der ISDN-Blöcke im NT-Modus

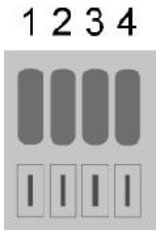
Pin	Funktion
1	TX+

Pin	Funktion
2	TX-
3	RX+
4	RX-

Pin-Belegung der ISDN-Blöcke im Up0-Modus

Pin	Funktion
1	Up0 a
2	Up0 b

6.5.9 Klemmblock Up0



Pin-Belegung des Up0-Blocks

Pin	Funktion
1	UPn1 La
2	UPn1 Lb
3	UPn2 La
4	UPn2 Lb

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 Grundkonfiguration

Sie können die Konfiguration Ihres Geräts auch selber mit der Konfigurationsoberfläche durchführen.

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

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

7.1 Vorbereitungen

Ihr Gerät ist werksseitig als DHCP-Server eingerichtet, es übermittelt also PCs in Ihrem LAN, die über keine IP-Konfiguration verfügen, alle für eine Verbindung notwendigen Einstellungen. Wie Sie Ihren PC, mit dem Sie die Grundkonfiguration durchführen wollen, für den automatischen Bezug einer IP-Konfiguration einrichten, ist in *PC einrichten* auf Seite 51 beschrieben.

Hinweis

Sollten Sie in Ihrem LAN bereits einen DHCP-Server betreiben, empfiehlt sich die Konfiguration des Geräts an einem Einzel-PC, der nicht in Ihr LAN integriert ist. Schließen Sie diesen PC allein an Ihre **hybird 120** / **hybird 130** an, so dass zur Konfiguration ein eigenes Netz entsteht.

7.1.1 Systemsoftware

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 der Konfigurationsoberfläche im Menü **Wartung**->**Software &Konfiguration** vornehmen. Eine Beschreibung der Vorgehensweise finden Sie in *Softwareaktualisierung hybird 120 / hybird 130* auf Seite 57.

7.1.2 System-Voraussetzungen

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

- Betriebssystem Microsoft Windows ab Windows 2000; Windows XP SP3 erfordert folgen-

den Hotfix: *http://support.microsoft.com/kb/953761*.

- Internet Explorer 7 oder 9 (ggf. Sicherheitseinstellungen anpassen), Mozilla Firefox ab Version 4
- Installierte Netzwerkkarte (Ethernet)
- Installiertes TCP/IP-Protokoll
- Hohe Farbanzeige (mehr als 256 Farben) für die korrekte Darstellung der Grafiken

7.1.3 Daten sammeln

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

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

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

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

Grundkonfiguration

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

Netzwerkeinstellungen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	`192.168.0.250`	
Netzmaske Ihres Gateways	`255.255.255.0`	

SIP-Provider

Zugangsdaten	Beispielwert	Ihre Werte
Beschreibung	Geben Sie den Namen Ihres SIP-Providers an, z.B. `Sipgate`.	

Zugangsdaten	Beispielwert	Ihre Werte
Authentifizierungs-ID	Geben Sie Ihre ID ein, bei Sipgate z.B.: *3223174e1*	
Passwort	Geben Sie Ihr Passwort ein, das Sie vom SIP-Provider erhalten haben.	
Registrar	Geben Sie den entsprechenden Registrar ein. Bei Sipgate: *sipgate.de*	
Rufnummer	z. B. *123456*	

ISDN-Mehrgeräteanschluss

Zugangsdaten	Beispielwert	Ihre Werte
Mehrgeräteanschlussrufnummer	*123456*	
Durchwahlrufnummern	*10, 11, 12, 13 usw.*	

Daten für den Internetzugang über ADSL

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

7.1.4 PC einrichten

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

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

TCP/IP-Protokoll prüfen

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

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

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

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

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

TCP/IP-Protokoll installieren

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

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

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

(3) Klicken Sie auf **Hinzufügen**.

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

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

Windows PC als DHCP-Client konfigurieren

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

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

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

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

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

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

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

Hinweis

Zur Konfiguration können Sie nun die Konfigurationsoberfläche aufrufen, indem Sie in einem unterstützten Browser (Internet Explorer ab Version 6, Mozilla Firefox ab Version 1.2) die vorkonfigurierte IP-Adresse Ihres Gerätes eingeben (192.168.0.250) und sich mit den voreingestellten Anmeldedaten (**User**: `admin`, **Password**: `admin`) anmelden.

7.2 Konfiguration des Systems

7.2.1 Systempasswort ändern

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

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

  - Kleinbuchstaben [a-z]

  - Großbuchstaben [A-Z]

  - Zahlen [0-9]

  - Sonderzeichen

Hinweis

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

7.2.2 Netzwerkeinstellung (LAN)

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

7.2.3 SIP-Provider eintragen

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

7.2.4 ISDN-Mehrgeräteanschluss

Im Auslieferungszustand ist die **hybird 120** / **hybird 130** bereits für den Betrieb an einem ISDN-Mehrgeräteanschuss vorbereitet. Nach dem Anschließen der **hybird 120** / **hybird 130** am ISDN-Mehrgeräteanschluss muss die Status-Anzeige auf einen grünen Pfeil wechseln.

(1) Gehen Sie ins Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN Extern**.

Gehen Sie in folgendes Menü, um die Einzelrufnummer (MSN) zu konfigurieren:

(1) Gehen Sie zu **Nummerierung**->**Externe Anschlüsse**->**Rufnummern**->**Neu**.

(2) Wählen Sie bei **Externer Anschluss** den Anschluss aus, für den Sie die Rufnummernkonfiguration vornehmen wollen, hier *ISDN Extern*.

(3) Bei **Rufnummerntyp** wurde bereits die Option *Einzelrufnummer (MSN)* vorbelegt.

(4) Im Feld **Einzelrufnummer (MSN)** wird eine der vom Provider vergebenen Rufnummern hinterlegt, z. B. *123456*.

(5) Bestätigen Sie mit **OK**.

Durchwahlrufnummern tragen Sie in einem späteren Schritt in den **Benutzereinstellungen** ein. Gegebenenfalls nutzen Sie die für die Benutzer voreingestellten Werte.

Ihr Gerät ist nun für das Telefonieren über Ihren ISDN-Mehrgeräteanschluss eingerichtet.

7.2.5 ISDN-Anlagenanschluss

Haben Sie einen ISDN-Anlagenanschluss beauftragt, müssen Sie noch einige Eintragungen vornehmen.

Gehen Sie in folgendes Menü, um den externen ISDN-Port zu konfigurieren:

(1) Gehen Sie zu **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN Extern**->  .

(2) Geben Sie eine benutzerdefinierte **Beschreibung** der ISDN-Schnittstelle an, z. B. *ISDN Extern*.

(3) Wählen Sie für **Anschlussart** die Einstellung *Anlagenanschluss*.

(4) Bestätigen Sie die Angaben mit **OK**.

Gehen Sie in folgendes Menü, um den externe ISDN-Anschluss zu konfigurieren:

(1) Gehen Sie zu **Nummerierung**->**Externe Anschlüsse**->**Anschlüsse**.

(2) Löschen Sie den vordefinierten Eintrag *ISDN Extern* indem Sie auf das  -Symbol klicken.

Mit **Neu** fügen Sie einen neuen Eintrag zur Konfiguration Ihres ISDN-Anlagenanschlusses ein.

(1) Gehen Sie zu **Nummerierung**->**Externe Anschlüsse**->**Anschlüsse**->**Neu** bei dem Eintrag mit **Beschreibung** *ISDN Extern*.

(1) Wählen Sie bei **Anschlussart** *Anlagenanschluss* aus.

(2) Bei **Externer Port** fügen sie mit der Option **Hinzufügen** den bereits konfigurierten externen Port z. B. *ISDN Extern* ein.

(3) Bestätigen Sie Ihre Angaben mit **OK**.

Gehen Sie in folgendes Menü, um die Anlagenanschlussrufnummer zu konfigurieren:

(1) Gehen Sie zu **Nummerierung**->**Externe Anschlüsse**->**Rufnummern**->**Neu**.

(2) Wählen Sie bei **Externer Anschluss** den Anschluss aus, für den Sie die Rufnummernkonfiguration vornehmen wollen, hier *ISDN Extern*.

(3) Belassen Sie bei **Rufnummerntyp** die Auswahl *Anlagenanschluss-Rufnummer*.

(4) Tragen Sie bei **Anlagenanschluss-Rufnummer** Ihre Anlagenanschlussrufnummer ein (ohne Durchwahlrufnummer), z. B. *123456*.

(5) Bestätigen Sie mit **OK**.

Durchwahlrufnummern tragen Sie in einem späteren Schritt in den **Benutzereinstellungen** ein. Gegebenenfalls nutzen Sie die für die Benutzer voreingestellten Werte.

Ihr Gerät ist nun für das Telefonieren über Ihren ISDN-Anlagenanschluss eingerichtet.

7.3 Internetverbindung einrichten

Sie können mit Ihrem Gerät eine Internetverbindung aufbauen.

7.3.1 Internetverbindung über das interne ADSL-Modem

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

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

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

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

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

7.3.2 Andere Internetverbindungen

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

7.3.3 Konfiguration prüfen

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

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

(1) Testen Sie die Verbindung von einem beliebigen Gerät im lokalen Netzwerk zum Gerät. Klicken Sie im Windows-Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihres Geräts ein (z. B. *192.168.0.250*). Es erscheint ein Fenster mit dem Hinweis `"Antwort von..."`.

(2) Testen Sie den Internetzugang, indem Sie im Internet Browser *http://www.bintec-elmeg.com* eingeben.

Hinweis

Durch eine Fehlkonfiguration von Endgeräten kann es zu ungewollten Verbindungen und erhöhten Gebühren kommen! Kontrollieren Sie, ob das Gerät Verbindungen nur zu gewollten Zeiten aufbaut! Beobachten Sie die Leuchtanzeigen Ihres Geräts (Leuchtanzeige ISDN, DSL und die der Ethernet-Schnittstellen).

7.4 Benutzerzugang

Der Administrator des Systems kann jedem Benutzer einen individuellen Konfigurationszugang einrichten. So können die Benutzer ihre wichtigsten persönlichen Einstellungen einsehen und individuell anpassen.

Hinweis

Der Administrator hat Zugriff auf Einstellungen und Daten aller Benutzer. Lediglich das persönliche Telefonbuch (**Benutzertelefonbuch**), das der Benutzer sich individuell einrichten kann, kann nur mit den persönlichen Benutzer-Login-Daten verwaltet und eingesehen werden.

Um sich mit den Ihnen zugewiesenen Zugangsdaten an der Konfigurationsoberfläche anzumelden, geben Sie im Login-Fenster Ihren **Benutzernamen** und Ihr **Passwort** ein.

Der Administrator konfiguriert die Benutzerzugänge im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**.

Hilfe zu den verfügbaren Konfigurationsoptionen erhalten die Benutzer ebenfalls über das Online-Hilfe-System.

7.5 Softwareaktualisierung hybird 120 / hybird 130

Die Funktionsvielfalt der **hybird 120** / **hybird 130** wird permanent erweitert. Diese Erweiterungen stellt Ihnen die bintec elmeg GmbH zur Verfügung. Die Überprüfung auf neue Software-Versionen und die Aktualisierung können einfach über das **GUI** vorgenommen werden. Voraussetzung für ein automatisches Update ist eine bestehende Internetverbindung.

Gehen Sie folgendermaßen vor:

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

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

(3) Bestätigen Sie mit **Los**.

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

Achtung

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

Kapitel 8 Bedienung über das Telefon

Die Bedienung bzw. Konfiguration der Anlage über ein Telefon ist in zwei eigenen Dokumenten beschrieben:

- Eine ausführliche Beschreibung aller verfügbaren Prozeduren finden Sie in "Bedienung über das Telefon". Sie finden das Dokument auf der Companion CD oder aber als Download unter *http://bintec-elmeg.com*
- Ein Faltblatt mit den wichtigsten Prozeduren steht ebenfalls auf der CD und als Download zur Verfügung.

Kapitel 9 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

9.1 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 (nur für Service-Techniker und Debug-Zwecke)

9.1.1 Zugang über LAN

Der Zugang über eine der Ethernet-Schnittstellen Ihres Geräts ermöglicht es Ihnen, die Konfigurationsoberfläche in einem Web-Browser zu öffnen.

9.1.1.1 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://192.168.0.250*

  oder

  https://192.168.0.250

9.1.2 Zugang über die serielle Schnittstelle

Die **hybird 120** / **hybird 130** 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.

Achtung

Der Zugang über die serielle Schnittstelle wird nur für Service-Techniker empfohlen, für Debug-Zwecke und wenn ein LAN-Zugang über die vorkonfigurierte IP-Adresse (192.168.0.250 / 255.255.255.0) nicht möglich ist. Die möglichen Operationen, die ausgeführt werden können, werden angezeigt, wenn Sie `?` in die Kommandozeile eingeben und mit der **Eingabetaste** bestätigen.

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) Starten Sie das Terminal-Programm, z. B. HyperTerminal.

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

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

Überprüfen

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

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

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

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

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

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

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

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

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

Unix

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

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

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

9.2 Konfiguration

Die Konfiguration wird mit der HTML-Konfigurationsoberfläche durchgeführt.

9.2.1 Konfigurationsoberfläche

Die Konfigurationsoberfläche 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 der Konfigurationsoberfläche können Sie alle Konfigurationsaufgaben einfach und komfortabel durchführen. Es ist in Ihr Gerät integriert und steht in Englisch zur Verfügung.

Die Einstellungsänderungen, die Sie 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 der Konfigurationsoberfläche können Sie ebenfalls die wichtigsten Funktionsparameter Ihres Geräts überwachen.

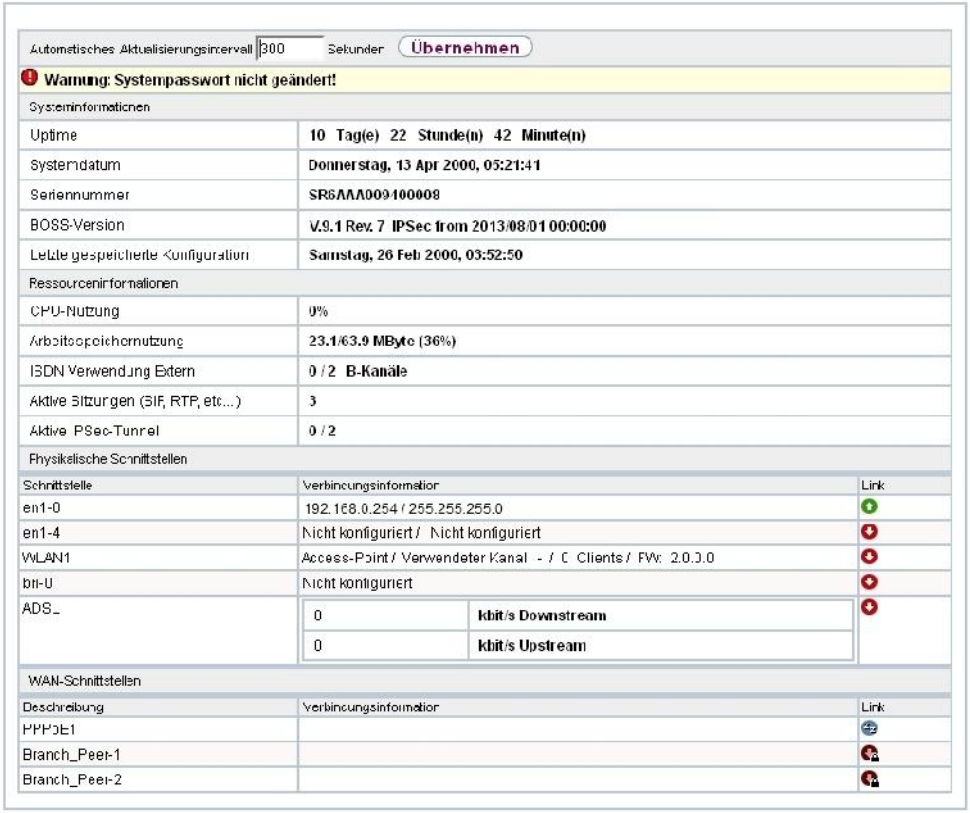


Abb. 23: Konfigurationsoberfläche Startseite

9.2.1.1 Die Konfigurationsoberfläche aufrufen

(1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind (siehe *Aufstellen und Anschließen* auf Seite 12).

(2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten.

(3) Öffnen Sie einen Webbrowser.

(4) Geben Sie `http://192.168.0.250` in das Adressfeld des Webbrowsers ein.

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

Sie befinden sich nun im Statusmenü der Konfigurationsoberfläche Ihres Geräts.

9.2.1.2 Bedienelemente

Fenster der Konfigurationsoberfläche

Das Fenster der Konfigurationsoberfläche ist in drei Bereiche geteilt:

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

Abb. 24: Bereiche der Konfigurationsoberfläche

Kopfleiste

Abb. 25: Konfigurationsoberfläche Kopfleiste

Konfigurationsoberfläche Kopfleiste

Menü	Funktion
Sprache Deutsch	**Sprache**: Wählen Sie in dem Dropdown-Menü die gewünschte

Menü	Funktion
	Sprache aus, in der die Konfigurationsoberfläche angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen *Deutsch* und *English*.
	**Ansicht**: Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl steht *Standard* und *SNMP-Browser*.
Online-Hilfe	**Online-Hilfe**: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Die Beschreibung des Untermenüs, in dem Sie sich gerade befinden, wird angezeigt.
Ausloggen	**Ausloggen**: Wenn Sie die Konfiguration beenden möchten, klicken Sie auf diese Schaltfläche, um sich von Ihrem Gerät abzumelden. Es wird ein Fenster geöffnet, in dem Ihnen folgende Optionen angeboten werden: • mit der Konfiguration fortfahren, • die Konfiguration speichern und das Fenster schließen, • die Konfiguration ohne Speichern verlassen.

Navigationsleiste

Abb. 26: Konfiguration speichern Schaltfläche

Abb. 27: 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 auf die Schaltfläche **Konfiguration speichern** klicken, erscheint die Frage: "Möchten Sie die aktuelle Konfiguration wirklich als Boot-Konfiguration speichern?"

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 die Konfigurationsoberfläche aufrufen, erscheint nach der Anmeldung zunächst die Statusseite Ihres Geräts. Auf dieser werden die wichtigsten Daten Ihres Geräts auf einen Blick sichtbar.

Hauptkonfigurationsfenster

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

Konfigurationselemente

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

Schaltflächen

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

Symbole

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

Symbol	Funktion
	Zeigt die Details eines Eintrags an.
	Können die Voice-Mail-Nachricht angehört werden.
	Werden die Nachrichten gespeichert.
	Mit diesem Symbol gelangen Sie auf die Benutzeroberfläche des **elmeg** IP1x0-Telefons.
	Verschiebt einen Eintrag. Es öffnet sich eine Combobox, in der Sie auswählen können, vor / hinter welchen Listeneintrag der ausgewählte Eintrag verschoben werden soll.
	Legt einen weiteren Listeneintrag vorher an und öffnet das Konfigurationsmenü.
	Setzt den Status des Eintrags auf *Inaktiv*.
	Setzt den Status des Eintrags auf *Aktiv*.
	Kennzeichnet den Status "Ruhend" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Aktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Inaktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Blockiert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet 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.

Listenoptionen

Menü	Funktion
Aktualisierungsintervall	Hier können Sie das Intervall einstellen, in dem die Ansicht aktualisiert werden soll.

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

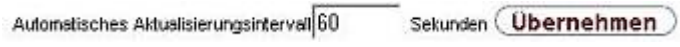


Abb. 28: Konfiguration des Aktualisierungsintervalls

Abb. 29: Liste filtern

Struktur der Konfigurationsmenüs

Die Menüs enthalten folgende Grundstrukturen:

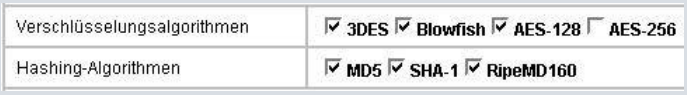
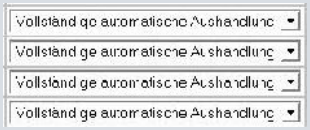
Menüstruktur

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

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

Für die Konfiguration stehen folgende Optionen zur Verfügung:

Konfigurationselemente

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

Menü	Funktion
Interne Listen	z. B.  Klicken Sie auf die Schaltfläche Hinzufügen. 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 über eine serielle Verbindung vorgenommen wurden.
	Dieses Symbol erscheint in Meldungen, die Sie darauf hinweisen, dass Werte falsch eingegeben bzw. ausgewählt wurden.

9.2.1.3 Menüs

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

Hinweis

Beachten Sie, dass nicht alle Geräte über den maximal möglichen Funktionsumfang verfügen. Prüfen Sie die Software-Ausstattung Ihres Geräts anhand Ihrer Produktspezifikation.

Kapitel 10 Assistenten

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

- **Erste Schritte**
- **Internetzugang**
- **VPN**
- **PBX**

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

Kapitel 11 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.

11.1 Status

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

Sie erhalten einen Überblick über folgende Daten:

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

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

Achtung

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

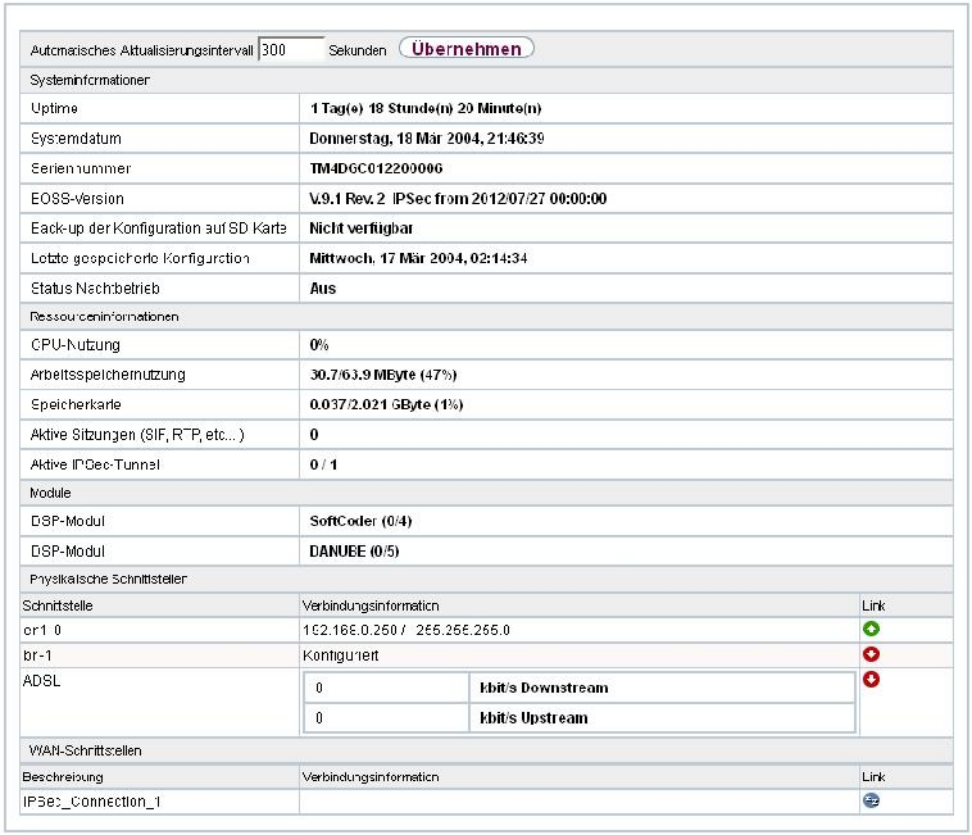


Abb. 30: **Systemverwaltung->Status**

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.
Back-up der Konfiguration auf SD Karte	Zeigt an, ob ein Back-up der Konfiguration auf der SD-Karte verfügbar ist oder nicht.

Feld	Wert
Letzte gespeicherte Konfiguration	Zeigt Tag, Datum und Uhrzeit der letzten Konfigurationsspeicherung (Boot-Konfiguration im Flash) an.
Status Nachtbetrieb	Zeigt an, ob sich Ihr Gerät im Normalbetrieb (*Aus*) oder im Nachtbetrieb (*An*) befindet.

Felder im Menü Ressourceninformationen

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

Felder im Menü Module

Feld	Wert
DSP-Modul	Zeigt den Typ eines gegebenenfalls gesteckten DSP-Moduls und die aktuell belegten DSP-Kanäle (belegt / vorhanden) an. Optional wird eine ggf. erworbene Fax-Lizenz angezeigt.

Felder im Menü Physikalische Schnittstellen

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

Feld	Wert
	• Netzmaske • Nicht konfiguriert Schnittstellendetails für ISDN-Schnittstellen: • Konfiguriert • Nicht konfiguriert Schnittstellendetails für xDSL-Schnittstellen: • Leitungsgeschwindigkeit Downstream/Upstream

Felder im Menü WAN-Schnittstellen

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

11.2 Globale Einstellungen

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

11.2.1 System

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

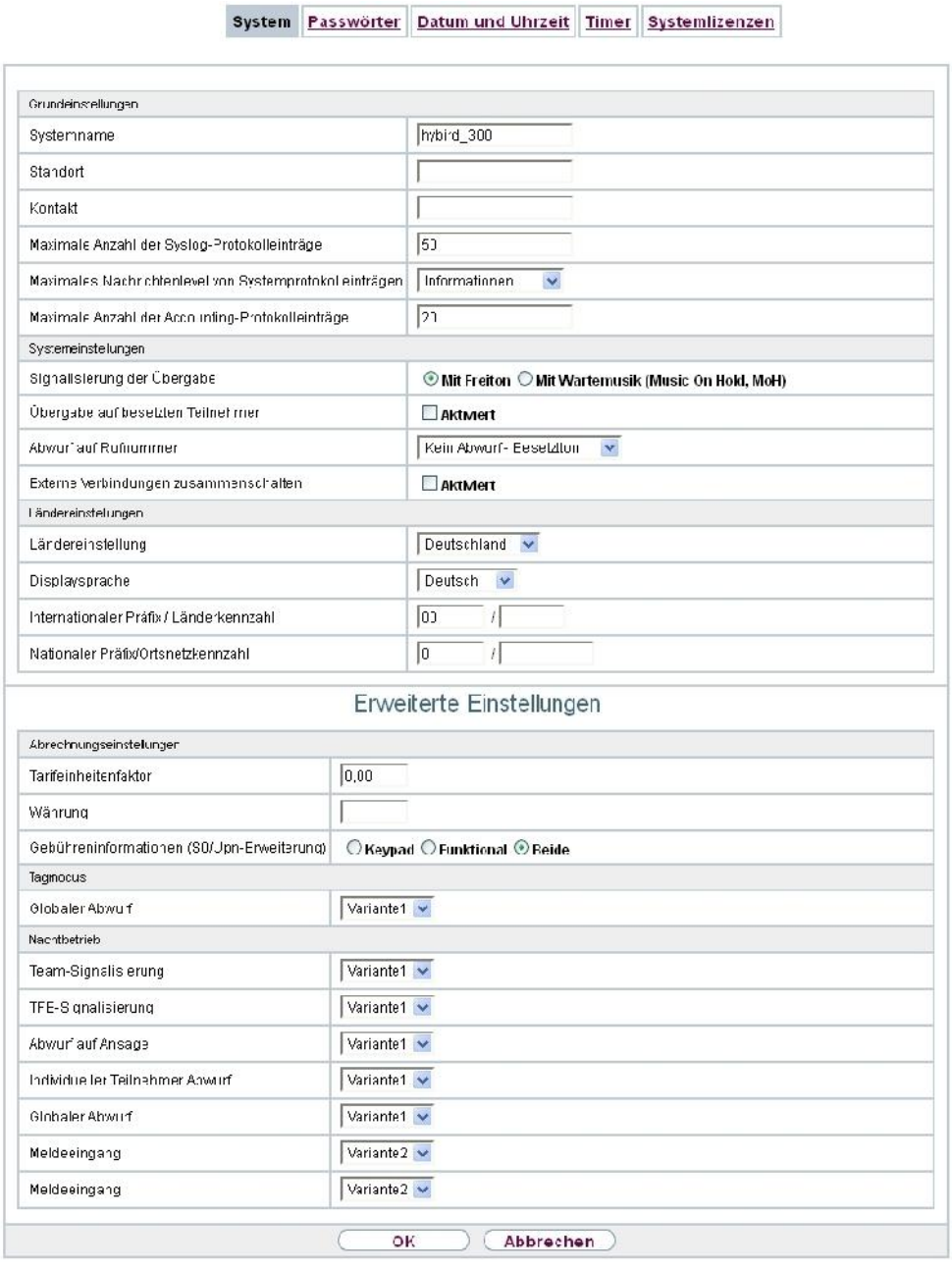


Abb. 31: **Systemverwaltung**->**Globale Einstellungen**->**System**

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

Felder im Menü Grundeinstellungen

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

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 für Login-Vorgänge auf dem Gerät intern gespeichert werden sollen. Mögliche Werte sind *0* bis *1000*. Der Standardwert ist *20*.

Übergabe auf besetzten Teilnehmer

In der Konfiguration kann festgelegt werden, ob die Weitergabe eines Gesprächs auf einen besetzten Teilnehmer möglich ist oder bei "Aus" der Anrufer den Besetztton hört und damit der Anruf beendet ist. Sonst wird der Anrufer gehalten und hört den Freiton oder die Wartemusik. Legt der Zielteilnehmer den Hörer auf, hört der gehaltenen Teilnehmer den Freiton. Der Zielteilnehmer wird gerufen und er kann das gehaltene Gespräch übernehmen.

Felder im Menü Systemeinstellungen

Feld	Wert
Signalisierung der Übergabe	Stellen Sie ein, wie das Vermitteln auf einen internen Teilnehmer erfolgen soll. Mögliche Werte: • *Mit Freiton* (Standardwert): Der Anrufer hört während er vermittelt wird den Freiton. • *Mit Wartemusik (Music On Hold, MoH)*: Der Anrufer hört während er vermittelt wird eine Wartemusik des Systems.
Übergabe auf besetzten Teilnehmer	Stellen Sie ein, ob das Vermitteln eines Anrufers auf einen besetzten Teilnehmer möglich ist. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv.

Feld	Wert
Abwurf auf Rufnummer	Stellen Sie ein, auf welches Ziel kommende Anrufe z. B. bei Falschwahl abgeworfen werden sollen. Mögliche Werte: • *Kein Abwurf - Besetztton*: Der Anrufer hört standardmäßig den Besetztton und kann nicht auf ein Ziel abgeworfen werden. • *<Rufnummer>*: Der kommende Anruf wird standardmäßig an die ausgewählte Rufnummer geleitet. Standardwert ist die voreingestellte Internrufnummer *40 (Team global)*.
Externe Verbindungen zusammenschalten	Wählen Sie aus, ob beim Makeln mit zwei Externteilnehmern diese, nachdem Sie den Hörer aufgelegt haben, verbunden werden. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv.

Ländereinstellungen

Ihr Unternehmen ist international ausgerichtet und hat Niederlassungen in mehreren Ländern. Trotz der abweichenden Netz-Realisierung in den einzelnen Ländern möchten Sie in jeder Niederlassung das gleiche System einsetzen. Durch die Einstellung der Ländervariante wird das System an die Besonderheiten des Netzes in dem gewünschten Land angepasst.

Da die Anforderungen an das System von Land zu Land unterschiedlich sind, muss die Funktionalität einiger Leistungsmerkmale angepasst werden. Im System sind die Grundeinstellungen für verschiedene Ländervarianten gespeichert.

Felder im Menü Ländereinstellungen

Feld	Wert
Ländereinstellung	Wählen Sie das Land aus, in dem das System genutzt werden soll. Beachte: Hiermit wird nicht die Sprache der Texte im Systemmenü der Systemtelefone umgestellt. Mögliche Werte:

Feld	Wert
	• *Deutschland* (Standardwert) • *Nederland* • *Great Britain* • *België* • *Italia* • *Danmark* • *España* • *Sverige* • *Norge* • *France* • *Portugal* • *Österreich* • *Schweiz* • *Česko* • *Slovenija* • *Polska* • *Magyarország* • *Ellada*
Displaysprache	Stellen Sie die gewünschte Sprache für das Systemmenü ein. Das System stellt Systemtelefonen ein spezielles Menü - Systemmenü - mit systemtypischen Funktionen zur Verfügung. Die Anzeigen im Systemmenü können in verschiedenen Sprachen erfolgen. Diese Sprachanzeigen sind unabhängig von den Einstellungen in den einzelnen Systemtelefonen. Mögliche Werte: • *Deutsch* (Standardwert) • *Englisch* • *Italienisch*
Internationaler Präfix / Länderkennzahl	Geben Sie die Länderkennzahl ein. Sie benötigen diesen Eintrag, wenn Sie z. B. unter **SIP-Provider** eine internationale Rufnummer automatisch generieren lassen möchten. Sie wählen wie gewohnt die nationale Vor-

Feld	Wert
	wahl z. B. 05151 909999 und das System wählt dann automatisch +495151 909999. Tragen Sie die Länderkennzahl nicht ein, kann es zur Falschwahl kommen, das System wählt dann +5151 909999. Ohne den Eintrag **Internationale Rufnummer erzeugen** und **Internationaler Präfix / Länderkennzahl** muss bei SIP-Providern immer die vollständige Rufnummer mit Länderkennzahl gewählt werden. Beachte: Nicht alle SIP-Provider unterstützen diese Einstellung.
Nationaler Präfix/ Ortsnetzkennzahl	Tragen Sie den nationalen Präfix bzw. die Ortsnetzkennzahl für den Ort ein, an der Ihr System installiert ist. Diese Ortsnetzkennzahl wird beim Anlagenanschluss dringend benötigt, da sonst z. B. der automatische Rückruf nach extern nicht möglich ist.

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

Felder im Menü Abrechnungseinstellungen

Feld	Wert
Tarifeinheitenfaktor	Geben Sie den Faktor für die Verbindungskosten ein. Der Standardwert ist *0,00*.
Währung	Geben Sie hier den Namen der Währung, z. B. *EUR* , ein (max. dreistellig). Diese Eingabe ist nur ein Name der in keiner Berechnung des Tarifeinheitenfaktors berücksichtigt wird. Sonderzeichen sind nicht erlaubt.
Gebühreninformationen (S0/Upn-Erweiterung)	Wählen Sie die Übertragungsmethode von Gebühreninformationen am internen S0-Bus aus. Mögliche Werte: • *Keypad*: Abhängig von Land und Provider werden die Gebühreninformationen so übertragen, dass sie direkt vom Endgerät angezeigt werden können. • *Funktional*: Die Gebühreninformationen werden binär kodiert übertragen und müssen von den Endgeräten erst dekodiert werden (EURO ISDN). • *Beide* (Standardwert): Beide Protokolle werden erkannt.

Felder im Menü Tagmodus

Feld	Wert
Globaler Abwurf	Wählen Sie die Anrufvariante im Tagmodus aus, die für das Gesamtsystem gelten soll, wenn kein spezieller Abwurf eingerichtet ist. Der Standardwert ist *Variante 1*.

Nachtbetrieb

Sie können das System in den Nachtbetrieb schalten und so bestimmte Anrufvarianten für die Team-Signalisierung, die TFE-Signalisierung und die Abwurffunktionen aktivieren.

Eine erweiterte Umschaltung der Anrufvarianten ist über eine Kennziffer oder den Kalender möglich, der für den Nachtbetrieb konfiguriert ist. Die Konfiguration eines Kalenders für den Nachtbetrieb führen Sie im Menü **Anwendungen**->**Kalender**->**Kalender**->**Neu** durch.

Felder im Menü Nachtbetrieb

Feld	Wert
Team-Signalisierung	Wählen Sie die Anrufvariante für die Team-Signalisierung im Nachtbetrieb aus.
TFE-Signalisierung	Wählen Sie die TFE-Anrufvariante für die TFE-Signalisierung im Nachtbetrieb aus.
Abwurf auf Ansage	Wählen Sie die Anrufvariante für Abwurf auf Ansage im Nachtbetrieb aus.
Individueller Teilnehmer Abwurf	Wählen Sie die Anrufvariante für Abwurf auf Durchwahl im Nachtbetrieb aus.
Globaler Abwurf	Wählen Sie die Anrufvariante für Allgemeinen Abwurf im Nachtbetrieb aus.
Meldeeingang	Wählen Sie die Anrufvariante für Alarm im Nachtbetrieb aus.

11.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

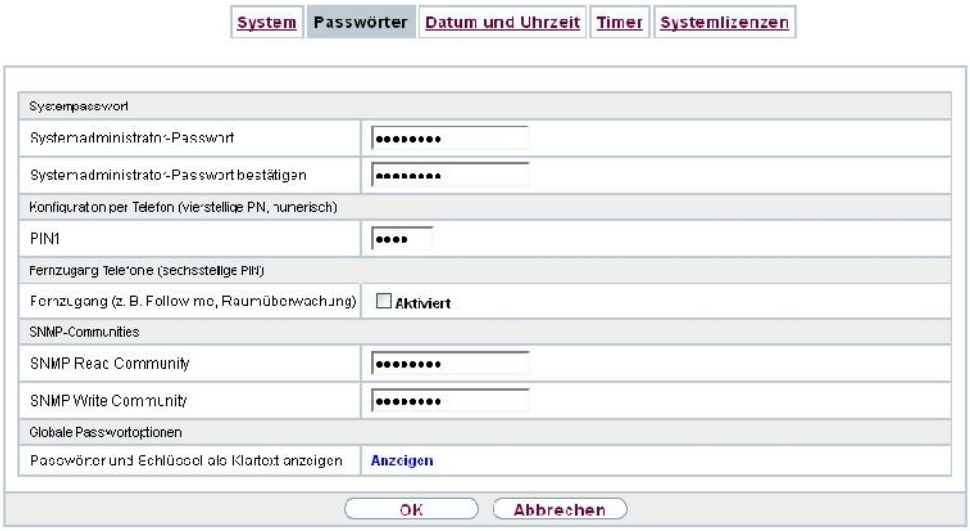


Abb. 32: **Systemverwaltung->Globale Einstellungen->Passwörter**

Hinweis

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

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

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

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

Felder im Menü Systempasswort

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

PIN1 und PIN2

Mit verschiedenen Schutzfunktionen können Sie den Missbrauch Ihres Systems durch andere verhindern. Die Einstellungen Ihres Systems schützen Sie durch eine 4-stellige PIN1 (Geheimzahl). Der Zugang von extern (Fernzugang) ist über eine 6-stellige PIN2 geschützt.

Die PIN1 ist eine vierstellige Geheimzahl, mit der Sie Anlageneinstellungen vor unbefugtem Zugriff schützen. Die PIN2 ist eine 6-stellige Geheimzahl, die verhindert, dass nicht berechtigte externe Teilnehmer Ihr System benutzen können. Erst nach Eingabe einer 6-stelligen PIN2 sind diese Funktionen nutzbar.

Verschiedene Einstellungen sind über die PIN1 des Systems geschützt. In der Grundeinstellung ist die PIN1 auf *none* eingestellt.

Folgende Leistungsmerkmale werden über die PIN2 geschützt:

- Fernzugang für Follow me, Raumüberwachung

Felder im Menü Konfiguration per Telefon (vierstellige PIN, numerisch)

Feld	Wert
PIN1	Geben Sie PIN1 ein. Durch die 4-stellige PIN1 (Geheimzahl) schützen Sie die Einstellungen Ihres Systems durch die Konfiguration über ein Telefon.

Felder im Menü Fernzugang Telefonie (sechsstellige PIN)

Feld	Wert
Fernzugang (z. B. Follow me, Raumüberwachung)	Wählen Sie aus, ob ein Fernzugang auf Ihr System gestattet werden soll. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv.
PIN2	Nur wenn **Fernzugang (z. B. Follow me, Raumüberwachung)** aktiviert ist. Geben Sie die **PIN2** ein. Der Standardwert ist *000000*. Durch die 6-stellige **PIN2** schützen Sie den Zugang von extern (Fernzugang).

Felder im Menü SNMP-Communities

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

Feld im Menü Globale Passwortoptionen

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

11.2.3 Datum und Uhrzeit

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

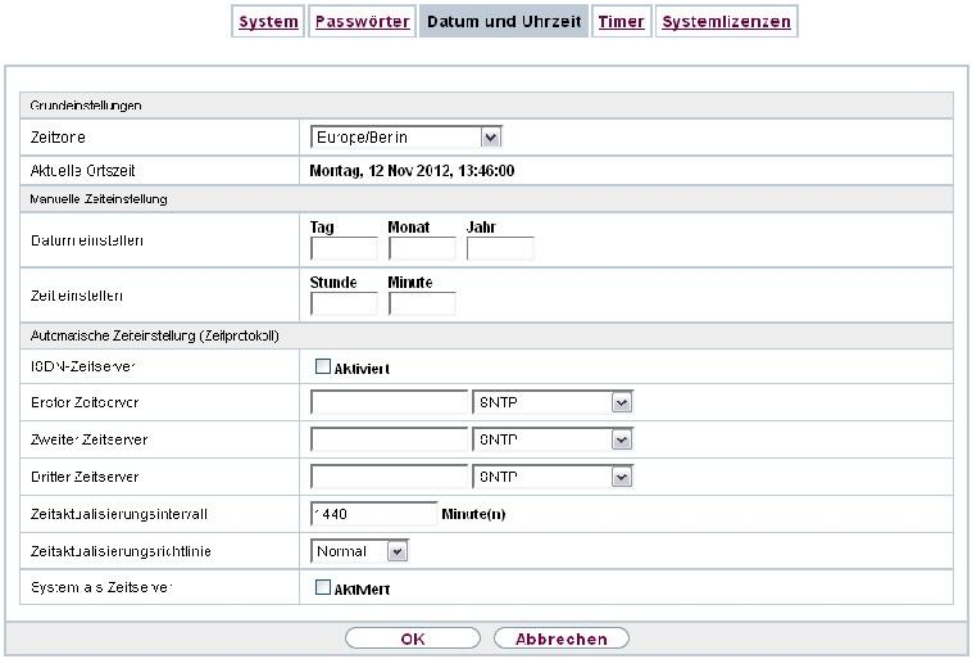


Abb. 33: **Systemverwaltung->Globale Einstellungen->Datum und Uhrzeit**

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

ISDN/Manuell

Die Systemzeit kann über ISDN aktualisiert werden, d. h. mit jeder bestehenden externen Verbindung werden Datum und Uhrzeit aus dem ISDN entnommen. Datum und Uhrzeit können auch manuell eingegeben werden z. B. wenn im ISDN Zeit und Datum nicht übertragen werden oder kein Zeitserver zur Verfügung steht. Die Uhrzeit bleibt ca. 3 Stunden nach dem Abschalten der Stromversorgung des Systems erhalten.

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

Zeitserver

Sie können die Systemzeit auch automatisch über verschiedene Zeitserver beziehen. Um

sicherzustellen, dass das Gerät die gewünschte aktuelle Zeit verwendet, sollten Sie einen oder mehrere Zeitserver konfigurieren.

Hinweis

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

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

Felder im Menü Grundeinstellungen

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

Felder im Menü Manuelle Zeiteinstellung

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

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	Legen Sie fest, ob die Systemzeit über ISDN aktualisiert werden soll. Falls ein Zeitserver konfiguriert ist, wird die Zeit nur solange über ISDN ermittelt, bis ein erfolgreiches Update von diesem Zeitserver empfangen wurde. Für den Zeitraum, in dem die Zeit über einen Zeitserver ermittelt wird, wird die Aktualisierung über ISDN außer Kraft gesetzt. Mit Auswahl von *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion aktiv.
Erster Zeitserver	Geben Sie den ersten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt. Im Auslieferungszustand ist hier der Server *ntp1.sda.t-online.de* eingetragen.
Zweiter Zeitserver	Geben Sie den zweiten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst

Feld	Beschreibung
	über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt. Im Auslieferungszustand ist hier der Server *ntp1.sul.t-online.de* eingetragen.
Dritter Zeitserver	Geben Sie den dritten Zeitserver an, entweder mit Domänennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte: • *SNTP* (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • *Time Service / UDP*: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • *Time Service / TCP*: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • *Keiner*: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird. Der Standardwert ist *1440*.
Zeitaktualisierungsrichtlinie	Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen. Mögliche Werte: • *Normal* (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen. • *Aggressiv*: Zehn Minuten lang wird versucht, den Zeitserver zuerst nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen.

Feld	Beschreibung
	• *Endlos*: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. Bei der Verwendung von Zertifikaten für die Verschlüsselung des Datenverkehrs in einem VPN ist es von zentraler Bedeutung, dass auf dem Gerät die korrekte Zeit eingestellt ist. Um dies sicherzustellen, wählen Sie für **Zeitaktualisierungsrichtlinie** den Wert *Endlos*.
System als Zeitserver	Wählen Sie aus, ob der interne Zeitserver verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Zeitanfragen eines Clients werden mit der aktuellen Systemzeit beantwortet. Diese wird als GMT ohne Offset angegeben. Standardmäßig ist die Funktion aktiv. Zeitanfragen der Clients im LAN werden beantwortet.

11.2.4 Timer

Im Menü **Timer** können Sie die Zeiten konfigurieren, nach denen bestimmte Systemmerkmale standardmäßig geschaltet werden sollen.

Abb. 34: **Systemverwaltung->Globale Einstellungen->Timer**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Rufweiterleitung (CFNR)	Geben Sie die Zeit ein, nach der eine **Rufweiterleitung (CFNR)** ausgeführt wird. Möglich sind Werte von *1* bis *99*. Der Standardwert ist *15*.
Direktruf	Geben Sie die Zeit ein, nach der beim Abheben des Hörers die konfigurierte Rufnummer gewählt wird. Sie möchten ein Telefon einrichten, bei dem die Verbindung zu einer bestimmten Rufnummer auch ohne die Eingabe der Rufnummer aufgebaut wird (z. B. Notruftelefon). Sie befinden sich außer Haus. Es gibt jedoch jemanden zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Haben Sie für ein oder mehrere Telefone die Funktion "Direktruf" eingerichtet, braucht nur der Hörer des entsprechenden Telefons abgehoben zu werden. Nach einer in der Konfiguration eingestellten Zeit ohne weitere Eingaben wählt das System automatisch die festgelegte Direktrufnummer. Wählen Sie nach dem Abheben des Hörers nicht innerhalb der vorgegebenen Zeit, wird die automatische Wahl eingeleitet. Möglich sind Werte von *1* bis *30*. Der Standardwert ist *5*.
Externe TFE-Verbindung	Wird ein TFE-Gespräch von einem externen Telefon abgefragt, können Sie hier die Zeit einstellen, nach der dieses Gespräch zwangsgetrennt wird. Mögliche Werte: • *Endlos* • *60 Sekunden* • *120 Sekunden* • *180 Sekunden* (Standardwert) • *240 Sekunden* • *300 Sekunden*

Felder im Menü Erweiterte Einstellungen

Feld	Wert
Gesprächsweitergabe ohne Melden (UbA)	Geben Sie die Zeit ein, nach der beim einleitenden Teilnehmer wieder angerufen oder angeklopft werden soll, wenn der gewünschte Teilnehmer nicht erreichbar war. Sie haben einen Anrufer an einen anderen Teilnehmer durch Vermitteln oder Übergabe weitergeleitet. Dieser Teilnehmer ist nicht erreichbar oder besetzt. Sie möchten aber verhindern, dass der Teilnehmer dann den Anruf beendet oder vom System nach Zeit abgeworfen wird. Das erreichen Sie durch einen automatischen Wiederanruf an Ihrem Telefon. Bei Gesprächen, die ohne Ankündigung weitergegeben werden (Umlegen besonderer Art, UbA) erfolgt nach der hier eingegebenen Zeit ein Wiederanruf oder Anklopfen (wenn bereits ein neues Gespräch besteht) beim einleitenden Teilnehmer. Möglich sind Werte von *10* bis *179*. Der Standardwert ist *30*.
Übergabe auf besetzten Teilnehmer	Geben Sie die Zeit ein, nach der ein Teilnehmer in der Warteschleife wieder mit der Vermittlung verbunden wird. Die Vermittlung möchte ein Gespräch an einen bestimmten Mitarbeiter weitergeben. Dieser telefoniert jedoch zur Zeit. Dann kann der Anruf in die Warteschlange des Teilnehmers geschaltet werden. Wird das Gespräch in der hier eingegebenen Zeit nicht angenommen, wird wieder die Vermittlung gerufen. Möglich sind Werte von *10* bis *600*. Der Standardwert ist *30*.
Offene Rückfrage	Geben Sie die Zeit ein, nach der eine offene Rückfrage beendet wird und der Teilnehmer wieder angerufen oder bei ihm angeklopft wird. Sie führen ein Gespräch und möchten dieses zu einem Kollegen vermitteln. Leider wissen Sie nicht, wo dieser Kollege sich zur Zeit aufhält. Mit **Offene Rückfrage** wird der Gesprächspartner im Wartefeld des Systems gehalten. Sie können nun von Ihrem Telefon eine Durchsage durchführen, in der Sie Ihren Kollegen auf das wartende Gespräch hinweisen. Durch eine Kennzif-

Feld	Wert
	fer der offenen Rückfrage kann der Kollege das Gespräch an einem beliebigen Telefon annehmen. Wird ein im Wartefeld wartendes Gespräch nicht innerhalb der hier eingegebenen Zeit wieder von einem Teilnehmer angenommen, erfolgt ein Wiederanruf oder Anklopfen beim einleitenden Teilnehmer. Möglich sind Werte von *10* bis *600*. Der Standardwert ist *30*.

11.2.5 Systemlizenzen

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

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

Mögliche Werte für Status

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

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

11.2.5.1 Bearbeiten oder Neu

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

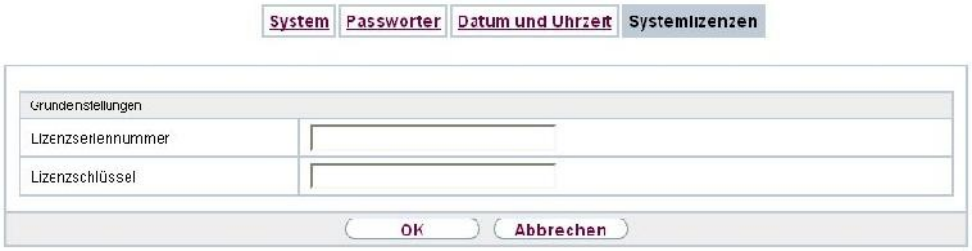


Abb. 35: **Systemverwaltung**->**Globale Einstellungen**->**Systemlizenzen**->**Neu**

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

Felder im Menü Grundeinstellungen

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

11.3 Kennziffern

Im Geschäftsalltag haben Sie zur Bedienung bestimmter Leistungsmerkmale Kennziffern genutzt, die Sie mit Ihrem neuen System weiterhin verwenden möchten. Jedoch sind in der Grundeinstellung für diese Leistungsmerkmale andere Kennziffern eingestellt. Kein Problem - für einzelne Leistungsmerkmale können Sie die Kennziffern individuell erweitern. So können Sie auch in Zukunft diese Leistungsmerkmale mit den bisher gewohnten Kennziffern bedienen.

11.3.1 Änderbare Kennziffern

Im Menü **Änderbare Kennziffern** konfigurieren Sie den Kennziffernplan des Systems.

Für einige Leistungsmerkmale können in der Konfiguration des Systems die Kennziffern individuell eingestellt werden. Dabei wird die voreingestellte Kennziffer des Systems durch eine Rufnummer aus dem internen Rufnummernplan des Systems ergänzt. Für die Leistungsmerkmale **Offene Rückfrage** und **Bündel** können mehrere Kennziffern vergeben werden. Die Bedienung der Leistungsmerkmale mit geänderter Kennziffer erfolgt, wie für das entsprechende Leistungsmerkmal beschrieben. Sie können wahlweise die geänderte Kennziffer (interne Rufnummer) oder die in der Bedienungsanleitung beschriebene Kenn-

ziffer nutzen (außer Amtskennziffer).

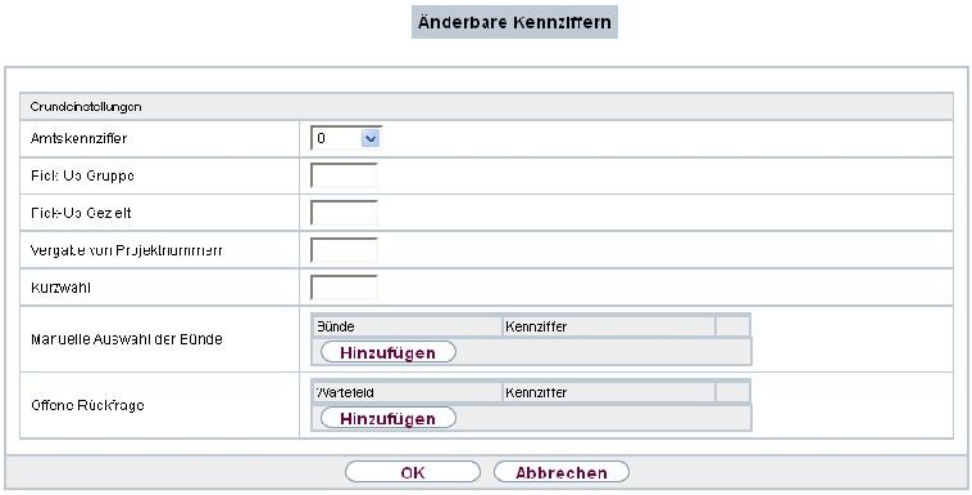


Abb. 36: **Systemverwaltung->Kennziffern->Änderbare Kennziffern**

Das Menü **Systemverwaltung->Kennziffern->Änderbare Kennziffern** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Amtskennziffer	Wählen Sie die Amtskennziffer aus. Mögliche Werte: • *Keine* • *0* (Standardwert) • *6* • *7* • *8* • *9*
Pick-Up Gruppe	Geben Sie die neue Kennziffer für das Leistungsmerkmal **Pick-Up (Gruppe)** ein.
Pick-Up Gezielt	Geben Sie die neue Kennziffer für das Leistungsmerkmal **Pick-Up (Interner Teilnehmer)** ein.
Vergabe von Projekt-	Geben Sie die neue Kennziffer für das Leistungsmerkmal **Ver-**

Feld	Beschreibung
nummern	**gabe von Projektnummern** ein.
Kurzwahl	Geben Sie die neue Kennziffer für das Leistungsmerkmal **Kurzwahl** ein.
Manuelle Auswahl der Bündel	Legen Sie die neuen Kennziffern für das Leistungsmerkmal **Manuelle Auswahl der Bündel** an. Legen Sie dafür zunächst durch Klicken von **Hinzufügen** eine Bündelauswahl an, wählen Sie das Bündel aus und geben Sie die gewünschte Kennziffer für das Bündel ein.
Offene Rückfrage	Legen Sie die neuen Kennziffern für das Leistungsmerkmal **Offene Rückfrage** an. Legen Sie dafür zunächst durch Klicken von **Hinzufügen** ein Wartefeld, in dem der Anrufer gehalten werden soll, an und geben Sie die gewünschte Kennziffer für das Wartefeld ein. Sie können maximal 10 Einträge anlegen.

11.4 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

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

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

Konventionen für die Port-/Schnittstellennamen

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

(a) WLAN

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

Beispiel: *WLAN1*

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

(a) ETH

(b) Nummer des Ports

Beispiel: *ETH1*

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

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

(b) Nummer des Ethernet-Ports

(c) Nummer der Schnittstelle

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

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

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

(b) Nummer der Bridge-Gruppe

Beispiel: *br0* (erste Bridge-Gruppe)

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

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

(b) Nummer des Funkmoduls

(c) Nummer der Schnittstelle

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

Der Name des WDS-Links bzw. Bridge-Links setzt sich aus den folgenden Bestandteilen zusammen:

(a) Abkürzung für den Schnittstellentyp

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

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

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

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

(a) Abkürzung für den Schnittstellentyp

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

(c) Nummer des Client-Links

Beispiel: `sta1-0` (erster Client-Link auf dem ersten Funkmodul)

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

(a) Abkürzung für den Schnittstellentyp

(b) Nummer des Ethernet-Ports

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

(d) Nummer der virtuellen Schnittstelle

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

11.4.1 Schnittstellen

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

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

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

Abb. 37: **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-Gruppe	Wählen Sie aus, ob Sie die Schnittstelle im *Routing-Modus* betreiben möchten oder ordnen die Schnittstelle einer bestehenden (*br0*, *br1* usw.) oder neuen Bridge-Gruppe (*Neue Bridge-Gruppe*) zu. Bei Auswahl von *Neue Bridge-Gruppe* wird nach Anklicken des **OK**-Buttons automatisch eine neue Bridge-Gruppe erzeugt.
Konfigurationsschnittstelle	Wählen Sie aus, über welche Schnittstelle die Konfiguration durchgeführt wird. Mögliche Werte: • *Eine auswählen* (Standardwert): Einstellung im Auslieferungszustand. Die richtige Konfigurationsschnittstelle muss aus den anderen Optionen ausgewählt werden. • *Nicht beachten*: Keine Schnittstelle wird als Konfigurationsschnittstelle definiert. • *<Schnittstellenname>*: Legen Sie die Schnittstelle fest, die zur Konfiguration benutzt wird. Wenn diese Schnittstelle Mitglied einer Bridge-Gruppe ist, übernimmt sie deren IP-Adresse, wenn sie aus der Bridge-Gruppe herausgenommen wird.

11.4.1.1 Hinzufügen

Hinzufügen

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

Abb. 38: **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**->**Hinzufügen**

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

Felder im Menü Schnittstellen

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

Bearbeiten für Geräte der WIxxxxn und RS-Serie

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

Abb. 39: **Systemverwaltung**->**Schnittstellenmodus / Bridge-Gruppen**->**Schnittstellen**->

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

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

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

(3) Wählen Sie das Menü **Systemverwaltung**->**Schnittstellenmodus /**

->**Schnittstellen**. Die zusätzliche Schnittstelle **sta1-0** wird angezeigt.

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

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

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

Felder im Menü Layer 2.5-Optionen

Feld	Wert
Schnittstelle	Zeigt die Schnittstelle an, die gerade bearbeitet wird.
Wildcard-Modus	Wählen Sie aus, welchen Wilrdcard-Modus Sie auf der Schnittstelle nutzen wollen. Mögliche Werte: • *Keiner* (Standardwert): Es wird kein Wildcard-Modus verwendet. • *statisch*: Mit dieser Einstellung müssen Sie bei **Wildcard-MAC-Adresse** die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist. Jedes Paket ohne IP und ohne ARP wird an dieses Gerät weitergereicht. Dieses Vorgehen wird auch dann beibehalten, wenn das entsprechende Gerät nicht mehr angeschlossen ist. • *zuerst*: Mit dieser Einstellung wird die MAC-Adresse des ersten Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame, der an irgendeiner der Ethernet-Schnittstellen ankommt, als Wildcard-MAC-Adresse benutzt. Diese Wildcard-MAC-Adresse kann nur durch einen Neustart des Geräts oder die Auswahl eines anderen Wildcard-Modus zurückgesetzt werden. • *letzte*: Mit dieser Einstellung wird die eigene WLAN-MAC-Adresse benutzt, um die Verbindung zum Access Point herzustellen. Sobald ein Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame auftaucht, wird er an diejenige MAC-Adresse weitergeleitet, von welcher der letzte Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame bei einer Ethernet-Schnittstelle des Geräts eingetroffen ist. Diese Wildcard-MAC-Adresse wird mit jedem Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame erneuert.

Feld	Wert
Wildcard-MAC-Adresse	Nur für **Wildcard-Modus** = *statisch* Geben Sie die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist.
Transparente MAC-Adresse	Nur für **Wildcard-Modus** = *statisch*, *zuerst* Wählen Sie aus, ob die **Wildcard-MAC-Adresse** zusätzlich als WLAN-MAC-Adresse benutzt werden, um damit die Verbindung zum Access Point herzustellen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

11.5 Administrativer Zugriff

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

11.5.1 Zugriff

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

Abb. 40: **Systemverwaltung**->**Administrativer Zugriff**->**Zugriff**

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

Nur für Telefonanlagen: Weiterhin können Sie Ihr Gerät für Wartungsarbeiten durch den

bintec elmeg-Kundenservice freischalten. Hierzu aktivieren Sie je nach angeforderter Service-Leistung die Option **Service Login (ISDN Web-Access)** oder **Service Call Ticket (SSH Web-Access)** und wählen die Schaltfläche **OK**. Folgen Sie den Anweisungen des bintec elmeg-Kundenservice!

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

Felder im Menü Erweiterte Einstellungen

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

11.5.1.1 Hinzufügen

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

Abb. 41: **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.

11.5.2 SSH

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

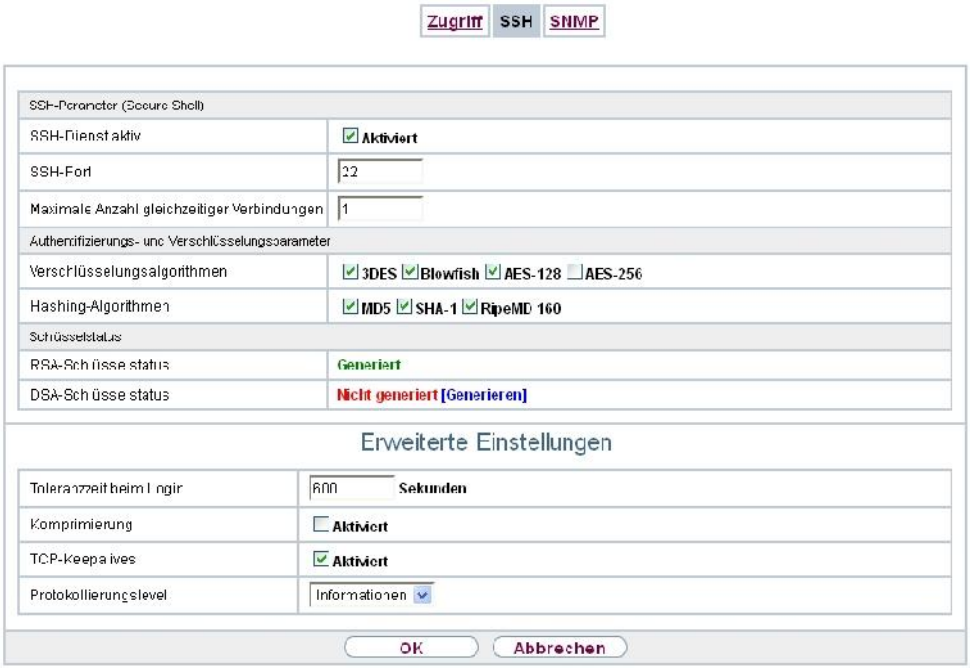


Abb. 42: **Systemverwaltung->Administrativer Zugriff->SSH**

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

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

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

Hinweis

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

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

Felder im Menü SSH-Parameter (Secure Shell)

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

Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

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

Felder im Menü Schlüsselstatus

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Wert
Toleranzzeit beim Login	Geben Sie die Zeit (in Sekunden) ein, die für den Verbindungsaufbau zur Verfügung steht. Wenn ein Client innerhalb dieser Zeit nicht erfolgreich authentifiziert werden kann, wird die Verbindung getrennt.

Feld	Wert
	Standardwert ist *600* Sekunden.
Komprimierung	Wählen Sie aus, ob Datenkompression verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-Keepalives	Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Protokollierungslevel	Wählen Sie den Syslog-Level für die vom SSH Daemon generierten Syslog-Messages aus. Zur Verfügung stehen: • *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.

11.5.3 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. 43: **Systemverwaltung->Administrativer Zugriff->SNMP**

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

Felder im Menü Grundeinstellungen

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

Tipp

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

11.6 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

11.6.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete

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

Pakettypen

Feld	Wert
ACCESS_REQUEST	Client -> Server Wenn ein Verbindungs-Request auf Ihrem Gerät empfangen wird, wird beim RADIUS-Server angefragt, falls in Ihrem Gerät kein entsprechender Verbindungspartner gefunden wurde.

Feld	Wert
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.

11.6.1.1 Bearbeiten oder Neu

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

Abb. 44: **Systemverwaltung->Remote Authentifizierung->RADIUS->Neu**

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

Felder im Menü Basisparameter

Feld	Wert
Authentifizierungstyp	Wählen Sie aus, wofür der RADIUS-Server verwendet werden soll. Mögliche Werte: • *PPP-Authentifizierung* (Standardwert, nur für PPP-Verbindungen): Der RADIUS-Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. • *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 kon-

Feld	Wert
	trollieren. • *IPSec-Authentifizierung*: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln. • *WLAN (802.1x)*: Der RADIUS-Server wird verwendet, um den Zugang zu einem Drahtlosnetzwerk zu regeln. • *XAUTH*: Der RADIUS-Server wird verwendet, um IPSec-Peers über XAuth zu authentisieren.
Betreibermodus	Nur für **Authentifizierungstyp** = *Accounting* Wählen Sie in Hotspot-Anwendungen den Modus aus, der vom Anbieter definiert ist. In Standardanwendungen belassen Sie den Wert bei *Standard*. Mögliche Werte für Hotspot-Anwendungen: • *France Telecom*: Für Hotspot-Anwendungen der France Telecom. • *bintec HotSpot Server*: Für Hotspot-Anwendungen.
Server-IP-Adresse	Geben Sie die IP-Adresse des RADIUS-Servers ein.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein.
Standard-Benutzerpasswort	Einige RADIUS-Server benötigen für jede RADIUS-Anfrage ein Benutzerpasswort. Geben Sie daher das Passwort hier ein, das Ihr Gerät als Standard-Benutzerpasswort in der Anfrage für die Dialout-Routen an den RADIUS-Server mitsendet.
Priorität	Wenn mehrere RADIUS-Server-Einträge angelegt wurden, wird der Server mit der obersten Priorität als erstes verwendet. Wenn dieser Server nicht antwortet, wird der Server mit der nächstniedrigeren Priorität verwendet usw. Mögliche Werte von *0* (höchste Priorität) bis *7* (niedrigste Priorität). Standardwert ist *0*. Siehe auch **Richtlinie** in den erweiterten 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. • *Standardgruppe 0*: Wählen Sie diesen Eintrag für spezielle Anwendungen, wie z. B. Hotspot-Server-Konfiguration, aus. • *<Gruppenname>*: Wählen Sie aus der Liste eine schon definierte Gruppe aus.

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

Felder im Menü Erweiterte Einstellungen

Feld	Wert
Richtlinie	Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht. Mögliche Werte: • *Verbindlich* (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. • *Nicht verbindlich*: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS-Server wird angefragt, bis Ihr Gerät eine Antwort von einem als autoritativ konfigurierten Server erhält.
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 erneuter Erreichbarkeit wird der **Status** wieder auf *aktiv* gesetzt. Wenn der RADIUS-Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit *inaktiv* ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Wiederholungen	Geben Sie die Anzahl der Wiederholungen für den Fall ein, dass eine Anfrage nicht beantwortet wird. Falls nach diesen Versuchen dennoch keine Antwort erhalten wurde, wird der **Status** auf *inaktiv* gesetzt. bei **Erreichbarkeitsprüfung** = *Aktiviert* versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird **Status** wieder auf *aktiv* zurückgesetzt. 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*.

Feld	Wert
RADIUS-Dialout	Nur für **Authentifizierungstyp** = *PPP-Authentifizierung* und *IPSec-Authentifizierung*. Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion aktiv ist, können Sie folgende Optionen eingeben: • *Neulade-Intervall*: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. Standardmäßig ist hier *0* eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.

11.6.2 TACACS+

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

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

Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:

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

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

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

11.6.2.1 Bearbeiten oder Neu

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

Abb. 45: **Systemverwaltung->Remote Authentifizierung->TACACS+ ->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Authentifizierungstyp	Zeigt an, welche TACACS+-Funktion genutzt werden soll. Der Wert kann nicht verändert werden. Mögliche Werte: • *Login-Authentifizierung*: Hier können Sie festlegen, ob der aktuelle TACACS+-Server für die Login-Authentifizierung zu Ihrem Gerät benutzt werden soll.
Server-IP-Adresse	Geben Sie die IP-Adresse des TACACS+-Servers ein, der für eine Login-Authentifizierung abgefragt werden soll.

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Richtlinie	Wählen Sie die Interpretation der TACACS+-Antwort aus. Mögliche Werte: • *Nicht verbindlich* (Standardwert): Die TACACS+-Server werden gemäß ihrer Priorität (siehe **Priorität**) abgefragt, bis eine positive Antwort oder von einem authoritativen Server eine negative Antwort empfangen wurde. • *Verbindlich*: Eine negative Antwort auf eine Anfrage wird akzeptiert, d. h. es wird kein weiterer TACACS+-Server abgefragt. Die Geräte-interne Benutzerverwaltung wird durch TACACS+ nicht ausgeschaltet. Sie wird geprüft, nachdem alle TACACS+Server abgefragt wurden.
TCP-Port	Zeigt den für das TACACS+-Protokoll verwendeten Standard-

Feld	Beschreibung
	TCP-Port (*49*) an. Der Wert kann nicht verändert werden.
Timeout	Geben Sie die Zeit in Sekunden ein, die der NAS auf eine Antwort von TACACS+ warten soll. Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+-Server abgefragt (nur für **Richtlinie** = *Nicht verbindlich*) und der aktuelle Server in einen *blockiert*-Status versetzt. Mögliche Werte sind *1* bis *60*, der Standardwert ist *3*.
Blockzeit	Geben Sie die Zeit in Sekunden ein, die der aktuelle Server in einem blockierten Status verbleiben soll. Nach Ende der Blockierung wird der Server in den Status versetzt, der im Feld **Eintrag aktiv** angegeben ist. Mögliche Werte sind *0* bis *3600*, der Standardwert ist *60*. Der Wert *0* bedeutet, dass der Server nie in einen *blockiert*-Status versetzt wird und somit keine weiteren Server angefragt werden.
Verschlüsselung	Wählen Sie aus, ob der Datenaustausch zwischen dem TACACS+-Server und dem NAS mit MD5 verschlüsselt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Ist die Funktion nicht aktiv, werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung sondern nur für Debug-Zwecke empfohlen.

11.6.3 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. 46: **Systemverwaltung->Remote Authentifizierung->Optionen**

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

Felder im Menü Globale RADIUS-Optionen

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

11.7 Konfigurationszugriff

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

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

11.7.1 Zugriffsprofile

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

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

Abb. 47: **Systemverwaltung**->**Konfigurationszugriff**->**Zugriffsprofile**

11.7.1.1 Bearbeiten oder Neu

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

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

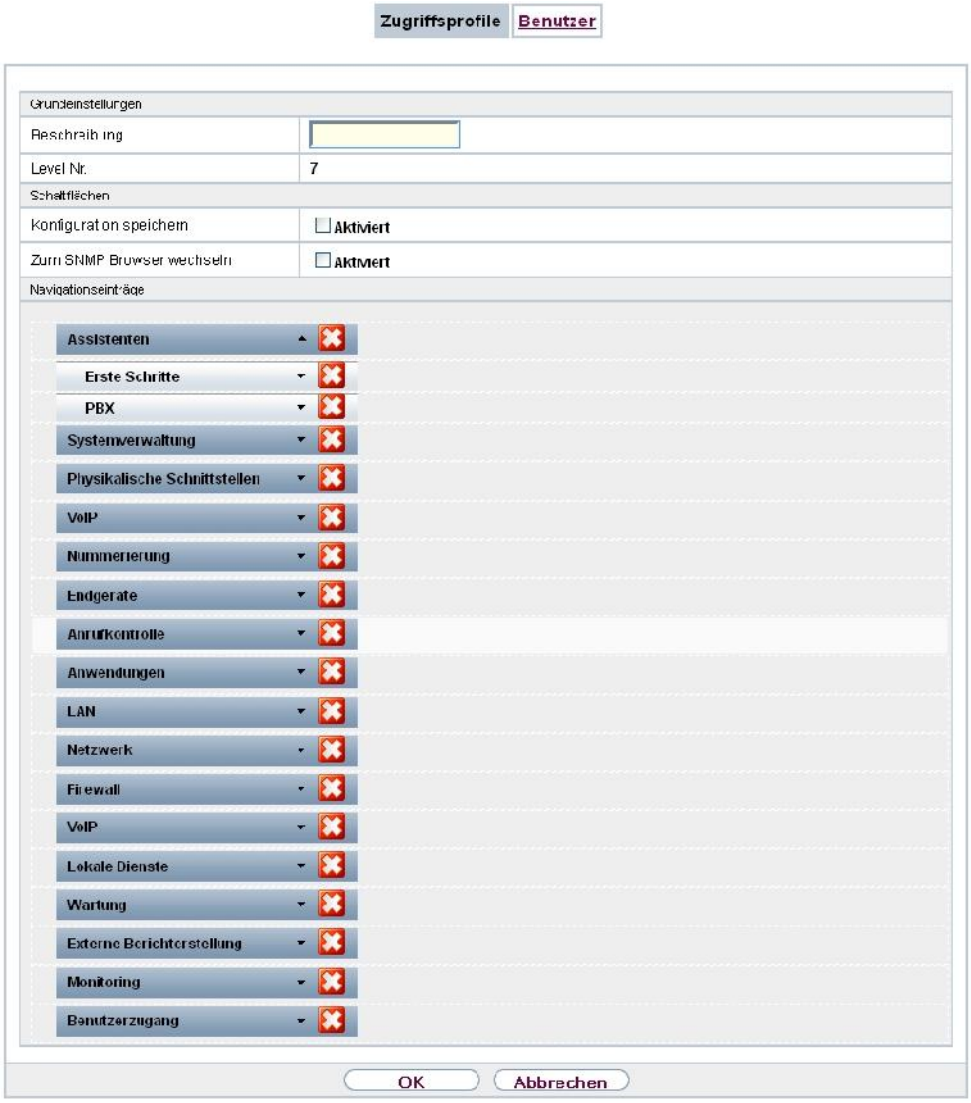


Abb. 48: **Systemverwaltung->Konfigurationszugriff->Zugriffsprofile->Neu**

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

Felder im Menü Grundeinstellungen

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

Feld	Beschreibung
	Zugriffsprofil. Diese kann nicht editiert werden.

Felder im Menü Schaltflächen

Feld	Beschreibung
Konfiguration speichern	Wenn Sie die Schaltfläche **Konfiguration speichern** aktivieren, darf der Benutzer Konfigurationen speichern.  **Hinweis** Beachten Sie, dass die Passwörter in der gespeicherten Datei im Klartext eingesehen werden können. Aktivieren oder deaktivieren Sie **Konfiguration speichern**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zum SNMP Browser wechseln	Wenn Sie die Schaltfläche **Zum SNMP Browser wechseln** aktivieren, kann der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und alle dort angezeigten Einstellungen ändern.  **Achtung** Beachten Sie, dass die Berechtigung für **Zum SNMP Browser wechseln** bedeutet, dass der Benutzer auf die gesamte MIB zugreifen kann, da in dieser Ansicht kein individuelles Zugangsprofil angelegt werden kann. Mit der Berechtigung für **Konfiguration speichern** kann er die geänderte MIB speichern. Mit der Berechtigung für **Zum SNMP Browser wechseln** heben Sie die konfigurierten GUI- Einschränkungen auf der MIB-Ebene wieder auf. Aktivieren oder deaktivieren Sie **Zum SNMP Browser wechseln**. Mit *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Navigationseinträge

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

11.7.2 Benutzer

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

Abb. 49: **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer**

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

Abb. 50: **Systemverwaltung**->**Konfigurationszugriff**->**Benutzer**->

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

11.7.2.1 Bearbeiten oder Neu

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

Abb. 51: **Systemverwaltung->Konfigurationszugriff->Benutzer->Neu**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Benutzer	Geben Sie eine eindeutige Bezeichnung für den Benutzer ein.
Passwort	Geben Sie ein Passwort für den Benutzer ein.
Benutzer muss das Passwort ändern	Mit der Option **Benutzer muss das Passwort ändern** kann der Administrator bestimmen, dass der Benutzer beim ersten Login ein eigenes Passwort vergeben muss. Dazu muss die Option **Konfiguration speichern** im Menü **Zugriffsprofile** aktiv sein. Ist diese Option nicht aktiv, so wird ein Warnhinweis angezeigt. Aktivieren oder deaktivieren Sie **Benutzer muss das Passwort ändern**. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zugangs-Level	Mit **Hinzufügen** weisen Sie dem Benutzer mindestens ein Zugriffsprofil zu. Mit der Auswahl von **Nur lesen** wird festgelegt, dass der Benutzer die Parameter des Zugriffsprofils ansehen, aber nicht ändern kann. Die Auswahl **Nur lesen** ist nur möglich, wenn die Option **Zum SNMP Browser wechseln** im Menü **Zugriffsprofile** nicht aktiv ist. Ist die Option **Zum SNMP Browser wechseln** aktiv, so wird ein Warnhinweis angezeigt, weil der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und beliebi-

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

11.8 Zertifikate

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

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

Ein digitales Zertifikat bestätigt u. a. die Echtheit und den Eigentümer eines öffentlichen Schlüssels. Es ist vergleichbar mit einem amtlichen Ausweis, in dem bestätigt wird, dass der Eigentümer des Ausweises bestimmte Merkmale aufweist, wie z. B. das angegebene Geschlecht und Alter, und dass die Unterschrift auf dem Ausweis echt ist. Da es für Zertifikate nicht nur eine einzige Ausgabestelle gibt, wie z. B. das Passamt für einen Ausweis, sondern Zertifikate von vielen verschiedenen Stellen und in unterschiedlicher Qualität ausgegeben werden, kommt der Vertrauenswürdigkeit der Ausgabestelle eine zentrale Bedeutung zu. Die Qualität eines Zertifikats regelt das deutsche Signaturgesetz bzw. die entsprechende EU-Richtlinie.

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

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

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

Ihr Gerät ist für die Verwendung von Zertifikaten für VPN-Verbindungen und für Sprachver-

bindungen über Voice over IP ausgestattet.

11.8.1 Zertifikatsliste

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

11.8.1.1 Bearbeiten

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

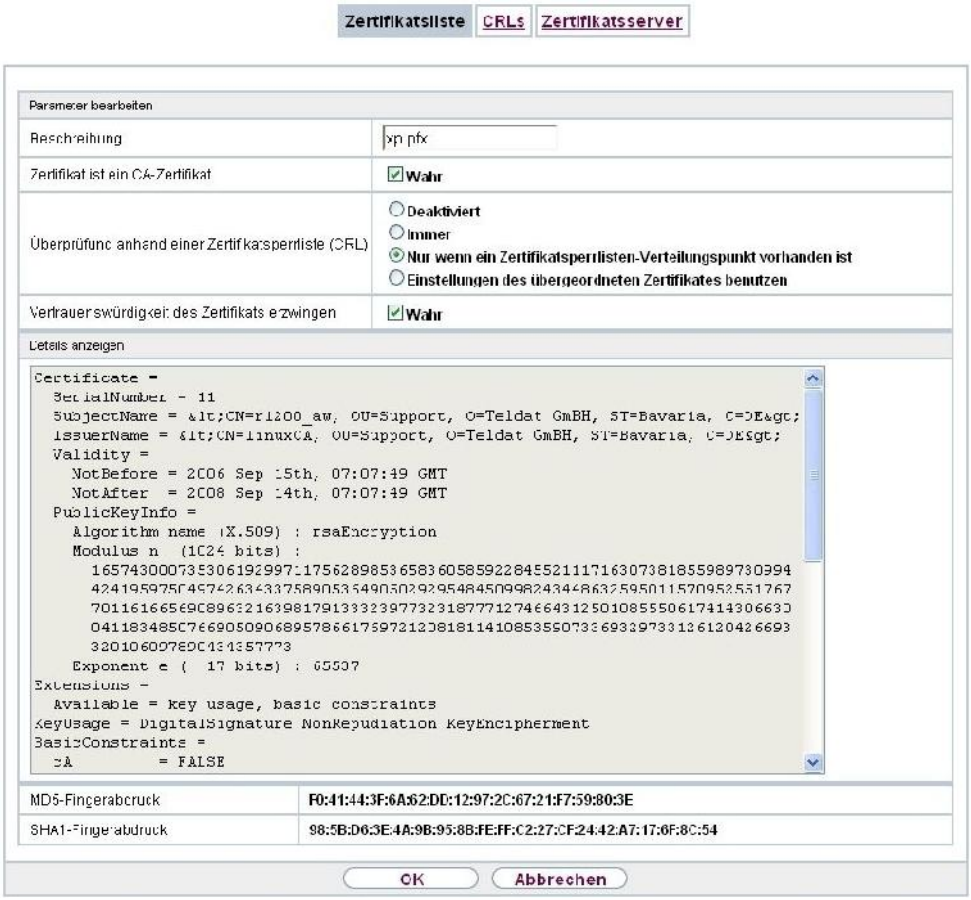


Abb. 52: **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste**->

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

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

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

Felder im Menü Parameter bearbeiten

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.
Zertifikat ist ein CA-Zertifikat	Markieren Sie das Zertifikat als Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA). Zertifikate, die von dieser CA ausgestellt wurden, werden bei der Authentifizierung akzeptiert. Mit *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Überprüfung anhand einer Zertifikatsperrliste (CRL)	Nur für **Zertifikat ist ein CA-Zertifikat** = *Wahr* Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen. Mögliche Einstellungen: • *Deaktiviert*: keine Überprüfung von CRLs. • *Immer*: CRLs werden grundsätzlich überprüft. • *Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist* (Standardwert): Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden. • *Einstellungen des übergeordneten Zertifikates benutzen*: Es werden die Einstellungen des übergeordneten Zertifikates verwendet, falls eines vorhanden ist. Falls nicht, wird genauso verfahren, wie unter "Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist" beschrieben.
Vertrauenswürdigkeit des Zertifikats erzwingen	Legen Sie fest, dass dieses Zertifikat ohne weitere Überprüfung bei der Authentifizierung als Benutzerzertifikat akzeptiert werden soll.

Feld	Beschreibung
	Mit *Wahr* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Achtung

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

11.8.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

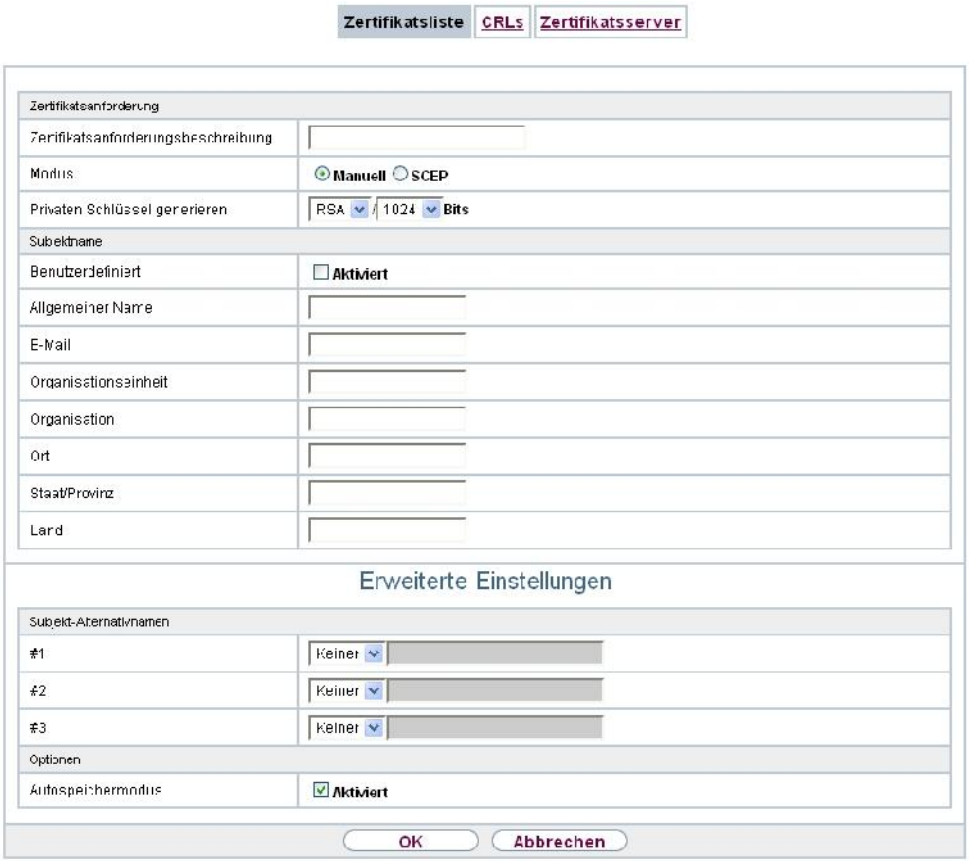


Abb. 53: **Systemverwaltung->Zertifikate->Zertifikatsliste->Zertifikatsanforderung**

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

Felder im Menü Zertifikatsanforderung

Feld	Beschreibung
Zertifikatsanforderungsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Modus	Wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen. Zur Verfügung stehen: • `Manuell` (Standardwert): Ihr Gerät erzeugt für den Schlüssel eine PKCS#10-Datei, die direkt im Browser hochgeladen oder

Feld	Beschreibung
	im -Menü über das Feld **Details anzeigen** kopiert werden kann. Diese Datei muss der CA zugestellt und das erhaltene Zertifikat anschließend manuell auf Ihr Gerät importiert werden. • *SCEP*: Der Schlüssel wird mittels des Simple Certificate Enrollment Protocols bei einer CA beantragt.
Privaten Schlüssel generieren	Nur für **Modus** = *Manuell* Wählen Sie einen Algorithmus für die Schlüsselerstellung aus. Zur Verfügung stehen *RSA* (Standardwert) und *DSA*. Wählen Sie weiterhin die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte: *512*, *768*, *1024*, *1536*, *2048*, *4096*. Beachten Sie, dass ein Schlüssel mit der Länge 512 Bit als unsicher eingestuft werden könnte, während ein Schlüssel mit 4096 Bit nicht nur viel Zeit zur Erzeugung erfordert, sondern während der IPSec-Verarbeitung einen wesentlichen Teil der Ressourcen belegt. Ein Wert von 768 oder mehr wird jedoch empfohlen, als Standardwert ist 1024 Bit vorgegeben.
SCEP-URL	Nur für **Modus** = *SCEP* Geben Sie die URL des SCEP-Servers ein, z. B. http://scep.beispiel.com:8080/scep/scep.dll Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
CA-Zertifikat	Nur für **Modus** = *SCEP* Wählen Sie das CA-Zertifikat aus. • *-- Download --*: Geben Sie in **CA-Name** den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. *cawindows*. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator. Falls keine CA-Zertifikate zur Verfügung stehen, wird Ihr Gerät zuerst das CA-Zertifikat der betroffenen CA herunterladen.

Feld	Beschreibung
	Es fährt dann mit dem Registrierungsprozess fort, sofern keine wesentlichen Parameter mehr fehlen. In diesem Fall kehrt es in das Menü **Zertifikatsanforderung generieren** zurück. Falls das CA-Zertifikat keine CRL-Verteilstelle (Certificate Revocation List, CRL) enthält und auf Ihrem Gerät kein Zertifikatsserver konfiguriert ist, werden Zertifikate von dieser CA nicht auf ihre Gültigkeit überprüft. • <Name eines vorhandenen Zertifikats>: Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, wählen Sie diese manuell aus.
RA-Signierungszertifikat	Nur für **Modus** = *SCEP* Nur für **CA-Zertifikat** nicht = *-- Download --* Wählen Sie ein Zertifikat für die Signierung der SCEP-Kommunikation aus. 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 Subjektname

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

Feld	Beschreibung
Land	Nur für **Benutzerdefiniert** = deaktiviert. Geben Sie das Land laut CA ein.

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

Felder im Menü Subjekt-Alternativnamen

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

Feld im Menü Optionen

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

11.8.1.3 Importieren

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

Abb. 54: **Systemverwaltung->Zertifikate->Zertifikatsliste->Importieren**

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

Felder im Menü Importieren

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen des Zertifikats ein, welches importiert werden soll oder wählen Sie die Datei mit **Durchsuchen...** über den Dateibrowser aus.
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät das Zertifikat dekodieren kann. Mögliche Werte: • `Auto` (Standardwert): Aktiviert die automatische Kodiererkennung. Falls der Zertifikat-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung. • `Base64` • `Binär`
Passwort	Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort.

Feld	Beschreibung
	Tragen Sie das Passwort hier ein.

11.8.2 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.

11.8.2.1 Importieren

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

Abb. 55: **Systemverwaltung**->**Zertifikate**->**CRLs**->**Importieren**

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

Felder im Menü CRL-Import

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen der CRL ein, welche importiert werden soll oder wählen Sie die Datei mit **Durchsuchen...** über den Dateibrowser aus.

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

11.8.3 Zertifikatsserver

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

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

11.8.3.1 Neu

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

Abb. 56: **Systemverwaltung**->**Zertifikate**->**Zertifikatsserver**->**Neu**

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

Felder im Menü Basisparameter

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

Kapitel 12 Physikalische Schnittstellen

12.1 Ethernet-Ports

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

Die Ethernet-Ports **ETH1** bis **ETH4** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle *en1-0* ist zugewiesen und mit **IP-Adresse** *192.168.0.250* und **Netzmaske** *255.255.255.0* vorkonfiguriert.

Hinweis

Um die Erreichbarkeit Ihres Systems zu gewährleisten, achten Sie beim Aufteilen der Ports darauf, dass die Ethernet-Schnittstelle *en1-0* mit der vorkonfigurierten IP-Adresse und Netzmaske einem Port zugewiesen wird, der per Ethernet erreichbar ist. Führen Sie im Zweifelsfall die Konfiguration per serieller Verbindung über die Schnittstelle **Serial 1** durch.

ETH1 - ETH4

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

VLANs für Routing-Schnittstellen

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

12.1.1 Portkonfiguration

Portseparation

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

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

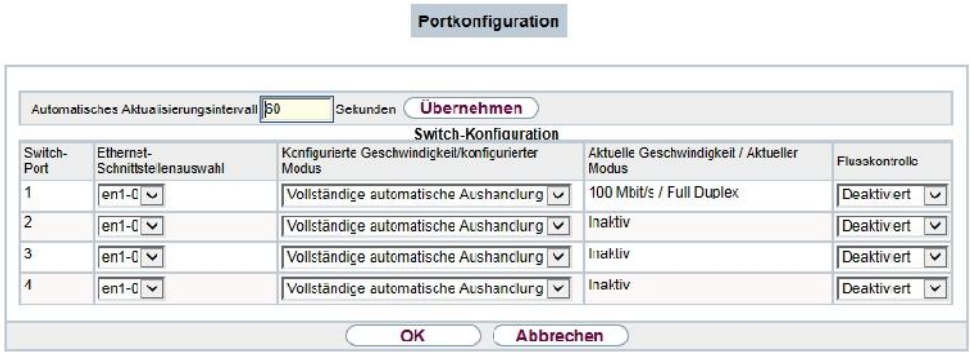


Abb. 57: **Physikalische Schnittstellen->Ethernet-Ports->Portkonfiguration**

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

Felder im Menü Switch-Konfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Ethernet-Schnittstellenauswahl	Ordnen Sie dem jeweiligen Switch-Port eine logische Ethernet-Schnittstelle zu. Zur Auswahl stehen vier Schnittstellen, `en1-0` bis `en1-3`. In der Grundeinstellung ist Switch Port **1**-**4** die Schnittstelle `en1-0` zugeordnet.
Konfigurierte Geschwindigkeit/konfigu-	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll.

Feld	Beschreibung
rierter Modus	Mögliche Werte: • *Vollständige automatische Aushandlung* (Standardwert) • *Auto 1000 Mbit/s only* • *Auto 100 Mbit/s only* • *Auto 10 Mbit/s only* • *Auto 100 Mbit/s / Full Duplex* • *Auto 100 Mbit/s / Half Duplex* • *Auto 10 Mbit/s / Full Duplex* • *Auto 10 Mbit/s / Half Duplex* • *Fest 1000 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Full Duplex* • *Fest 100 Mbit/s / Half Duplex* • *Fest 10 Mbit/s / Full Duplex* • *Fest 10 Mbit/s / Half Duplex* • *Keiner* : Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit deadminr Schnittstelle an. Mögliche Werte: • *1000 Mbit/s / Full Duplex* • *100 Mbit/s / Full Duplex* • *100 Mbit/s / Half Duplex* • *10 Mbit/s / Full Duplex* • *10 Mbit/s / Half Duplex* • *Inaktiv*
Flusskontrolle	Wählen Sie aus, ob auf der entsprechenden Schnittstelle eine Flusskontrolle vorgenommen werden soll. Mögliche Werte: • *Deaktiviert* (Standardwert): Es wird keine Flusskontrolle vorgenommen. • *Aktiviert*: Es wird eine Flusskontrolle durchgeführt.

Feld	Beschreibung
	• *Auto*: Es wird eine automatische Flusskontrolle durchgeführt.

12.2 ISDN-Ports

Die ISDN-Anschlüsse des Systems können wahlweise als interne oder externe ISDN-Anschlüsse konfiguriert werden. Die externen ISDN-Anschlüsse dienen zur Anschaltung an das ISDN-Netz des Netzbetreibers. Die internen ISDN-Anschlüsse sind zur Anschaltung verschiedener ISDN-Endgeräte (Systemtelefone, ISDN-Telefone, ...) vorgesehen.

12.2.1 ISDN Extern

Im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN Extern** konfigurieren Sie die externen ISDN-Anschlüsse Ihres Systems.

Die Anschlussart eines externen ISDN-Anschlusses ist zwischen Mehrgeräteanschluss (P-MP) und Anlagenanschluss (P-P) einstellbar.

Beim Anschluss an mehrere ISDN-Anschlüsse sind folgende Varianten möglich:

- Alle externen ISDN-Anschlüsse sind nur Mehrgeräteanschlüsse (P-MP).
- Alle externen ISDN-Anschlüsse sind nur Anlagenanschlüsse (P-P).
- Die externen ISDN-Anschlüsse sind Mehrgeräteanschlüsse (P-MP) und Anlagenanschlüsse (P-P).

12.2.1.1 Bearbeiten mit

Wählen Sie die Schaltfläche , um einen Eintrag zu bearbeiten.

Abb. 58: **Physikalische Schnittstellen->ISDN-Ports->ISDN Extern->**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine benutzerdefinierte Beschreibung der ISDN-Schnittstelle an. Der Standardwert ist *ISDN Extern*.
Name	Zeigt die Bezeichnung der ISDN-Schnittstelle an. Mögliche Werte: • *S/U*: 4-Draht (S) • */*: Zeigt den Port auf dem Modul an, an den die ISDN-Schnittstelle angeschlossen ist. Beispiel: *S/U 1* = Die Schnittstelle befindet sich in Port 1 und wird als S-Anschluss genutzt.
Anschlussart	Wählen Sie aus, ob die ISDN-Schnittstelle als Mehrgeräteanschluss oder als Anlagenanschluss betrieben wird. Mögliche Werte: • *Anlagenanschluss* (Standardwert) • *Mehrgeräteanschluss*

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Schicht 2 daueraktiv halten	Mit dieser Funktion (auch Dauerüberwachung genannt) wird die Funktionsfähigkeit und die Übertragungsqualität eines externen ISDN-Anschlusses ständig überwacht. Hierfür steht das System ständig mit der Vermittlungsstelle Ihres Netzbetreibers in Kontakt. Wird die ISDN-Schicht 2 nicht von der Vermittlungsstelle daueraktiv gehalten, kann das System den immer wiederkehrenden Aufbau der Schicht 2 initiieren. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Schicht 1 Dauersynchronisation	Beim Anschalten eines externen Gerätes (z. B. GSM-Gateway) an einen externen Anlagenanschluss des Systems kann der Takt des externen Gerätes zu Störungen der Synchonisierung des Anlagentaktes führen. Nur wenn eine solche Störung auftritt, sollten Sie die Schicht 1 Synchronisierung ausschalten. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

12.2.2 ISDN Intern

Im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN Intern** konfigurieren Sie die internen ISDN-Schnittstellen Ihres Systems.

Interne ISDN-Anschlüsse sind immer Mehrgeräteanschlüsse.

Beim Anschluss von Endgeräten an einen internen ISDN-Anschluss beachten Sie bitte, dass nicht alle im Handel angebotenen ISDN-Endgeräte die vom System bereitgestellten Leistungsmerkmale über ihre Tastenoberfläche nutzen können.

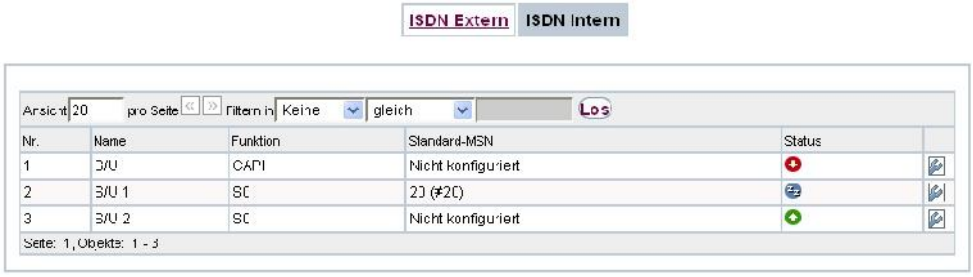


Abb. 59: **Physikalische Schnittstellen->ISDN-Ports->ISDN Intern**

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

Felder im Menü ISDN Intern

Feld	Beschreibung
Name	Zeigt die Bezeichnung der ISDN-Schnittstelle an. Mögliche Werte: • *S/U*: 4-Draht (S) • */*: Zeigt den Port auf dem Modul an, an den die ISDN-Schnittstelle angeschlossen ist. Beispiel: *S/U 2* = Die Schnittstelle befindet sich in Port 2 und wird als S-Anschluss genutzt.
Funktion	Zeigt die Funktion der ISDN-Schnittstelle an. Mögliche Werte: • *Upn*: Schnittstelle für CAPI-Endgeräte. • *Upn*: Schnittstelle für UPN-Endgeräte. • *S0*: Schnittstelle für ISDN-S0-Anschluss.
Standard-MSN	Zeigt, ob für einen internen S0-Bus eine Standard-MSN zugewiesen ist. Über eine Standard-MSN können Sie nicht konfigurierte S0-Endgeräte erreichen. Als Standard-MSN können Sie interne Rufnummern wählen, die im Menü **Nummerierung->Benutzereinstellungen->Benutzer** konfiguriert sind und im Menü **Endgeräte** einem Endgerät zuge-

Feld	Beschreibung
	ordnet sind.
Status	Zeigt den Status der Schnittstelle an.

12.2.2.1 Bearbeiten

Wählen Sie die Schaltfläche , um einen Eintrag zu bearbeiten.

Abb. 60: **Physikalische Schnittstellen->ISDN-Ports->ISDN Intern->**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Standard-MSN	Wählen Sie die gewünschte Rufnummer. Sie können unter den Rufnummern wählen, die Sie im Menü **Nummerierung->Benutzereinstellungen->Benutzer->Rufnummern** konfiguriert haben. Mögliche Werte: • *Nicht konfiguriert* • *<Rufnummer>*

12.3 Analoge Ports

12.3.1 Analog Extern (FXO)

Im Menü **Analog Extern (FXO)** werden alle verfügbaren analogen externen Anschlüsse Ihres Systems angezeigt.

Abb. 61: **Physikalische Schnittstellen->Analoge Ports->Analog Extern (FXO)**

Das Menü **Physikalische Schnittstellen->Analoge Ports->Analog Extern (FXO)** besteht aus folgenden Feldern:

Werte in der Liste Analog Extern (FXO)

Feld	Beschreibung
Name	Zeigt die Bezeichnung der analogen Schnittstelle an. Mögliche Werte: • *FXO*: Bezeichung für den analogen Anschluss.
Beschreibung	Zeigt die benutzerdefinierte Beschreibung der analogen Schnittstelle an.
Wahlverfahren	Zeigt das verwendete Wahlverfahren an. Mögliche Werte: • *Frequenzwahlverfahren (DTMF)* (Standardwert) • *Impulswahlverfahren (IWV)*
Status	Zeigt den Status der Schnittstelle an.
Aktion	Durch Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert.

12.3.1.1 Bearbeiten

Wählen Sie die Schaltfläche , um einen Eintrag zu bearbeiten.

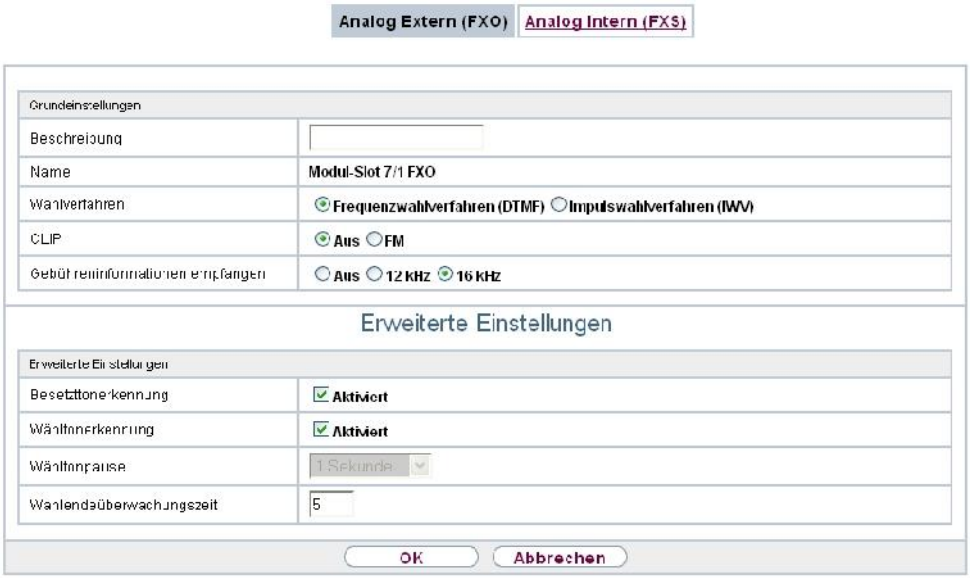


Abb. 62: **Physikalische Schnittstellen->Analoge Ports->Analog Extern (FXO)->**

Das Menü **Physikalische Schnittstellen->Analoge Ports->Analog Extern (FXO)->** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine benutzerdefinierte Beschreibung der analogen Schnittstelle an.
Name	Zeigt die Bezeichnung der analogen Schnittstelle an. Mögliche Werte: • *FXO*: Bezeichung für den analogen Anschluss.
Wahlverfahren	Wählen Sie, welches Wahlverfahren verwendet werden soll. Mögliche Werte: • *Frequenzwahlverfahren (DTMF)* (Standardwert) • *Impulswahlverfahren (IWV)*
CLIP	Wählen Sie aus, ob das Leistungsmerkmal CLIP verwendet werden soll, d. h. ob die Rufnummer des Anrufers beim Angerufenen angezeigt werden soll.

Feld	Beschreibung
	Mögliche Werte: • *Aus* (Standardwert): Die Rufnummer des Anrufers wird beim Angerufenen nicht angezeigt. • *FM*: Die Daten werden als DTMF gesendet.
Gebühreninformationen empfangen	Wählen Sie aus, ob Ihr Gerät Gebühreninformationen aus dem Netz empfangen soll. Hierfür können Sie einstellen, ob der Gebührenimpuls 12 kHz oder 16 kHz betragen soll. Mögliche Werte: • *Aus* (Standardwert): Gebühreninformationen werden nicht empfangen. • *12 kHz* • *16 kHz*

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Besetztttonerkennung	Wählen Sie, ob **Besetztttonerkennung** verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Wähltonerkennung	Wählen Sie, ob **Wähltonerkennung** verwendet werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn die **Wähltonerkennung** aktiv ist und der externe Wählton erkannt wurde, beginnt Ihre **hybird 120** / **hybird 130** sofort mit der Wahl.
Wähltonpause	Nur für **Wähltonerkennung** deaktiviert. Geben Sie den gewünschten Wert ein, den das System beim Wählen einer Telefonnummer maximal warten soll, bis es mit der Wahl beginnt. Die **Wähltonpause** können Sie einschalten, wenn die **hybird 120** / **hybird 130** den externen Wählton nicht erkennt oder kein

Feld	Beschreibung
	Wählton gesendet wird. Die Dauer der **Wähltonpause** müssen Sie ermitteln. Mögliche Werte sind ganzzahlige Werte zwischen `1` Sekunde und `5` Sekunden.
Wahlendeüberwachungszeit	Geben Sie die Zeit ein, die das System nach dem Wählen einer Ziffer warten soll, bis es die Telefonnummer als vollständig betrachtet und die Verbindung aufbaut. Der Standardwert ist `5` Sekunden.

12.3.2 Analog Intern (FXS)

Im Menü **Analog Intern (FXS)** werden alle verfügbaren analogen internen Anschlüsse Ihres Systems angezeigt.

Abb. 63: **Physikalische Schnittstellen->Analoge Ports->Analog Intern (FXS)**

Das Menü **Physikalische Schnittstellen->Analoge Ports->Analog Intern (FXS)** besteht aus folgenden Feldern:

Werte in der Liste Analog Intern (FXS)

Feld	Beschreibung
Name	Zeigt die Bezeichnung der analogen Schnittstelle an. Mögliche Werte: • `FXS`: Bezeichung für den analogen Anschluss.
Funktion	Zeigt die Funktion der analogen Schnittstelle an. Mögliche Werte:

Feld	Beschreibung
	• *Telefon* • *TFE-Adapter* • *Multifunktionsgerät/Telefax* • *Modem* • *Anrufbeantworter* • *Notfalltelefon* Die Funktion des analogen Endgeräts wird im Menü **Endgeräte**->**Andere Telefone**->**analog** konfiguriert.
Status	Zeigt den Status der Schnittstelle an.

12.4 DSL-Modem

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

12.4.1 DSL-Konfiguration

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

Abb. 64: **Physikalische Schnittstellen**->**DSL-Modem**->**DSL-Konfiguration**

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

Felder im Menü DSL-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* • *ADSL2 Annex J* • *ADSL2+ Annex J*

Felder im Menü Aktuelle 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 DSL Parameter

Feld	Beschreibung
DSL-Modus	Wählen Sie den ADSL-Synchronisierungstyp aus. 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. • *Automatischer Modus (Annex-M)*: Nur für Annex-A-Geräte. Der ADSL-Modus wird dem der Gegenstelle automatisch angepasst unter Einbeziehung von G.992.3 Annex-M. • *ADSL2 Plus (Annex-M)*: Nur für Annex-A-Geräte. ADSL2 Plus / G.992.3 Annex-M wird angewendet. • *ADSL2 Annex J*: Nur für Annex-J-Geräte. ADSL2 Plus / G.992.3 Annex-J wird angewendet. • *ADSL2+ Annex J*: Nur für Annex-J-Geräte. ADSL2 Plus / G.992.5 Annex-J 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)* (Standardwert): Die Datenrate in Senderichtung wird nicht reduziert. • *128.000 Bit/s* bis *2.048.000 Bit/s*: Die Datenrate in Senderichtung wird reduziert auf maximal 128.000 bit/s bis 2.048.000 bit/s in festgesetzten Schritten. • *Benutzerdefiniert*: Die Datenrate wird reduziert auf den in **Maximale Upstream-Bandbreite** eingegebenen Wert. Der Standardwert ist *Standard (Leitungsgeschwindigkeit)*.

Feld	Beschreibung
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 Erweiterte Einstellungen

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

12.5 Relais

Die **hybird 130** verfügt über einen unabhängigen Schaltkontakt.

Ein Schaltkontakt kann als Ein-/Ausschalter oder als Taster konfiguriert werden. Über eine Kennziffer kann dann die entsprechende Funktion von intern oder extern (mit zusätzlicher PIN) geschaltet werden.

Hinweis

Bei Reset oder Stromausfall der TK-Anlage wird der Schaltkontakt in seine Ruheposition zurückgesetzt!

12.5.1 Relaiskonfiguration

Im Menü **Physikalische Schnittstellen**->**Relais**->**Relaiskonfiguration** wird die Konfiguration des Schaltkontakts vorgenommen.

Abb. 65: **Physikalische Schnittstellen->Relais->Relaiskonfiguration**

Das Menü **Physikalische Schnittstellen->Relais->Relaiskonfiguration** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Kontakt 1	Geben Sie bei **Beschreibung** eine beliebige Bezeichnung des Schaltkontakts ein. Jedem Schaltkontakt kann nur eine Funktion zugewiesen werden. Bei **Funktion** wählen Sie die Art der Verwendung aus. Mögliche Werte: • *Kennziffern*: Das Relais wird über eine Kennziffernprozedur geschaltet. • *Meldeausgang*: Das Relais wird geschaltet, wenn ein Alarmruf eingeht. Bei **Signalisierungszeitraum** stellen Sie die Zeitdauer für das Relais ein. Die Schaltzeit kann zwischen 1 und 999 Sekunden programmiert werden. Der Standardwert ist *3* Sekunden.

Kapitel 13 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.

13.1 Einstellungen

Im Menü **VoIP**->**Einstellungen** richten Sie Ihre VoIP-Anschlüsse ein.

Sie haben die Möglichkeit mit allen intern angeschlossenen Telefonen über das Internet zu telefonieren. Die Anzahl der Verbindungen ist von verschiedenen Parametern abhängig:

- Der Verfügbarkeit von freien Kanälen des Systems.
- Der verfügbaren Bandbreite des DSL-Anschlusses.
- Den konfigurierten, verfügbaren SIP-Providern.
- Die eingetragenen SIP-out-Lizenzen.

13.1.1 SIP-Provider

Im Menü **VoIP**->**Einstellungen**->**SIP-Provider** konfigurieren Sie die gewünschten SIP-Provider.

Durch Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status des SIP-Providers geändert.

Nach etwa einer Minute ist die Registrierung beim Provider erfolgt und der Status wird automatisch auf (aktiv) gesetzt.

13.1.1.1 Bearbeiten oder Neu

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

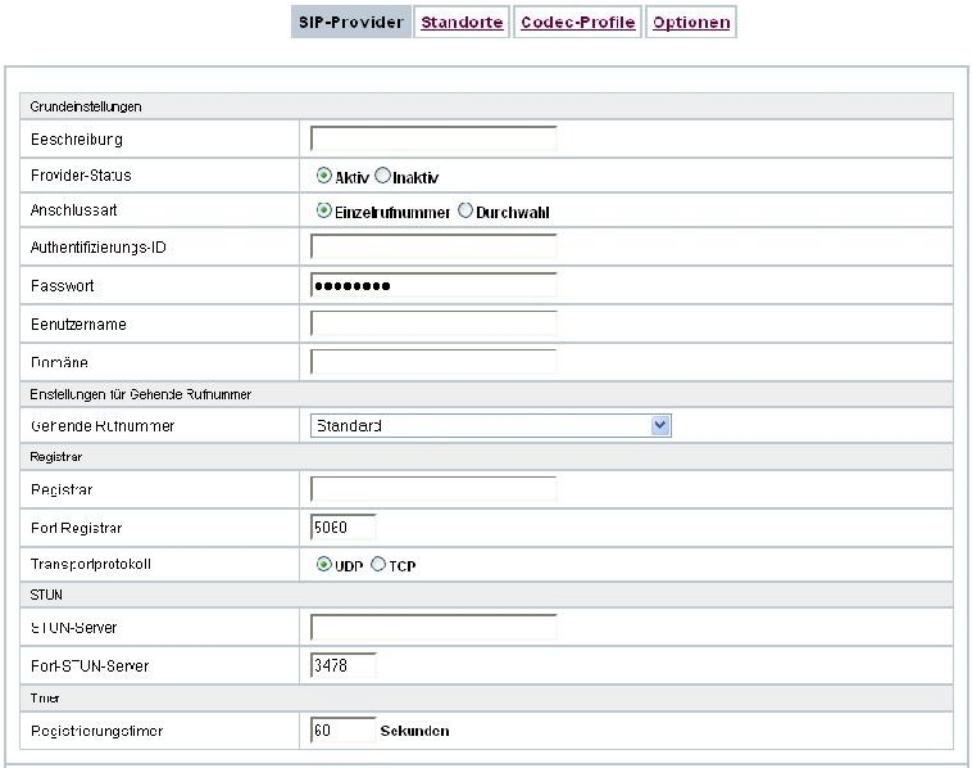


Abb. 66: **VoIP**->**Einstellungen**->**SIP-Provider**->**Neu**

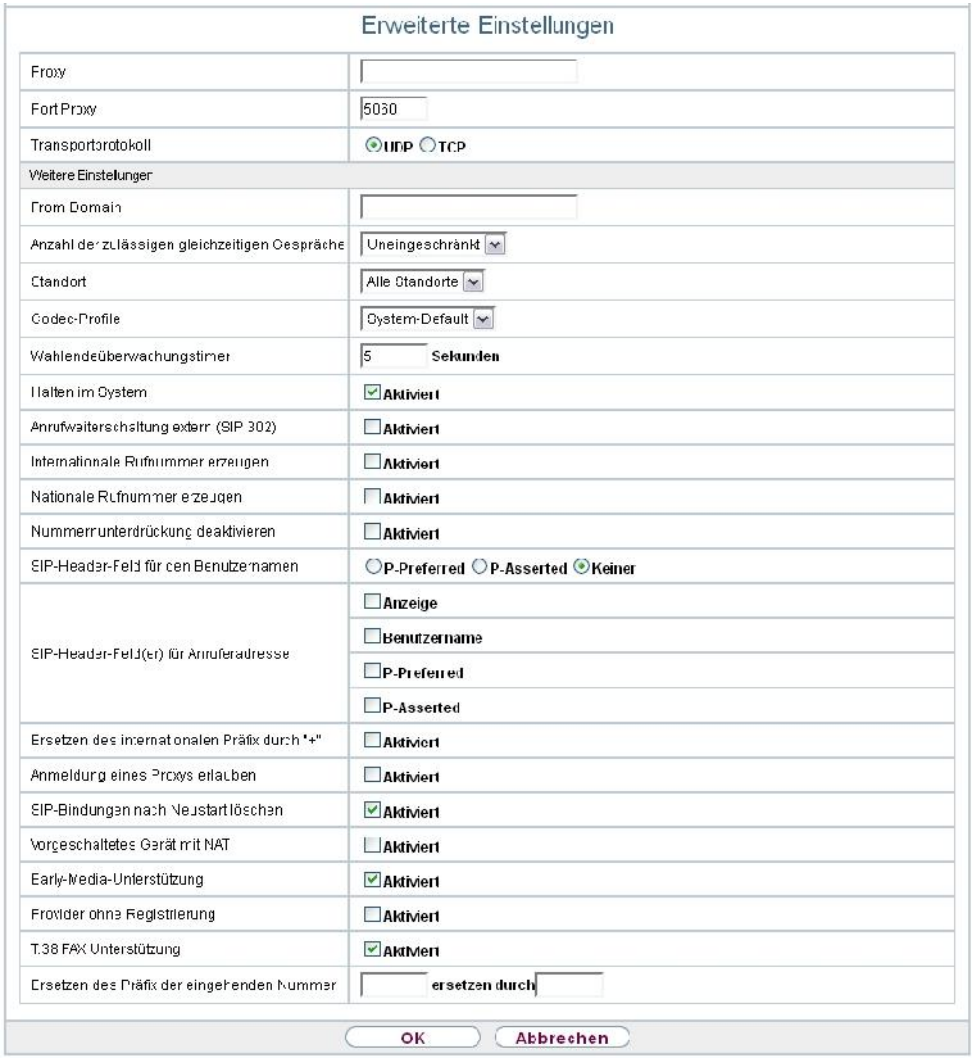


Abb. 67: **VoIP**->**Einstellungen**->**SIP-Provider**->**Neu**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Sie können eine Bezeichnung für den SIP-Provider eingeben. Möglich ist eine 20-stellige alphanumerische Zeichenfolge.
Provider-Status	Wählen Sie aus, ob dieser VoIP-Provider-Eintrag aktiv sein soll (*Aktiv*, Standardwert) oder nicht (*Inaktiv*).

Feld	Beschreibung
Anschlussart	Wählen Sie aus, welche Art von VoIP-Rufnummer Sie konfigurieren möchten. Mögliche Werte: • *Einzelrufnummer* (Standardwert): Geben Sie einzelne VoIP-Rufnummern ein. • *Durchwahl*: Geben Sie eine Basisnummer in Verbindung mit einem Rufnummernblock an.
Authentifizierungs-ID	Geben Sie die Authentifizierungs-ID Ihres Providers ein. Möglich ist eine 64-stellige alphanumerische Zeichenfolge.
Passwort	Sie können an dieser Stelle ein Passwort vergeben. Möglich ist eine 32-stellige alphanumerische Zeichenfolge.
Benutzername	Geben Sie den Benutzernamen ein, den Sie von Ihrem VoIP-Provider erhalten haben. Möglich ist eine 64-stellige alphanumerische Zeichenfolge.
Domäne	Tragen Sie einen weiteren Domänennamen oder eine weitere IP-Adresse des SIP-Proxy-Servers ein. Wenn Sie keine Angaben machen, wird der Eintrag im Feld **Registrar** verwendet. Beachte: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dieser explizit vom Provider vorgegeben wird.

Felder im Menü Einstellungen für Gehende Rufnummer

Feld	Beschreibung
Gehende Rufnummer	Wählen Sie die gewünschte Signalisierung für Rufe nach außen aus. Mögliche Werte: • *Standard* (Standardwert) • *Globale Rufnummer für CLIP-No-Screening* • *Individuelle Rufnummer für CLIP-No-Screening* • *Feste DDI nach Extern* (Nur für **Anschlussart** = *Durchwahl*)

Feld	Beschreibung
Globale Rufnummer für CLIP-No-Screening	Nur für **Gehende Rufnummer** *Globale Rufnummer für CLIP-No-Screening* Geben Sie die Rufnummer ein, die bei allen Verbindungen nach extern beim Angerufenen angezeigt werden soll. Diese Rufnummer wird nicht überprüft.
Rufnummer des entfernten Gesprächspartners anzeigen	Nur für **Gehende Rufnummer** = *Globale Rufnummer für CLIP-No-Screening* und *Individuelle Rufnummer für CLIP-No-Screening* Sie können die Rufnummer eines externen Gesprächspartners anzeigen lassen, sofern diese signalisiert wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Feste Rufnummer für ausgehende Gespräche anzeigen	Nur für **Gehende Rufnummer** = *Feste DDI nach Extern* Geben Sie die Rufnummer ein, die bei allen Verbindungen nach extern beim Angerufenen angezeigt werden soll.

Felder im Menü Registrar

Feld	Beschreibung
Registrar	Geben Sie den DNS-Namen oder die IP-Adresse des SIP-Servers an. Möglich ist eine 26-stellige alphanumerische Zeichenfolge.
Port Registrar	Geben Sie die Nummer des Ports ein, der für die Verbindung zum Server benutzt werden soll. Standardmäßig ist der Wert *5060* vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.
Transportprotokoll	Wählen Sie das Transportprotokoll für die Verbindung aus. Mögliche Werte: • *UDP* (Standardwert) • *TCP*

Felder im Menü STUN

Feld	Beschreibung
STUN-Server	Geben Sie den Namen oder die IP-Adresse des STUN-Servers ein. STUN = Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) Ein STUN-Server wird benötigt, um VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Internet zu ermöglichen. Hierbei wird die aktuelle öffentliche IP-Adresse des Anschlusses ermittelt und für eine genaue Adressierung von außen verwendet. Maximale Zeichenzahl: 32.
Port-STUN-Server	Geben Sie Nummer des Ports ein, der für die Verbindung zum STUN-Server benutzt werden soll. Standardmäßig ist der Wert *3478* vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.

Felder im Menü Timer

Feld	Beschreibung
Registrierungstimer	Geben Sie hier die Zeitdauer in Sekunden ein, vor deren Ablauf sich der SIP-Client erneut registrieren muss, damit die Verbindung nicht automatisch getrennt wird. Standardmäßig ist der Wert *60* vorgegeben.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Proxy	Geben Sie den DNS-Namen oder die IP-Adresse des SIP-Servers an. Möglich ist eine 26-stellige alphanumerische Zeichenfolge.
Port Proxy	Geben Sie Nummer des Ports ein, der für die Verbindung zum Proxy benutzt werden soll. Standardmäßig ist der Wert *5060* vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.
Transportprotokoll	Wählen Sie das Transportprotokoll für die Verbindung aus. Mögliche Werte:

Feld	Beschreibung
	• *UDP* (Standardwert) • *TCP*

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
From Domain	Geben Sie die „From Domain“ Ihres SIP-Providers ein. Diese wird nach dem @ als Absendeinformation im SIP-Header der SIP-Datenpakete verwendet.
Anzahl der zulässigen gleichzeitigen Gespräche	Wählen Sie die maximale Anzahl von Gesprächen aus, die gleichzeitig möglich sein sollten. Beachten Sie hier auch die Einstellungen des Bandbreitenmanagements. Mögliche Werte: • *International* (Standardwert): Es sind unbegrenzt gleichzeitige Gespräche möglich. • *1* • *2* • *3* • *4* • *5* • *10*
Standort	Wählen Sie den Standort des SIP-Servers aus. Standorte werden im Menü **VoIP**->**Einstellungen**->**Standorte** definiert. Mögliche Werte: • *Alle Standorte* (Standardwert): Der Server wird an keinem definierten Standort betrieben. • *<Standort-Name>*
Codec-Profile	Wählen Sie das Codec-Profil für diesen SIP-Server aus. Codec-Profile werden im Menü **VoIP**->**Einstellungen**->**Codec-Profile** definiert. Mögliche Werte: • *System-Default* (Standardwert): Der Server wird mit einem im System vordefinierten Codec-Profil betrieben.

Feld	Beschreibung
	• *<Codec-Profil-Name>*
Wahlendeüberwachungstimer	Wählen Sie die Zeit (nach Wahl der letzten Ziffer einer Rufnummer) in Sekunden aus, nach der das System mit der Wahl nach extern beginnt. Standardwert ist *5*.
Halten im System	Wählen Sie aus, ob ein Telefongespräch im System auf Wartestellung geschaltet werden kann, ohne die Verbindung zu verlieren (Rückfragen/Makeln). Ist diese Funktion nicht aktiv, wird der Anruf beim SIP-Provider gehalten, sofern dieser dieses Leistungsmerkmal unterstützt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Anrufweiterschaltung extern (SIP 302)	Wählen Sie aus, ob eine Anrufumleitung extern beim SIP-Provider durchgeführt wird. Der Anrufer wird mittels SIP-Status-Code 302 weitergeschaltet. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Internationale Rufnummer erzeugen	Wenn Sie diese Funktion aktivieren und unter **Globale Einstellungen** die **Ländereinstellung** (für Deutschland *49*) eingetragen haben, wird automatisch bei einer mit Vorwahl gewählten Rufnummer die 0049 vor der Rufnummer erzeugt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Nationale Rufnummer erzeugen	Wenn Sie diese Funktion einschalten und unter **Globale Einstellungen** den **Nationaler Präfix/Ortsnetzkennzahl** (für z. B. Hamburg *40*) eingetragen haben, wird automatisch die Vorwahl 040 vor der gewählten Rufnummer erzeugt. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Nummernunterdrückung deaktivieren	Wenn Sie diese Funktion aktivieren, wird die Rufnummer immer mitgesendet unabhängig davon, ob Sie bei einem Teilnehmer **A-Rufnummer unterdrücken (CLIR)** ein- oder ausgeschaltet

Feld	Beschreibung
	haben. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
SIP-Header-Feld für den Benutzernamen	Wählen Sie für ausgehende Rufe die Position des Benutzernamens (User ID) im SIP-Header. Mögliche Werte: • *P-Preferred*: Der SIP-Header wird durch das sogenannte „p-preferred-identity“-Feld erweitert, um dort den **Benutzernamen** zu übertragen. • *P-Asserted*: Der SIP-Header wird durch das sogenannte „p-asserted-identity“-Feld erweitert, um dort den **Benutzernamen** zu übertragen. • *Keiner*: Der **Benutzername** wird nicht übertragen.
SIP-Header-Feld(er) für Anruferadresse	Wählen Sie für ausgehende Rufe die Position der Absender-ID (z. B. Rufnummer) im SIP-Header aus. (Bei eingehenden Rufen wird automatisch die Rufnummer aus dem SIP Header ermittelt.) Mögliche Werte: • *Anzeige*: Die Absender-ID wird im SIP-Header im Feld „Display“ übertragen. • *Benutzername*: Die Absender-ID wird im SIP-Header im Feld „User“ übertragen. • *P-Preferred*: Der SIP-Header wird durch das sogenannte „p-preferred-identity“ Feld erweitert, um dort die Absender-ID zu übertragen. • *P-Asserted*: Der SIP-Header wird durch das sogenannte „p-asserted-identity“ Feld erweitert, um dort die Absender-ID zu übertragen.
Ersetzen des internationalen Präfix durch "+"	Wählen Sie aus, ob bei internationalen Rufnummern der Präfix (z. B. 00) durch + ersetzt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
Anmeldung eines Proxys erlauben	Wählen Sie aus, ob eine weitere TK-Anlage sich bei Ihrem System registrieren kann. Dadurch können mehrere TK-Systeme miteinander gekoppelt werden. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
SIP-Bindungen nach Neustart löschen	Sollte z. B. nach der Registrierung bei einem Provider ein Reset des Systems erfolgen oder ein Netzausfall eintreten, kann je nach Provider eine weitere Registrierung nicht mehr möglich sein. Durch Einschalten dieses Leistungsmerkmals, wird eine erneute Registrierung nach Neustart ermöglicht. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Vorgeschaltetes Gerät mit NAT	Wenn Sie diese Funktion aktivieren, können Sie ein vorgeschaltetes Gerät mit NAT nutzen und trotzdem mit VoIP telefonieren. Ohne diese Funktion könnten Sie bei Nutzung eines vorgeschalteten Geräts mit NAT über VoIP nicht angerufen werden. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Early-Media-Unterstützung	Wählen Sie aus, ob Sie den Austausch von Sprach- oder Audiodaten erlauben wollen, bevor ein Empfänger einen Anruf annimmt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Provider ohne Registrierung	Wählen Sie, ob die Registrierung und Authentifizierung bei einem Provider entfallen kann. In diesem Fall werden die relevanten Daten an eine bestimmte IP-Adresse geschickt, die den Verbindungspartnern bereits bekannt ist. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
	Ist die Funktion nicht aktiv, wird standardmäßig eine authentisierung vorgenommen. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen Registrar-Server. Diese Information über den Benutzer und seine aktuelle Adresse wird vom Registrar auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.
T.38 FAX Unterstützung	Nur für modulare Telefonanlagen Wählen Sie, ob Sie FAX-Dokumente per Voice over IP mit dem Standard T.38 übertragen wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Wenn die Funktion deaktiviert ist, werden Fax-Dokumente mit G.711 übertragen.
Ersetzen des Präfix der eingehenden Nummer	Soll bei kommenden Anrufen die Rufnummer verändert im System weitergegeben werden, geben Sie in das erste Eingabefeld die Zahlenfolge der kommenden Rufnummer ein, die durch die im zweiten Eingabefeld eingetragene Zahlenfolge ersetzt werden soll.

13.1.2 Standorte

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

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

Abb. 68: **VoIP->Einstellungen->Standorte**

Felder im Menü Registrierungsverhalten für VoIP-Teilnehmer ohne definierten Standort

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

13.1.2.1 Bearbeiten oder Neu

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

Abb. 69: **VoIP**->**Einstellungen**->**Standorte**->**Neu**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie die Beschreibung des Eintrags ein.
Beinhalteter Standort (Parent)	Sie können die SIP-Standorte beliebig kaskadieren. Definieren Sie hier, welcher schon definierte SIP-Standort für den hier zu konfigurierenden SIP-Standort den übergeordneten Knoten bildet.
Typ	Wählen Sie aus, ob der Standort mittels IP-Adressen/DNS-Namen oder Schnittstellen definiert werden soll. Mögliche Werte: • *Adressen* (Standardwert): Der SIP-Standort wird über IP-Adressen bzw. DNS-Namen definiert. • *Schnittstellen*: Der SIP-Standort wird über die verfügbaren Schnittstellen definiert.
Adressen	Nur für **Typ** = *Adressen* Geben Sie die IP-Adressen der Geräte an den SIP-Standorten ein.

Feld	Beschreibung
	Klicken Sie auf **Hinzufügen** um neue Adressen zu konfigurieren. Geben Sie unter **IP-Adresse/DNS-Name** die gewünschte IP-Adresse bzw. den DNS-Namen ein. Geben Sie ebenfalls die erforderliche **Netzmaske** ein.
Schnittstellen	Nur für **Typ** = *Schnittstellen* Geben Sie die Schnittstellen an, an denen die Geräte eines SIP-Standorts angeschlossen sind. Klicken Sie auf **Hinzufügen**, um neue Schnittstelle auszuwählen. Wählen Sie unter **Schnittstelle** die gewünschte Schnittstelle aus.
Bandbreitenbegrenzung Upstream	Legen Sie fest, ob die Upstream-Bandbreite begrenzt werden soll. Mit *Aktiviert* wird die Bandbreite reduziert. Standardmäßig ist die Funktion nicht aktiv.
Maximale Upstream-Bandbreite	Geben Sie die maximale Datenrate in Senderichtung in kBits pro Sekunde ein.
Bandbreitenbegrenzung Downstream	Legen Sie fest, ob die Downstream-Bandbreite begrenzt werden soll. Mit *Aktiviert* wird die Bandbreite reduziert. Standardmäßig ist die Funktion nicht aktiv.
Maximale Downstream-Bandbreite	Geben Sie die maximale Datenrate in Empfangsrichtung in kBits pro Sekunde ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
DSCP-Einstellungen	Wählen Sie die Art des Dienstes für RTP-Daten aus (TOS, Type

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

13.1.3 Codec-Profile

Im Menü **VoIP**->**Einstellungen**->**Codec-Profile** können Sie verschiedene Codec-Profile definieren, um die Sprachqualität zu beeinflussen und bestimmte Provider-abhängige Vorgaben einzurichten.

Beachten Sie bei der Einrichtung der Codecs, dass eine gute Sprachqualität eine entsprechende Bandbreite benötigt und damit die Anzahl der gleichzeitigen Gespräche begrenzt wird. Außerdem muss die Gegenstelle die entsprechende Codec-Auswahl mit unterstützen.

13.1.3.1 Bearbeiten oder Neu

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

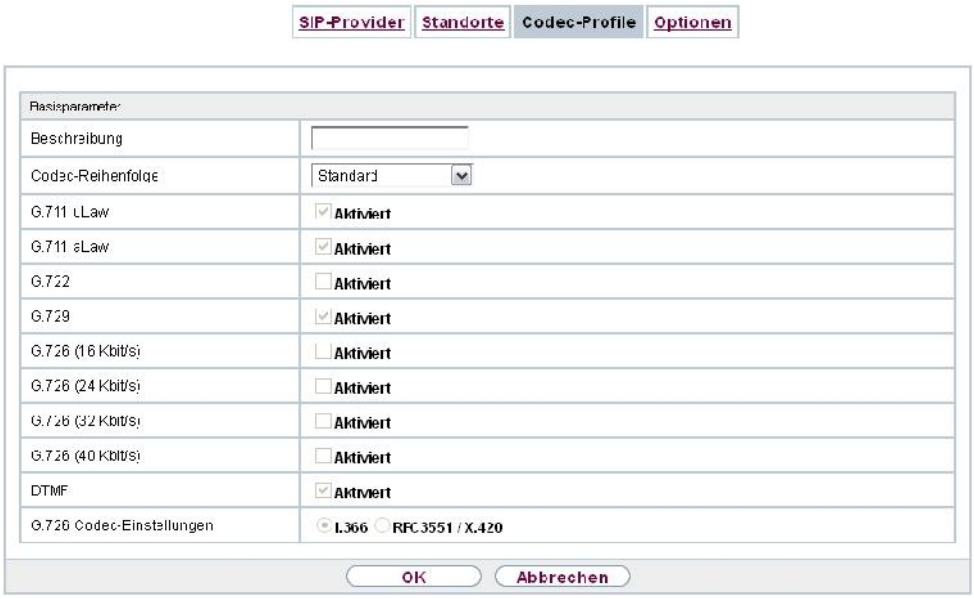


Abb. 70: **VoIP**->**Einstellungen**->**Codec-Profile**->**Neu**

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	te benötigt, wird verwendet, wenn möglich.
G.711 uLaw	Nur für **Codec-Reihenfolge** nicht `Standard` ISDN-Codec nach US-Kennlinie. G.711 uLaw erfasst den Frequenzbereich von 300 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,4. Dieser Audio-Codec verwendet das µlaw-Quantisierungsverfahren.
G.711 aLaw	Nur für **Codec-Reihenfolge** nicht `Standard` ISDN-Codec nach EU-Kennlinie G.711 aLaw erfasst den Frequenzbereich von 300 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,4. Dieser Audio-Codec verwendet das alaw-Quantisierungsverfahren.
G.722	Nur für **Codec-Reihenfolge** nicht `Standard` G.722 erfasst den Frequenzbereich von 50 Hz bis 7000 Hz mit einer Abtastrate von 16 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,5.
G.729	Nur für **Codec-Reihenfolge** nicht `Standard` G.729 erfasst den Frequenzbereich von 300 Hz bis 2400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 8 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,9.
G.726 (16 Kbit/s)	Nur für **Codec-Reihenfolge** nicht `Standard` G.726 (16 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 16 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,7.
G.726 (24 Kbit/s)	Nur für **Codec-Reihenfolge** nicht `Standard`

Feld	Beschreibung
	G.726 (24 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 24 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,8.
G.726 (32 Kbit/s)	Nur für **Codec-Reihenfolge** nicht *Standard* G.726 (32 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 32 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,9.
G.726 (40 Kbit/s)	Nur für **Codec-Reihenfolge** nicht *Standard* G.726 (40 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 40 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,2.
DTMF	Nur für **Codec-Reihenfolge** nicht *Standard* Wählen Sie aus, ob der Codec DTMF Outband verwendet werden soll. Zuerst wird versucht RFC 2833 zu verwenden. Wenn die Gegenstelle diesen Standard nicht beherrscht, wird SIP Info verwendet. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
G.726 Codec-Einstellungen	Nur für **Codec-Reihenfolge** nicht *Standard* Wählen Sie das Kodierverfahren für den G.726 Codec aus. Mögliche Werte: • *I.366* • *RFC3551 / X.420*

13.1.4 Optionen

Im Menü **VoIP**->**Einstellungen**->**Optionen** finden sich allgemeine Einstellungen zu VoIP.

Abb. 71: **VoIP**->**Einstellungen**->**Optionen**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
RTP-Port	Geben Sie den Port an, über den die RTP-Daten geleitet werden sollen. Standardmäßig ist der Wert *10000* vorgegeben.
Endgeräte-Registrierungstimer	Geben Sie hier einen Standardwert für die Zeitdauer in Sekunden ein, vor deren Ablauf sich die SIP-Clients erneut registrieren müssen, damit die Verbindung nicht automatisch getrennt wird. Standardmäßig ist der Wert *60* vorgegeben.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
DSCP-Einstellungen für SIP-Daten	Wählen Sie die Art des Dienstes für SIP-Daten aus (TOS, Type of Service). Mögliche Werte: • *DSCP-Binärwert* (Standardwert): Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). Der Standardwert ist *101110*. • *DSCP-Dezimalwert*: Differentiated Services Code Point

Feld	Beschreibung
	nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.

Kapitel 14 Nummerierung

14.1 Externe Anschlüsse

Ihr System ist eine Telekommunikationsanlage zur externen Anschaltung an das Euro-ISDN (DSS1) und das Internet:

ISDN-Anschlüsse (S0): Das System verfügt je nach Modulausbau über externe ISDN-Anschlüsse, die zur Anschaltung an den ISDN-Anschluss des Netzbetreibers konfiguriert sind. Je nach Modulausbau können mehrere ISDN-Anschlüsse wahlweise als interner oder als externer ISDN-Anschluss eingestellt werden.

Hinweis

Wenn Sie in diesen Einstellungen für die Anschlüsse einen Namen vergeben, wird dieser in der weiteren Konfiguration nicht genutzt. Er dient nur zur Beschreibung des Anschlusses.

14.1.1 Anschlüsse

Im Menü **Nummerierung**->**Externe Anschlüsse**->**Anschlüsse** konfigurieren Sie die externen Anschlüsse Ihres Systems.

14.1.1.1 Bearbeiten oder Neu

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

Abb. 72: **Nummerierung->Externe Anschlüsse->Anschlüsse->Neu**

Das Menü **Nummerierung->Externe Anschlüsse->Anschlüsse->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Sie können eine Bezeichnung für den von Ihnen gewählten Anschluss eingeben.
Anschlussart	Zeigt die konfigurierte Anschlussart an. Mögliche Werte: • *Mehrgeräteanschluss* (Standardwert) • *Anlagenanschluss* • *FXO*
Port	Nur für **Anschlussart** = *Mehrgeräteanschluss* Wählen Sie die Beschreibung für den Port aus, über den dieser externe Anschluss angeschlossen ist.
Ports	Nur für **Anschlussart** = *Anlagenanschluss* oder **Anschlussart** = *FXO* Wählen Sie die Beschreibung für den Port aus, über den dieser externe Anschluss angeschlossen ist.

Feld	Beschreibung
	Zur Verfügung stehen alle freien externen ISDN-Schnittstellen. Wählen Sie mit der Schaltfläche **Hinzufügen** weitere Ports aus, um z. B. einen Sammelanschluss zu konfigurieren.

Felder im Menü Einstellungen für Gehende Rufnummer

Feld	Beschreibung
Gehende Rufnummer	Wählen Sie die gewünschte Signalisierung für Rufe nach außen aus. Mögliche Werte: • *Standard* (Standardwert) • *Globale Rufnummer für CLIP-No-Screening* • *Individuelle Rufnummer für CLIP-No-Screening* • *Feste DDI nach Extern*
Globale Rufnummer für CLIP-No-Screening	Nur für **Gehende Rufnummer** = *Globale Rufnummer für CLIP-No-Screening* Hier könenn Sie eine Rufnummer eingeben, die bei allen Verbindungen nach extern beim Angerufenen angezeigt wird. Diese Rufnummer wird nicht überprüft.
Rufnummer des entfernten Gesprächspartners anzeigen	Nur für **Gehende Rufnummer** = *Globale Rufnummer für CLIP-No-Screening* und *Individuelle Rufnummer für CLIP-No-Screening* Sie können die Rufnummer eines externen Gesprächspartners anzeigen lassen, sofern diese signalisiert wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Feste Rufnummer für ausgehende Gespräche anzeigen	Nur für **Gehende Rufnummer** = *Feste DDI nach Extern* Sie können für alle Gespräche nach "außen" eine feste Rufnummer anzeigen lassen, z. B. die Rufnummer Ihrer Zentrale.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Rufnummerntyp	Wählen Sie den Rufnummerntyp für gehende Rufe. Mögliche Werte: • *Systemeinstellung*: Die Standardeinstellung (Ländereinstellung) des Systems wird verwendet. • *Unbekannt*: Wählen Sie diese Einstellung, wenn der Rufnummerntyp "Unbekannt" signalisiert werden soll. • *Subscriber*: Es handelt sich um eine Anschlussnummer. • *National*: Es handelt sich um eine nationale Rufnummer (Ortsnetzkennzahl + Anschlussnummer).
Halten im System	Wählen Sie aus, ob ein Telefongespräch im System auf Wartestellung geschaltet werden soll, ohne die Verbindung zu verlieren. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

14.1.2 Rufnummern

Im Menü **Nummerierung**->**Externe Anschlüsse**->**Rufnummern** weisen Sie den von Ihnen festgelegten externen Anschlüssen die externen Rufnummern und den im Display eines Systemtelefons angezeigten Namen zu.

Ein externer Anschluss kann als Mehrgeräte- oder Anlagenanschluss konfiguriert werden, dabei wird die Beschreibung des Anschlusses festgelegt. Für diesen Anschluss wird dann der vorgesehene Port-Name zugewiesen. Der Port-Name (**Beschreibung**) kann unter **Physikalische Schnittstellen**->**ISDN-Ports**->**ISDN Extern** für den Modul-Anschluss festgelegt werden.

Externe Rufnummern am Anlagenanschluss

Bei einem Anlagenanschluss erhalten Sie eine Anlagenrufnummer gemeinsam mit einem 1-, 2-, 3- oder 4-stelligen Rufnummernplan. Dieser Rufnummernplan bildet die Durchwahlen für den Anlagenanschluss. Haben Sie mehrere Anlagenanschlüsse beauftragt, kann die Anzahl der Durchwahlen erweitert werden oder Sie erhalten eine weitere Anlagenrufnummer mit einem eigenen Rufnummernplan.

Beim Anlagenanschluss werden externe Anrufe bei dem Teilnehmer signalisiert, dessen zugewiesene interne Rufnummer der gewählten Durchwahlrufnummer entspricht. Die internen Rufnummern die direkt über die Durchwahl des Rufnummernplans erreicht werden sollen, konfigurieren Sie als **Interne Rufnummer** im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Hinzufügen**->**Rufnummern**->**Interne Rufnummern**.

Beispiel: Sie haben einen Anlagenanschluss mit der Anlagenrufnummer *1234* und den Durchwahlrufnummern von *0* bis *30*. Ein Anruf unter *1234-22* wird normalerweise bei dem internen Teilnehmer mit der Rufnummer *22* signalisiert. Wenn Sie die Durchwahlrufnummer *22* jedoch in diese Liste eintragen, können Sie festlegen, dass Anrufe unter *1234-22* bei dem internen Teilnehmer mit der Rufnummer *321* signalisiert werden.

Externe Rufnummern am Mehrgeräteanschluss

Bei einem Mehrgeräteanschluss können Sie bis zu 10 Rufnummern (MSN, Mehrfachrufnummern) je ISDN-Anschluss beauftragen. Diese MSN's sind die externen Rufnummern Ihrer ISDN-Anschlüsse. Die Festlegung der internen Rufnummern erfolgt unter **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Hinzufügen**->**Rufnummern**.

14.1.2.1 Bearbeiten oder Neu

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

Abb. 73: **Nummerierung**->**Externe Anschlüsse**->**Rufnummern**->**Neu**

Das Menü **Nummerierung**->**Externe Anschlüsse**->**Rufnummern**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Externer Anschluss	Wählen Sie den in **Nummerierung**->**Externe Anschlüsse**->**Anschlüsse** definierten Anschluss aus, für den Sie die Rufnummernkonfiguration vornehmen wollen.
Rufnummerntyp	Wählen Sie je nach Anschlussart den Rufnummerntyp aus, der

Feld	Beschreibung
	definiert werden soll. Mögliche Werte: • *Einzelrufnummer (MSN)*: Nur für Mehrgeräteanschlüsse. • *Anlagenanschluss-Rufnummer*: Nur für Anlagenanschlüsse. • *Durchwahlausnahme (P-P)*: Nur für Anlagenanschlüsse. • *Anlagenanschluss Zusätzliche MSN*: Nur für Anlagenanschlüsse.
Angezeigter Name	Im Allgemeinen tragen Sie den Namen ein, der für diese Rufnummer im Display des angerufenen Systemtelefons angezeigt werden soll. Für **Rufnummerntyp** = *Anlagenanschluss-Rufnummer* zeigt dieses Feld den Namen des Anschlusses an.
Einzelrufnummer (MSN)	Tragen Sie hier die MSN für einen Mehrgeräteanschluss ein.
Anlagenanschluss-Rufnummer	Tragen Sie hier die Rufnummer für einen Anlagenanschluss ein (ohne Durchwahlrufnummer).
Durchwahlausnahme (P-P)	Tragen Sie hier die Durchwahlausnahme für einen Anlagenanschluss ein. Beachte: Geben Sie hier nur die Durchwahl laut Ihres Rufnummernplans ein, die auf unterschiedliche interne Rufnummern geleitet werden sollen. Die Durchwahl am Anlagenanschluss erfolgt immer zu dem Teilnehmer, dessen Rufnummer als Durchwahl mit gewählt wurde. z. B. der interne Teilnehmer hat die Rufnummer *16*. Wird dieser Teilnehmer von extern angerufen mit *1234567-16*, wird der Anruf an seinem Telefon signalisiert. Soll aber bei der Durchwahl *16* ein Teilnehmer mit der Rufnummer *888* gerufen werden, tragen Sie die *888* als Ausnahmerufnummer ein. Dann weisen Sie in der **Anrufzuordnung** dem Teilnehmer mit der Rufnummer *16* die Ausnahmerufnummer zu. In der **Anrufzuordnung** können Sie dann weitere Einstellungen vornehmen.
Anlagenanschluss Zu-	Tragen Sie hier eine zusätzliche MSN für einen Anlagenan-

Feld	Beschreibung
sätzliche MSN	schluss ein. Bei einigen Providern ist es möglich, parallel zur Durchwahlrufnummer noch eine Mehrgeräterufnummer auf einem Anlagenanschluss zu übertragen, z. B. eine bereits vor dem Einrichten eines Anlagenanschlusses vorhandene Faxrufnummer oder die alte Mehrgeräterufnummer.

14.1.3 Bündel

Im Menü **Nummerierung**->**Externe Anschlüsse**->**Bündel** können Sie verschiedene externe Anschlüsse zusammenfassen und für die Benutzer individuell zur Verfügung stellen.

Sie möchten den internen Teilnehmern bestimmte externe Anschlüsse für gehende Verbindungen zuweisen. Diese externen Anschlüsse können Sie zu Bündeln zusammenfassen und den Teilnehmern für die gehende Wahl zur Verfügung stellen. Auf diese Weise leiten alle Teilnehmer die externe Wahl mit der gleichen Amtskennziffer ein, können dabei aber nur eine Verbindung über die für sie freigegebenen Bündel aufbauen.

Die externen Anschlüsse Ihres Systems können zu Bündeln zusammengefasst werden. Sie können dabei bis zu 99 Bündel (01 - 99) einrichten. Die Kennziffer für die Bündelbelegung kann verändert werden (Menü **Änderbare Kennziffern**).

Bei der Einleitung eines externen Gespräches durch die Bündelkennziffer wird beim Verbindungsaufbau das für den Teilnehmer freigegebene Bündel verwendet.

14.1.3.1 Bearbeiten oder Neu

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

Abb. 74: **Nummerierung**->**Externe Anschlüsse**->**Bündel**->**Neu**

Das Menü **Nummerierung**->**Externe Anschlüsse**->**Bündel**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.
Reihenfolge im Bündel	Wählen Sie die gewünschten externen Anschlüsse für ein Bündel aus. Die Reihenfolge beim Wählen nach extern entspricht der Abfolge der externen Anschlüsse in dieser Liste. Sie möchten den internen Teilnehmern Ihres Systems bestimmte externe Anschlüsse für gehende Verbindungen zuweisen. Die externen Anschlüsse können Sie zu Bündeln zusammenfassen und den Teilnehmern für die gehende Wahl zur Verfügung stellen. Auf diese Weise leiten alle Teilnehmer die externe Wahl mit der gleichen Bündelkennziffer ein, können dabei aber nur eine Verbindung über die für sie freigegebenen Bündel aufbauen.

14.1.4 X.31

Paketvermittelte Datenübertragung (X.31)

Um den Service für Ihre Kunden zu verbessern, möchten Sie diesen auch die bargeldlose Zahlungsweise via ec-Karte oder Kreditkarte ermöglichen oder Kaufdaten für eine Kundenkarte erfassen. Hierzu schließen Sie an Ihr System ein Datengerät an, das die Daten der Kunden-/ Kreditkarten zu einer zentralen Stelle übermittelt.

An den internen ISDN-Anschlüssen des Systems können Sie ein Datenendgerät anschließen, das nach dem X.31-Übertragungsstandard (Datenübertragung im D-Kanal) arbeitet. Dieses sind zum Beispiel Kassenterminals, Geld- oder Kundenkartenautomaten.

Zur Nutzung dieses Leistungsmerkmales werden Ihnen von Ihrem Netzbetreiber TEI‘s (Terminal Endpoint Identifier) mitgeteilt, die Sie in der Konfiguration des Systems einzelnen Anschlüssen zuweisen. Über diese TEI’s erfolgt eine zusätzliche Adressierung dieser Endgeräte.

Hinweis

Dieses Leistungsmerkmal können Sie nur nutzen, wenn das Leistungsmerkmal **X.31** beim Netzbetreiber beauftragt ist und Sie ein entsprechendes Endgerät an diesem Anschluss betreiben. Die Bedienung entnehmen Sie bitte der Bedienungsanleitungen der Endgeräte.

14.1.4.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue X.31-Anwendungen einzurichten.

Abb. 75: **Nummerierung->Externe Anschlüsse->X.31->Neu**

Das Menü **Nummerierung->Externe Anschlüsse->X.31->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Schnittstelle auswählen	Wählen Sie die externe Schnittstelle aus, über die Sie den Netzbetreiber, der Ihnen das Leistungsmerkmal X.31 zur Verfügung stellt, erreichen.
Terminal Endpoint Identifier (TEI)	Wählen Sie hier den TEI-Wert (TEI, Terminal Endpoint Identifier) aus, den Sie von Ihrem Netzbetreiber erhalten haben. Über die TEI's erfolgt eine zusätzliche Adressierung dieser Endgeräte. Mögliche Werte sind *00* bis *63*. Der Standardwert ist *00*.
Interne Zuordnung	Wählen Sie die interne ISDN-Schnittstelle aus, an der Ihr Datengerät, das nach dem X.31-Übertragungsstandard

Feld	Beschreibung
	(Datenübertragung im D-Kanal) arbeitet, angeschlossen ist.

14.2 Benutzereinstellungen

In diesem Menü konfigurieren und verwalten Sie die Benutzer Ihres Systems. Die Benutzer werden in Berechtigungsklassen organisiert, denen die gewünschten externen Leitungen zugewiesen werden und die je nach Anforderung Leistungsmerkmale nutzen dürfen. Der Benutzer, der einer Berechtigungsklasse zugewiesen ist, erhält eine interne Rufnummer und bestimmte Berechtigungen. Im Auslieferzustand ist eine Standard-Berechtigungsklasse (Default CoS) voreingestellt, der neue Benutzer automatisch zugewiesen werden.

Nachdem in den Benutzereinstellungen festgelegt wurde, über welche Funktionen und Berechtigungen ein Benutzer oder mehrere Benutzer verfügen sollen, wird dann im Menü **Endgeräte** einem Endgerät die Berechtigung der Benutzereinstellungen zugewiesen. Somit ist es möglich die Einstellungen für mehrere Endgeräte über eine Berechtigungsklasse einzurichten, z. B. eine Benutzereinstellung *Chef*, eine Benutzereinstellung *Abteilungsleiter* und eine Benutzereinstellung *Sachbearbeiter*. Jetzt müssen die entsprechenden Benutzer nur noch einer dieser **Berechtigungsklasse** zugewiesen werden.

14.2.1 Benutzer

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer** konfigurieren Sie die Benutzer Ihres Systems, deren Klassenzugehörigkeit und weisen ihnen interne und externe Rufnummern zu.

Sie sehen eine Übersicht der bereits angelegten Benutzer. In der Spalte **Name** sind die Einträge alphabetisch sortiert. Sie können in jeder beliebigen anderen Spalte auf den Spaltentitel klicken und die Einträge in aufsteigender oder in absteigender Reihenfolge sortieren lassen.

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

14.2.1.1 Grundeinstellungen

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Grundeinstellungen** geben Sie Basisinformationen zu dem Benutzer an.

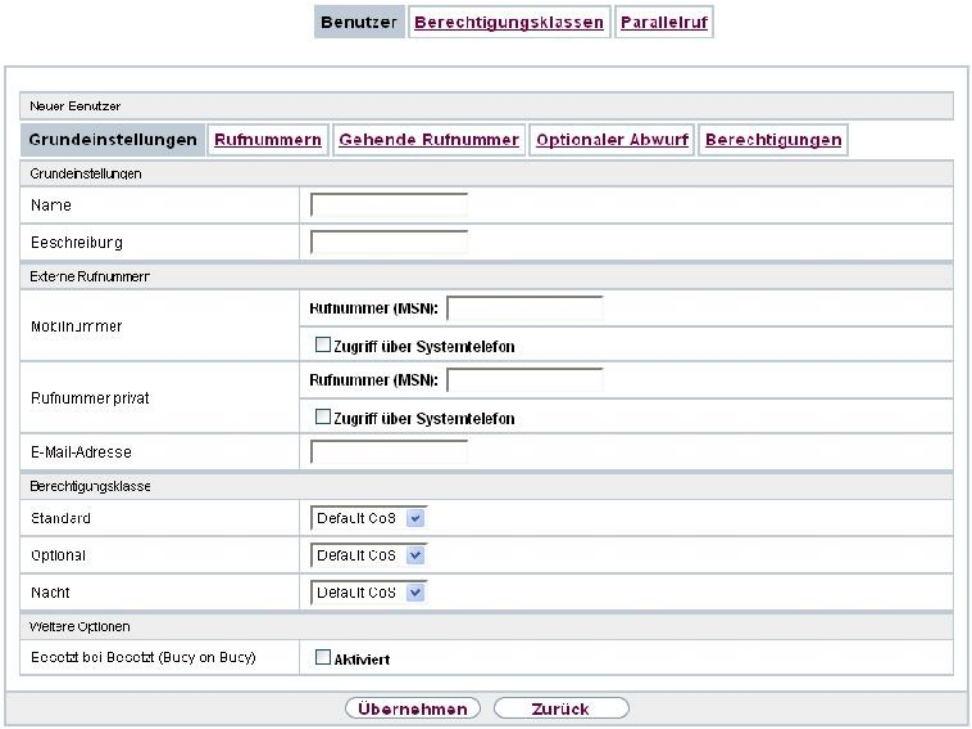


Abb. 76: **Nummerierung->Benutzereinstellungen->Benutzer->Grundeinstellungen**

Das Menü **Nummerierung->Benutzereinstellungen->Benutzer->Grundeinstellungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Name	Geben Sie den Namen des Benutzers ein. Dieser Name wird im Telefonbuch angezeigt, wenn Sie unter **Mobilnummer Rufnummer privat** eine Rufnummer eingetragen und für das Telefonbuch freigegeben haben. Der Name wird mit den Kennzeichnungen (M) für Mobilfunk und (H) für Rufnummer privat im Display des Systemtelefons angezeigt.
Beschreibung	Geben Sie zusätzliche Informationen zu dem Benutzer ein.

Felder im Menü Externe Rufnummern

Feld	Beschreibung
Mobilnummer	Geben Sie eine Rufnummer ein, unter der der Benutzer über

Feld	Beschreibung
	Mobilfunk erreichbar ist. Wählen Sie zusätzlich aus, ob diese Rufnummer im Display des Systemtelefons angezeigt werden soll, damit sie über das Systemtelefon, aus dem System-Telefonbuch gewählt werden kann (Option **Zugriff über Systemtelefon**).
Rufnummer privat	Geben Sie eine Rufnummer ein, unter der der Benutzer privat erreichbar ist. Wählen Sie zusätzlich aus, ob diese Rufnummer im Display des Systemtelefons angezeigt werden soll, damit sie über das Systemtelefon, aus dem System-Telefonbuch gewählt werden kann (Option **Zugriff über Systemtelefon**).
E-Mail-Adresse	Geben Sie die E-Mail-Adresse des Benutzers an.

Felder im Menü Berechtigungsklasse

Feld	Beschreibung
Standard	Wählen Sie die Berechtigungsklassen = CoS (Class of Service). Die Festlegung der Berechtigungsklasse und die Erstellung neuer Berechtigungsklassen erfolgt unter **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**. In dieser Einstellung erfolgt nur die Auswahl. Mögliche Werte: • *Default CoS* (Standardwert) • *Nicht erlaubt*: Keine Berechtigungsklasse • *<Berechtigungsklasse>*
Optional	Wählen Sie eine optionale Berechtigungsklasse aus. Diese CoS wird in den Kalendereinstellungen benötigt. Die Festlegung der Berechtigungsklasse und die Erstellung neuer Berechtigungsklassen erfolgt unter **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**. In dieser Einstellung erfolgt nur die Auswahl. Mögliche Werte: • *Default CoS* (Standardwert) • *Nicht erlaubt*: Keine Berechtigungsklasse • *<Berechtigungsklasse>*

Feld	Beschreibung
Nacht	Wählen Sie für den Nachtbetrieb die Berechtigungsklasse aus. Diese CoS wird in den Kalendereinstellungen benötigt. Die Festlegung der Berechtigungsklasse und die Erstellung neuer Berechtigungsklassen erfolgt unter **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**. In dieser Einstellung erfolgt nur die Auswahl. Mögliche Werte: • *Default CoS* (Standardwert) • *Nicht erlaubt*: Keine Berechtigungsklasse • *<Berechtigungsklasse>*

Felder im Menü Weitere Optionen

Feld	Beschreibung
Besetzt bei Besetzt (Busy on Busy)	Wählen Sie aus, ob für diesen Benutzer das Leistungsmerkmal "Busy on Busy" aktiviert sein soll. Führt ein Benutzer, für den mehrere Telefonnummern eingerichtet sind, ein Gespräch, so können Sie entscheiden, ob weitere Anrufe für diesen Benutzer signalisiert werden sollen. Ist die Funktion "Busy on Busy" für diesen Benutzer eingerichtet, so erhalten weitere Anrufer **Besetzt** signalisiert, wenn der Benutzer auf einer seiner Nummern telefoniert. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

14.2.1.2 Rufnummern

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Rufnummern** können die internen Rufnummern, die später den Endgeräten zugeordnet werden, eingetragen werden. Je nach Typ können dann pro Endgerät eine oder mehrere Rufnummern zugeordnet werden.

Abb. 77: **Nummerierung->Benutzereinstellungen->Benutzer->Rufnummern**

Das Menü **Nummerierung->Benutzereinstellungen->Benutzer->Rufnummern** besteht aus folgenden Feldern:

Felder im Menü Interne Rufnummern

Feld	Beschreibung
Interne Rufnummern	Geben Sie die internen Rufnummern für den Benutzer ein und die Beschreibung, die in den Displays der Systemtelefone angezeigt werden soll (**Angezeigte Beschreibung**). Wählen Sie außerdem aus, ob diese interne Rufnummer im **System-Telefonbuch** angezeigt werden soll, und ob die LED neben der entsprechend belegten Funktionstaste (**Besetztlampenfeld**) leuchten soll. Standardmäßig sind die Funktionen aktiviert. Fügen Sie mit **Hinzufügen** neue **Interne Rufnummern** hinzu.

14.2.1.3 Gehende Rufnummer

Im Menü **Nummerierung->Benutzereinstellungen->Benutzer->Gehende Rufnummer** wählen Sie die gehenden Rufnummern für den Benutzer aus.

Wenn bei einem gehenden Gespäch der ferne Teilnehmer nicht die Rufnummer, die dem eigenen Anschluss zugeordnet ist, sehen soll, kann hier eine der vorhandenen Rufnummern für die Anzeige ausgewählt werden. Wird keine Rufnummer festgelegt, sendet das System keine Rufnummer zum Provider mit.

Abb. 78: **Nummerierung->Benutzereinstellungen->Benutzer->Gehende Rufnummer**

Felder in der Liste Gehende Rufnummer

Feld	Beschreibung
Interne Rufnummer	Zeigt die internen Rufnummern, die für den Benutzer konfiguriert sind.
Angezeigte Beschreibung	Zeigt zu jeder internen Telefonnummer die Beschreibung, die für die Anzeige in den Displays der Systemtelefone konfiguriert ist.
Gehende Rufnummer	Wählen Sie die gewünschte Signalisierung für Rufe nach außen aus. Mögliche Werte: • *Standard, eigene DDI-Signale*: Die eigene Durchwahl wird als **Gehende Rufnummer** verwendet. Diese Option ist bei einem Anlagenanschluss oder bei einem SIP-Provider mit Durchwahl verfügbar. • *Standard*: Es wird keine **Gehende Rufnummer** gesendet. Die Vermittlungsstelle verwendet in diesem Fall die Hauptrufnummer des Anschlusses. • *<Feste Rufnummer>*: Für einen FXO-Anschluss ist die konfigurierte Rufnummer bereits als **Gehende Rufnummer** zugewiesen und wird angezeigt. • *<Rufnummer>* : Sie können bei mehreren konfigurierten Nummern eine Rufnummer wählen, die Sie als **Gehende Rufnummer** verwenden wollen.

Wählen Sie das Symbol , um für jede interne Rufnummer (in der Tabelle angezeigt mit **Interne Rufnummer** und **Angezeigte Beschreibung**) festzulegen, welche Rufnummer bei gehenden Rufen angezeigt werden soll. Dabei wählen Sie für jeden konfigurierten externen

Anschluss eine der dafür konfigurierten Rufnummern aus.

Abb. 79: **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Gehende Rufnummer**->

Wenn mehrere externe Anschlüsse konfiguriert sind, können Sie festlegen, wie mit gehenden Gesprächen verfahren werden soll. Die Reihenfolge der Einträge bestimmt, in welcher Reihenfolge bei belegter externer Leitung über die anderen zugewiesenen Leitungen gewählt werden soll.

Die konfigurierte **Gehende Rufnummer** kann individuell für jede Leitung nach außen verborgen werden, Dazu setzen Sie einen Haken unter **Nummer verbergen** in der entsprechenden Zeile.

Wenn Sie einen Eintrag in der angezeigten Liste verschieben wollen, wählen Sie das Symbol in der entsprechenden Zeile. Ein neues Fenster öffnet sich.

Abb. 80: **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Gehende Rufnummer**->->

Der gewählte Eintrag wird unter **Externer Anschluss** angezeigt, hier z. B. *ISDN_1*.

Gehen Sie folgendermaßen vor, um den gewählten Eintrag zu verschieben:

(1) Wählen Sie unter **Verschieben** in der Liste den Eintrag aus, relativ zu dem Sie den gewählten Eintrag verschieben wollen, hier z. B. *1.SIP-Provider_1*.

(2) Wählen Sie, ob Sie den Eintrag *über* oder *unter* dem gewählten Eintrag in der Liste einsortieren wollen, hier z. B. *über*.

(3) Wählen Sie **Übernehmen**.
Die Einträge werden in der geänderten Reihenfolge angezeigt.

(4) Falls die Liste mehr als zwei Einträge enthält, verschieben Sie gegebenenfalls weitere Einträge.

Die hier konfigurierte Reihenfolge überschreibt die Einstellung, die durch die Berechtigungsklasse zugewiesen ist. Die zugeordnete Berechtigungsklasse legt aber nach wie vor fest, ob ein Benutzer Zugriff auf einen bstimmten externen Anschluss hat.

14.2.1.4 Optionaler Abwurf

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Optionaler Abwurf** können Sie jeder der angezeigten internen Rufnummern eines Teilnehmers eine **Abwurfanwendung** und eine **Aktive Variante (Tag)** zuordnen.

Hier können Sie zum Beispiel regeln, an welchen Kollegen Anrufe weitergeleitet werden sollen, wenn Sie an einer Konferenz teilnehmen, und ob während der Mittagspause die Zentrale für Anrufe zuständig ist.

Abb. 81: **Nummerierung->Benutzereinstellungen->Benutzer->Optionaler Abwurf**

Felder im Menü Optionaler Abwurf

Feld	Beschreibung
Interne Rufnummer	Zeigt die internen Rufnummern, die für den Benutzer konfiguriert sind.
Angezeigte Beschrei-	Zeigt zu jeder internen Telefonnummer die Beschreibung, die

Feld	Beschreibung
bung	für die Anzeige in den Displays der Systemtelefone konfiguriert ist.
Abwurfanwendung	Wählen Sie aus der Dropdown-Liste die gewünschte Abwurfanwendung, die Sie der internen Rufnummer zuweisen wollen. Sie können aus den Abwurfanwendungen wählen, die Sie im Menü **Anwendungen**->**Abwurf**->**Abwurfanwendungen**->**Neu** mit **Typ der Abwurfanwendung** = *Interner Teilnehmer* konfiguriert haben. Mögliche Werte: • *Keiner* • <Abwurfanwendung>
Aktive Variante (Tag)	Wählen Sie die Variante der Abwurfanwendung aus, die zurzeit aktiv sein soll. Ist eine Umschaltung der Varianten über den Kalender eingerichtet, wird diese Einstellung zeitgerecht wieder umgeschaltet. Mögliche Werte: • *Variante 1* • *Variante 2* • *Variante 3* • *Variante 4*

14.2.1.5 Berechtigungen

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Berechtigungen** können Sie diesem Benutzer ermöglichen, bestimmte Einstellungen über die HTML-Konfiguration selbst vorzunehmen. Dazu müssen in der Benutzer-HTML-Konfiguration Benutzername und Passwort eingetragen werden und der persönliche Zugang freigegeben sein. Nach dem Ausloggen kann man dann nach Eingabe dieses Benutzernamens und Passworts die entsprechenden Einstellungen ansehen und ändern.

Abb. 82: **Nummerierung->Benutzereinstellungen->Benutzer->Berechtigungen**

Das Menü **Nummerierung->Benutzereinstellungen->Benutzer->Berechtigungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Passwort für IP-Telefonregistrierung	Geben Sie das Passwort ein, mit dem sich ein IP-Telefon des Benutzers am System anmelden muss. Das Passwort kann freibleiben, wenn IP-Telefone sich registrieren aber nicht authentifizieren müssen.
PIN für Zugang via Telefon	Hier können Sie die PIN für den persönlichen Anrufbeantworter (Voice Mailbox) des Benutzers ändern.. Der Standardwert ist *none*.

Felder im Menü Benutzer-HTML-Konfiguration

Feld	Beschreibung
Persönlicher Zugang	Wählen Sie aus, ob dieser Benutzer Zugriffsberechtigung auf eine personalisierte Benutzeroberfläche (Benutzerzugang) erhalten soll, in der er eigene Einträge oder Einstellungen vornehmen kann. Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Benutzername	Nur für **Persönlicher Zugang** aktiviert. Geben Sie einen Benutzernamen für diesen Benutzer ein. Dieser wird für den Login in die Benutzeroberfläche benötigt.
Passwort	Nur für **Persönlicher Zugang** aktiviert. Geben Sie ein Passwort für diesen Benutzer ein. Dieses wird für den Login in die Benutzeroberfläche benötigt.

Call Through

Unter Call Through versteht man die Einwahl über einen externen Anschluss in das System und die Weiterwahl aus dem System über einen anderen externen Anschluss.

Hinweis

In den Verbindungsdatensätzen wird für die kommende und gehende Verbindung je ein Datensatz erstellt.

Felder im Menü Weitere Optionen

Feld	Beschreibung
Call Through	Wählen Sie aus, ob für diesen Benutzer Call Through erlaubt werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn sie die Funktion aktivieren, müssen Sie unter **Nutze Einstellungen von Rufnummer** auswählen, von welcher internen Rufnummer die zugelassenen externen Leitungen und Anrufvarianten für den Call Through genutzt werden sollen.

14.2.2 Berechtigungsklassen

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen** (CoS) werden die Funktionen und Leistungsmerkmale für die Benutzereinstellungen festgelegt. Diese Berechtigungsklassen können dann in den Benutzereinstellungen den einzelnen Benutzern (Benutzergruppen) zugewiesen werden.

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere Berechtigungsklassen anzulegen. Standardmäßig ist die Berechtigungsklasse `Default CoS` konfiguriert.

14.2.2.1 Grundeinstellungen

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Grundeinstellungen** werden die grundsätzlichen Einstellungen sowie der Name für die neue Berechtigungsklasse festgelegt. Über den Namen ist die Berechtigungsklasse zu finden.

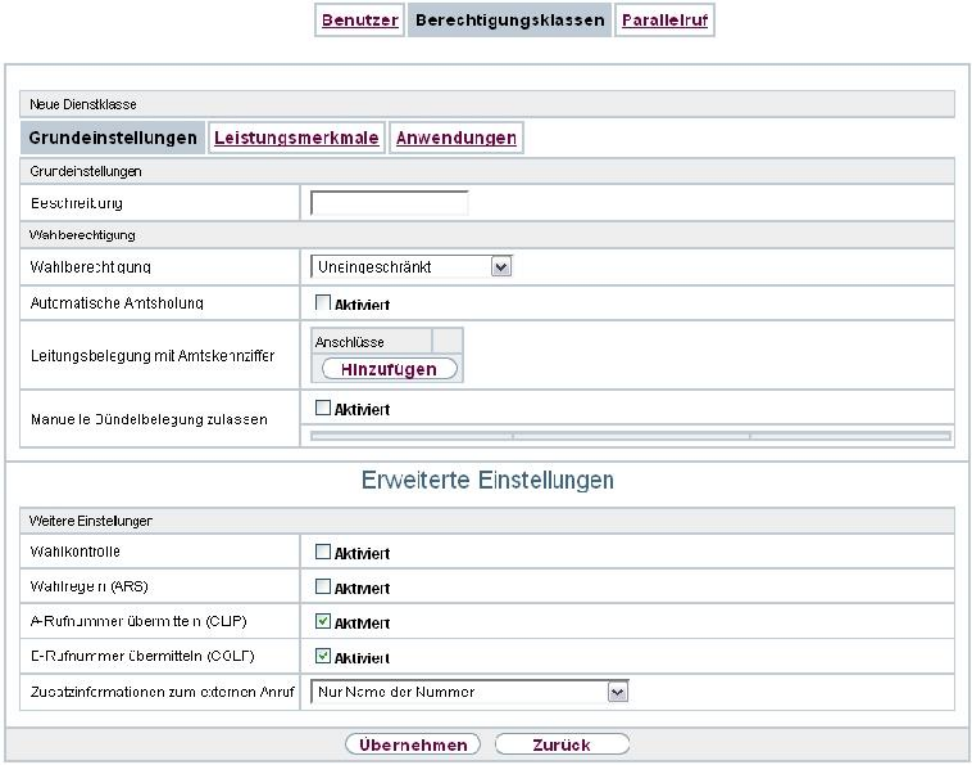


Abb. 83: **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Grundeinstellungen**

Das Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Grundeinstellungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.

Felder im Menü Wahlberechtigung

Feld	Beschreibung
Wahlberechtigung	Wählen Sie die Wahlberechtigung für die Berechtigungsklasse aus. Die Wahlberechtigung legt fest, welche Gespräche (intern, extern, ...) geführt werden dürfen. Im System werden mehrere Berechtigungsstufen unterschieden. Mögliche Werte: • *International* : Die Telefone haben uneingeschränkte Berechtigungen für die Wahl und können alle Verbindungen selbst einleiten. • *National*: Die Telefone können außer internationalen Gesprächen alle Gespräche selbst einleiten. Beginnt eine Rufnummer mit der Kennziffer für internationale Wahl, kann diese Rufnummer nicht gewählt werden. • *Kommend*: Die Telefone sind kommend für externe Gespräche erreichbar, können aber selbst keine externen Gespräche einleiten. Interne Gespräche sind möglich. • *Region*: Die Telefone können keine nationalen und internationalen Gespräche führen. Für diese Wahlberechtigung sind 10 Ausnahmerufnummern konfigurierbar, über die eine nationale oder internationale Wahl ermöglicht werden kann. Eine Ausnahmerufnummer kann aus vollständigen Rufnummern oder Teilen einer Rufnummer (z. B. die ersten Ziffern) bestehen. • *Ort*: Die Telefone können Ortsgespräche führen. Nationale und internationale Gespräche sind nicht möglich. • *Intern*: Die Telefone sind kommend und gehend nicht für externe Gespräche berechtigt. Es können nur interne Gespräche geführt werden.

Feld	Beschreibung
Automatische Amtsholung	Diese Einstellung legt fest, ob für die Berechtigungsklasse die automatische Amtsholung eingerichtet wird. Bei automatischer Amtsholung hören die Benutzer dieser Berechtigungsklasse nach Abheben des Hörers den externen Wählton und können sofort extern wählen. Zum internen Telefonieren muss dann nach dem Abheben des Hörers zuerst die Stern-Taste betätigt werden.
Leitungsbelegung mit Amtskennziffer	Wählen Sie die Anschlüsse aus, über die gehende Gespräche dieser Telefone nach Extern geleitet werden sollen. Die Reihenfolge des Eintrags legt fest, in welcher Reihenfolge bei belegter externer Leitung, über die anderen zugewiesenen Leitungen gewählt werden soll.
Manuelle Bündelbelegung zulassen	Neben der allgemeinen Amtsbelegung kann ein Telefon auch gezielt ein Bündel belegen. Hierbei wird eine externe Verbindung mit der entsprechenden Kennziffer zur gezielten Belegung des Bündels eingeleitet und nicht durch die Wahl der Amtskennziffer. Um eine gezielte Bündelbelegung durchführen zu können, muss die Berechtigungsklasse die Berechtigung dafür besitzen. Diese Berechtigung kann auch Bündel umfassen, die die Berechtigungsklasse sonst nicht belegen kann. Hat ein Telefon nicht die Berechtigung zur gezielten Bündelbelegung oder ist das gewählte Bündel belegt, hört es nach Wahl der Kennziffer den Besetztton. Ist für eine Berechtigungsklasse die **Automatische Amtsholung** eingerichtet, müssen Benutzer dieser Berechtigungsklasse vor einer gezielten Bündelbelegung die Stern-Taste betätigen und anschließend die externe Wahl durch die Kennziffer zur Bündelbelegung einleiten. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wählen sie anschließend die Bündel aus, für die die manuelle Bündelbelegung zugelassen werden soll. Bündel konfigurieren Sie im Menü **Nummerierung**->**Externe Anschlüsse**->**Bündel**.

Rufnummernanzeige

Wenn Sie einen Gesprächspartner anrufen, wird diesem Ihre Rufnummer angezeigt. Da-

durch sieht Ihr Gesprächspartner schon vor dem Abheben des Hörers, dass Sie ihn anrufen. Möchten Sie nicht, dass Ihr Gesprächspartner schon vor dem Abheben des Hörers Ihre Rufnummer sieht, können Sie die Anzeige der Rufnummer bei Ihrem Gesprächspartner verhindern.

Hat Ihr Gesprächspartner eine Anrufweiterschaltung eingerichtet, wissen Sie nicht, an welchem Telefon Sie Ihren Gesprächspartner erreicht haben. In diesem Fall können Sie sich die Rufnummer, zu der Ihr Gesprächspartner den Anruf weitergeschaltet hat, anzeigen lassen. Ihr Gesprächspartner hat aber auch die Möglichkeit, die Anzeige dieser Rufnummer zu verhindern.

Durch die Rufnummernanzeige kann bereits bei der Signalisierung eines Anrufes auch im Display eines analogen Telefons die Rufnummer des Anrufers angezeigt werden. Auf diese Weise wissen Sie schon vor der Annahme des Gespräches, wer Sie sprechen möchte.

Hinweis

Die Übermittlung von analogen CLIP-Informationen kann für jeden analogen Anschluss separat eingerichtet werden. Lesen Sie bitte in der Bedienungsanleitung Ihrer analogen Endgeräte nach, ob diese die Leistungsmerkmale "CLIP" und "CLIP off Hook" unterstützen.

Nicht alle beschriebenen Leistungsmerkmale sind im ISDN-Standard-Anschluss enthalten. Bitte erkundigen Sie sich bei Ihrem Netzbetreiber, inwiefern die einzelnen Leistungsmerkmale gesondert für Ihren ISDN-Anschluss beauftragt werden müssen.

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

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Wahlkontrolle	Wählen Sie aus, ob die im Menü **Anrufkontrolle**->**Ausgehende Dienste**->**Wahlkontrolle** eingetragenen Rufnummern auch für diese Berechtigungsklasse gesperrt oder zugelassen werden sollen. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Wahlregeln (ARS)	Wählen Sie aus, ob die im Menü **Anrufkontrolle**->**Wahlregeln** eingetragenen Routingregeln auch für diese Berechtigungsklasse angewendet werden sollen.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
A-Rufnummer übermitteln (CLIP)	Wählen Sie aus, ob die Rufnummer des Anrufers beim Angerufenen angezeigt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
B-Rufnummer übermitteln (COLP)	Wählen Sie aus, ob die Rufnummer des Angerufenen beim Anrufer angezeigt werden soll. Hat zum Beispiel der Angerufene eine Anrufweiterschaltung zu einem dritten Teilnehmer eingerichtet, so kann sich der Anrufer durch dieses Leistungsmerkmal die Rufnummer des Ziels der Anrufweiterschaltung anzeigen lassen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Zusatzinformationen zum externen Anruf	Wählen Sie aus, was bei einem Amtsruf im Display angezeigt werden soll. Mögliche Werte: • *Namen des Anschlusses und der Nummer*: Der Amtsanschluss und der zugewiesene Name werden abwechselnd im Display angezeigt. • *Nur Name des Anschlusses*: Es wird nur der zugewiesene Name des Amtsanschlusses angezeigt. • *Nur Name der Nummer* (Standardwert): Nur der zugewiesene Name der externen Rufnummer wird im Display angezeigt. • *Keiner*: Keine Anzeige im Display.

14.2.2.2 Leistungsmerkmale

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Leistungsmerkmale** werden zusätzliche Funktionen eingerichtet.

Abb. 84: **Nummerierung->Benutzereinstellungen->Berechtigungsklassen->Leistungsmerkmale**

Heranholen von Rufen (Pick-Up)

Ein Anruf wird bei einem Kollegen signalisiert, der sich aber gerade nicht an seinem Arbeitsplatz befindet. Sie haben nun zwei Möglichkeiten um den Anrufer trotzdem zu bedienen. Sie könnten aufstehen und zum Telefon Ihres Kollegen gehen, oder Sie holen den Anruf Ihres Kollegen zu Ihrem Telefon heran.

Über eine Kennziffer kann ein Anruf, der an einem andern Telefon signalisiert wird, herangeholt werden. Die Zuordnung erfolgt über die Option **Pick-Up-Gruppe** im Menü **Leistungsmerkmale**, welche dann den Teilnehmer zugeordnet ist. Bei identischem Wert ist ein Pick-Up möglich. Heranholen des Rufes ist bei offener Rückfrage nicht möglich.

Systemtelefone können Anrufe über programmierte Funktionstasten heranholen. Sie können an Systemtelefonen Leitungstasten, Linientasten oder Teamtasten einrichten.

- Leitungstaste: Unter einer Leitungstaste wird ein ISDN-Anschluss oder ein VoIP-Provider eingerichtet. Die der Leitungstaste zugeordnete Leuchtdiode zeigt den Status des Anschlusses an. Die LED leuchtet, wenn beide B-Kanäle eines Anschlusses belegt sind oder wenn die maximale Anzahl gleichzeitiger Verbindungen über einen VoIP-Provider erreicht ist. Wird ein externer Anruf an einem anderen internen Telefon signalisiert, können Sie diesen durch Betätigen der Leitungstaste heranholen.
- Linientaste: Unter einer Linientaste wird ein Benutzer des Systems eingerichtet. Die der Linientaste zugeordnete Leuchtdiode zeigt den Status des Teilnehmers an (Anruf, Ver-

bindung,...). Wird ein Anruf an diesem internen Teilnehmer signalisiert, können Sie diesen durch Betätigen der Linientaste heranholen.

- Teamtaste: Eine Teamtaste ist eine normale Linientaste, der die interne Rufnummer eines Teams zugeordnet wird. Die der Teamtaste zugeordnete Leuchtdiode zeigt den Status des Teams an (Anruf, Verbindung,...). Wird ein Anruf für dieses Team signalisiert, können Sie diesen durch Betätigen der Teamtaste heranholen.

Anklopfen

Sie möchten nach Möglichkeit den Anruf jedes Kunden entgegennehmen, auch wenn Sie gerade telefonieren. Wird ein weiterer Anruf durch einen Anklopfton oder eine Displayanzeige an Ihrem Telefon signalisiert, können Sie entscheiden, mit welchem der beiden Kunden Sie sprechen möchten.

Wird ein Internteilnehmer angerufen, der sich gerade im Gesprächszustand befindet, so wird bei ihm automatisch angeklopft. Das Anklopfen ist bei internen und externen Gesprächen möglich. Die anklopfende Verbindung wird beim Angerufenen optisch und / oder akustisch je nach Endgerät signalisiert.

Der Angerufene kann:

- Die anklopfende Verbindung abweisen und das aktuelle Gespräch fortsetzen. Dem Anrufer wird dann "besetzt" signalisiert.
- Die anklopfende Verbindung annehmen und seine aktuelle Verbindung halten.
- Die anklopfende Verbindung annehmen nachdem die aktuelle Verbindung beendet wurde.
- Die anklopfende Verbindung ignorieren. Nach 30 Sekunden wird das Anklopfen automatisch beendet und dem Anrufer "besetzt" signalisiert.

Analoge Endgeräte

Die Möglichkeit des Anklopfens kann für jeden Teilnehmer individuell eingestellt werden. Das Anklopfen erlauben oder nicht erlauben kann über die Konfiguration oder über eine Kennziffer in der Bedienung eingestellt werden.

Analoge Endgeräte hören den Anklopfton des Systems. Die Rufnummer des Anklopfenden kann im Display des analogen Telefons angezeigt werden, wenn dieses über das entsprechende Leistungsmerkmal (CLIP off Hook) verfügt. Bei analogen Endgeräten ist "CLIP off Hook" in der Grundeinstellung ausgeschaltet, kann aber über die Konfiguration eingeschaltet werden.

Im System kann nur auf eine begrenzte Anzahl von analogen Verbindungen gleichzeitig angeklopft werden. Wird bereits mit dieser maximalen Anzahl von Anklopftönen auf analoge Verbindungen angeklopft, wird bei weiteren anklopfenden Anrufern "besetzt" signalisiert.

Wenn Sie während eines Gespräches den Anklopfton hören, können Sie das Gespräch übernehmen und das bestehende Gespräch weitervermitteln. Durch eine Bedienprozedur ist es möglich, das bestehende Gespräch weiter zu vermitteln und das anklopfende Gespräch anzunehmen. Dabei gelten die folgenden Bedingungen:

- Jede gewählte Rufnummer wird vom System angenommen.
- Nach der Bedienprozedur sind Teilnehmer und der anklopfende Teilnehmer sofort miteinander verbunden (ohne Quittungstöne).
- Eine Übergabe auf die eigene Rufnummer ist möglich, es wird dann angeklopft.
- Interne, externe Zielteilnehmer sowie Teams können gewählt werden.
- Bei ungültiger oder besetzter Zielrufnummer erfolgt ein Wiederanruf.
- Ist der Teilnehmer frei, erfolgt nach der eingerichteten Zeit des Zielteilnehmers Wiederanruf.
- Bei Übergabe an eine Teamrufnummer erfolgt kein Wiederanruf bei einem besetzten oder nicht erreichbaren Team.
- Bei Übergabe an eine Teamrufnummer wird nur der Wiederanruf nach Zeit unterstützt.

ISDN-Endgeräte

Die Einstellung und Bedienung des Anklopfens erfolgt, wie in der Bedienungsanleitung der jeweiligen Endgeräte beschrieben. ISDN-Endgeräte verwenden zur Signalisierung des Anklopfens ihre eigenen Töne.

Hinweis

Anklopfen ist nicht möglich:

- bei Konferenzgesprächen
- bei Ruhe vor dem Telefon (analoge Endgeräte)
- bei Durchsage
- bei Raumüberwachung
- bei Endgeräten, für die das Leistungsmerkmal "Datenschutz" eingerichtet ist (z. B. Fax, Modem)
- im Wahlzustand eines analogen Teilnehmers (der Hörer ist abgehoben aber es besteht noch keine Gesprächsverbindung)
- bei bestehender Anklopfsperre
- bei Wahl einer Teamrufnummer. Bei analogen Teamteilnehmern wird dann nicht angeklopft.

ISDN-Telefone können einen anklopfenden Ruf auch über das Leistungsmerkmal "Call

Deflection" zu einem anderen Teilnehmer weiterleiten. Eine aktive Verbindung wird z. B. durch Auflegen des Hörers beendet. Daraufhin wird die anklopfende Verbindung signalisiert und kann z. B. durch Abheben des Hörers angenommen werden.

Das Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Leistungsmerkmale** besteht aus folgenden Feldern:

Felder im Menü Berechtigung

Feld	Beschreibung
Pick-Up-Gruppe	Geben Sie die Nummer der Gruppe ein, in der Rufe herangeholt werden dürfen.
Anklopfen	Wählen Sie aus, ob für diese Berechtigungsklasse Anklopfen erlaubt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Globalen Abwurf anwenden	Wählen Sie aus, ob für diese Berechtigungsklasse ein globaler Abwurf erlaubt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. **Hinweis** Das Abwurfziel muss sich in einer Berechtigungsklasse befinden, in der kein globaler Abwurf erlaubt ist.
Anrufvarianten manuell umschalten	Wählen Sie aus, ob für diese Berechtigungsklasse das manuelle Umschalten von Anrufvarianten erlaubt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Call Through	Wählen Sie aus, ob für diese Berechtigungsklasse Call Through erlaubt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

Wechselsprechen

Die Wechselsprech-Funktion ermöglicht es Ihnen, von einem Systemtelefon eine Verbindung zu einem anderen Systemtelefon aufzubauen, ohne dass diese Verbindung vom gerufenen Systemtelefon aktiv angenommen werden muss (Hörer abheben, Freisprechen/Lauthören einschalten). Sobald das Systemtelefon die Wechselsprech-Verbindung angenommen hat, wird die Verbindung hergestellt. Das anrufende und das angerufene Systemtelefon hören zu Beginn des Wechselsprechens einen Aufmerkton. Die Dauer des Wechselsprechens ist auf zwei Minuten begrenzt. Wird in dieser Zeit der Hörer eines beteiligten Telefons abgehoben, so wird das Gespräch in eine normale Verbindung umgesetzt.

Systemtelefone können einen Wechselsprech-Anruf über das Menü des Systemtelefons oder eine programmierte Funktionstaste einleiten. Wird das Wechselsprechen über eine Funktionstaste eingeleitet, erscheinen im Display des Systemtelefons die Anzeigen wie bei einem normalen Verbindungszustand und die Leuchtdiode der Wechselsprech-Taste wird eingeschaltet. Das Beenden des Wechselsprechens ist durch erneutes Betätigen der Funktionstaste oder durch Betätigen der Lautsprecher-Taste möglich. Nach Beenden des Wechselsprechens wird die Leuchtdiode wieder ausgeschaltet.

Ist ein Telefon oder ein Systemtelefon Ziel eines Wechselsprech-Anrufes, wird im Display die Rufnummer des Anrufers angezeigt. Über den Lautsprecher wird der Wechselsprech-Anruf mit einem Aufmerkton angekündigt. Mit der ESC-Taste kann das Wechselsprechen abgebrochen werden.

Zum Sperren oder Erlauben von Wechselsprech-Anrufen kann an einem Systemtelefon ebenfalls eine Funktionstaste eingerichtet werden.

Hinweis

Wechselsprech-Anrufe werden von dem gerufenen Telefon automatisch durch Aktivieren der Funktion Freisprechen angenommen, wenn:

- das Telefon sich in Ruhe befindet,
- das Wechselsprechen erlaubt ist und
- die Funktion "Ruhe vor dem Telefon" (Anrufschutz) nicht aktiviert ist.

Wird eine Wechselsprech-Verbindung nicht von einem der beiden Teilnehmer beendet, so wird diese Verbindung nach ca. 2 Minuten automatisch vom System beendet.

Durchsage

Sie möchten Ihre Mitarbeiter zu einer Besprechung oder zum Essen zusammenrufen? Sie könnten jeden einzeln anrufen oder einfach die Durchsage-Funktion nutzen. Mit nur einem Anruf erreichen Sie alle durchsageberechtigten Telefone, ohne dass Ihre Gesprächspartner die Hörer abheben müssen.

Achtung

Mit der Durchsage können Sie zwar gehört werden, jedoch können Sie die evtl. Kommentare Ihrer Mitarbeiter oder Ihrer Familienangehörigen nicht hören.

Die Durchsage-Funktion ermöglicht es Ihnen, eine Verbindung zu einem anderen Telefon aufzubauen, ohne dass diese Verbindung von diesem aktiv angenommen werden muss (Hörer abheben oder Freisprechen/Lauthören einschalten). Sobald ein Telefon die Durchsage angenommen hat, wird die Verbindung hergestellt. Der Durchsagende und der gerufene Teilnehmer hören zu Beginn einer Durchsage einen positiven Quittungston. Die Dauer einer Durchsage ist nicht begrenzt.

Die Durchsage ist zu ISDN- und analogen Telefonen möglich, wenn diese das Leistungsmerkmal Durchsage unterstützen. Lesen Sie bitte in der Bedienungsanleitung Ihrer Telefone nach, ob das Leistungsmerkmal unterstützt wird.

Telefonen kann über eine Kennziffer die Durchsage zu ihnen erlaubt oder gesperrt werden.

Systemtelefone

Die Durchsage von und zu Systemtelefonen ist möglich. Systemtelefone können eine Durchsage über das Menü des Systemtelefons oder über eine programmierte Funktionstaste einleiten. Wird eine Durchsage über eine Funktionstaste eingeleitet, erscheinen im Display Ihres Telefons die Anzeigen wie bei einem normalen Verbindungszustand und die Leuchtdiode der Durchsage-Taste wird eingeschaltet. Das Beenden der Durchsage ist durch erneutes Betätigen der Funktionstaste oder durch Betätigen der Lautsprecher-Taste möglich. Nach Beenden der Durchsage wird die Leuchtdiode wieder ausgeschaltet.

Ist ein Systemtelefon Ziel einer Durchsage, erscheint im Display des Telefons die Rufnummer des Durchsagenden. Über den Lautsprecher wird die Durchsage mit dem positiven Quittungston angekündigt. Mit der ESC-Taste kann die Durchsage abgebrochen werden.

Zum Sperren oder Erlauben von Durchsagen kann an einem Systemtelefon ebenfalls eine Funktionstaste mit zugehöriger Leuchtdiode eingerichtet werden.

Einzeldurchsage

Sie können durch Wahl der Internrufnummer eines Telefons die Durchsage gezielt einlei-

ten. Die Durchsage kann vom Zielteilnehmer über eine Bedienprozedur erlaubt oder gesperrt werden. Die Durchsage wird beim Zielteilnehmer und beim Durchsagenden mit dem positiven Quittungston angekündigt.

Teamdurchsage

Eine Durchsage kann durch Wahl einer Teamrufnummer auch auf ein Team erfolgen. Die Teamteilnehmer hören die Durchsage gleichzeitig. Die Durchsage wird bei den Zielteilnehmern und beim Durchsagenden mit dem positiven Quittungston angekündigt. Die Durchsage zu einem Team ist auch aus einer Rückfrage heraus möglich. Bei einer Teamdurchsage kann es bis zu vier Sekunden dauern, bevor die Verbindung zu den einzelnen Teamteilnehmern hergestellt wird. Die Durchsage erfolgt dann zu den Teamteilnehmern, die innerhalb dieser Zeit die Durchsage angenommen haben.

Hinweis

Durchsagen werden von den gerufenen Telefonen automatisch durch Aktivieren der Funktion Lauthören angenommen, wenn:

- das Telefon sich in Ruhe befindet,
- die Durchsage eingerichtet ist und
- die Funktion "Ruhe vor dem Telefon" nicht aktiviert ist.

MWI (Message Waiting Indication)

Sie haben neue Nachrichten auf Ihrer Mailbox oder bei Ihrem Internetanbieter warten neue E-Mails auf Sie. Sie müssen nun ständig selbst nachschauen, wissen aber vorher nicht, ob wirklich neue Nachrichten vorhanden sind. Durch das Leistungsmerkmal MWI erhält Ihr System von dem entsprechenden Diensteanbieter die Information über neue Nachrichten. Sie brauchen Ihre Mailbox oder Ihr E-Mail-Postfach jetzt nur noch abfragen, wenn wirklich neue Nachrichten vorhanden sind. Weiterhin können Sie eine MWI von einer an das System angeschalteten Voice Box oder von einem Systemtelefon, das als Rezeptionstelefon eingerichtet ist versenden.

Die Anzeige oder Signalisierung dieser Informationen kann bei Endgeräten (analoges Endgerät, ISDN-Endgerät und Systemtelefon) erfolgen, die dieses Leistungsmerkmal unterstützen. Die MWI-Informationen von extern werden vom System transparent durchgereicht. Das bintec elmeg-Telefon zeigt bei einer vorliegenden MWI das Symbol eines Briefumschlags und einen im Telefon generierten Text sowie die Telefonnummer des Anrufers an.

Analoge Endgeräte

- Das Einschalten der MWI kann nur bei aufgelegtem Hörer erfolgen.

- Liegt eine Nachricht von einem Voice Mail System vor, erfolgt ein kurzer Anruf. Es können je nach Endgerät ein Symbol, ein im Telefon generierten Text sowie die Telefonnummer des Anrufers angezeigt werden. Wird eine MWI-Information gelöscht, erfolgt keine Signalisierung.
- Für das Endgerät muss CLIP eingerichtet und in der Konfigurierung freigeschaltet sein.
- Ein Rückruf zum Voice Mail System oder Rezeptionstelefon ist möglich, dabei wird die MWI-Information gelöscht.

ISDN Endgeräte

- Das Einschalten der MWI kann jederzeit (auch im Gespräch) erfolgen.
- Liegt eine Nachricht von einem Voice Mail System vor, erfolgt ein kurzer Anruf. Es können je nach Endgerät ein Symbol, ein im Telefon generierten Text sowie die Telefonnummer des Anrufers angezeigt werden. Wird eine MWI-Information gelöscht, erfolgt keine Signalisierung.
- Ein Rückruf zum Voice Mail System oder Rezeptionstelefon ist möglich, dabei wird die MWI-Information gelöscht.

Systemtelefone

- Das Einschalten der MWI kann jederzeit (auch im Gespräch) erfolgen. Die Rufnummer des Anrufers wird in die Anruferliste eingetragen. Im Display wird je nach Typ des Systemtelefons z. B. Externe Voice-Mail, Netbox Heute und der Name sowie die Rufnummer des Anrufers eingetragen. Zusätzlich blinkt die LED **Anruferliste**.
- Ein Rückruf zum Voice Mail System oder Rezeptionstelefon ist möglich, dabei wird die MWI-Information gelöscht.

Zimmertelefon

- Liegt eine Nachricht von einem Voice Mail System vor, wird nach dem Abheben des Hörers ein Sonderwählton signalisiert.

Rezeptionstelefon

- Von einem Rezeptionstelefon kann über eine Telefonprozedur die MWI-Information in einem Zimmertelefon ein und ausgeschaltet werden. Wird eine MWI Information in einem Zimmertelefon eingeschaltet, wird die Rufnummer des Rezeptionstelefons in die Anruferliste eingetragen, und der Sonderwählton eingeschaltet.

Ausschalten der MWI-Nachricht

- Manuelles Ausschalten über die Telefonprozedur vom Rezeptionstelefon.
- Anruf vom Rezeptionstelefon an das Zimmertelefon. Die MWI-Information wird im Gesprächszustand automatisch gelöscht.

- Ein Rückruf vom Zimmertelefon zum Rezeptionstelefon löscht die MWI-Information.

Hinweis

Dieses Leistungsmerkmal müssen Sie für Ihren ISDN-Anschluss beim Netzbetreiber beauftragen. Dort wird man Sie auch über die verfügbaren Dienste informieren. Die Information kann am internen ISDN-Endgerät nur angezeigt werden, wenn dem Endgerät in der Konfigurierung eine externe MSN zugeordnet wurde.

Nach einem Systemreset sind alle MWI-Informationen gelöscht.

Net Direct (Keypad)

Sie haben sich vor einiger Zeit das seinerzeit modernste Telefon gekauft. Seitdem sind im öffentlichen Netz jedoch viele neue Leistungsmerkmale hinzugekommen, die Sie nun nicht einfach durch einen Tastendruck nutzen können. Mit Hilfe der Funktion Keypad können Sie durch die Eingabe einer Tastenfolge auch von Ihrem ISDN- oder analogen Telefon aus aktuelle ISDN-Funktionen Ihres Netzbetreibers nutzen.

Die Funktion Keypad ermöglicht Ihnen durch die Eingabe von Zeichen- und Ziffernfolgen die Steuerung von Dienst oder Leistungsmerkmalen im Netz Ihres Netzbetreibers.

Hinweis

Das Leistungsmerkmal Keypad können Sie nur nutzen, wenn es von Ihrem Netzbetreiber unterstützt wird und für Ihren ISDN-Anschluss beauftragt ist. Haben Sie für einen internen Teilnehmer die automatische Amtsholung eingerichtet, können die Keypad-Funktionen nicht direkt genutzt werden. Schalten Sie die **Automatische Amtsholung** vorher aus oder wählen Sie die Stern-Taste, anschließend die Kennziffer für die manuelle Amtsholung (z. B. die 0) danach die Keypad-Wahl, beginnend mit der Stern- oder Raute-Taste.

Keypad-Funktionen können nur von Endgeräten aus erfolgen, denen in der Konfigurierung eine externe Mehrfachrufnummer (MSN) zugeordnet ist und die über die Keypad-Berechtigung verfügen.

Die Leistungsmerkmale ihres Netzbetreibers werden immer für die von Ihrem Endgerät mitgesendete Rufnummer (MSN) eingerichtet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Wechselsprechen empfangen	Wählen Sie aus, ob für diese Berechtigungsklasse Wechselsprech-Anrufe zu dem Systemtelefon erlaubt sind. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Durchsage	Wählen Sie aus, ob diese Berechtigungsklasse Durchsagen empfangen darf. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
MWI-Informationen empfangen	Wählen Sie aus, ob diese Berechtigungsklasse Informationen über vorhandene Nachrichten (MWI = Message Waiting Indication) empfangen kann. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Net Direct (Keypad)	Wählen Sie aus, ob Sie durch Eingabe einer Tastenfolge auch von älteren ISDN- oder analogen Telefon aus aktuelle ISDN-Funktionen Ihres Netzbetreibers nutzen wollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

14.2.2.3 Anwendungen

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Berechtigungsklassen**->**Anwendungen** werden zusätzliche Anwendungen eingerichtet.

Abb. 85: **Nummerierung->Benutzereinstellungen->Berechtigungsklassen->Anwendungen**

Das Menü **Nummerierung->Benutzereinstellungen->Berechtigungsklassen->Anwendungen** besteht aus folgenden Feldern:

Felder im Menü Berechtigung

Feld	Beschreibung
System-Telefonbuchnutzung	Wählen Sie aus, ob diese Berechtigungsklasse die Einträge im System-Telefonbuch nutzen darf und wenn ja, in welchem Umfang. Mögliche Werte: • *Ja, gemäß Wahlberechtigung* (Standardwert): Die Einträge des System-Telefonbuchs dürfen verwendet werden, sofern sie nicht außerhalb der konfigurierten Wahlberechtigung liegen. • *Ja, uneingeschränkt*: Die Einträge des System-Telefonbuchs dürfen uneingeschränkt verwendet werden. • *Nein*: Die Einträge des System-Telefonbuchs dürfen nicht verwendet werden.
Wartemusik (MoH)	Wählen Sie aus, ob und welche MoH (Music on Hold) verwendet werden soll. Mögliche Werte: • *Aus* (Standardwert): Ein gehaltener Anrufer soll keine Wartemusik hören.

Feld	Beschreibung
	• *<MoH-Wave-Datei>*: Ein gehaltener Anrufer soll die ausgewählte Wave-Datei als Wartemusik hören. • *MOH Intern 1* • *MOH Intern 2* • *MoH Wave 1 bis 8*
TFE-Berechtigung	Wählen Sie aus, ob diese Berechtigungsklasse mit der Türsprechstelle Verbindung aufnehmen darf. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TAPI	Wählen Sie aus, ob diese Berechtigungsklasse die TAPI-Funktionalitäten des Systems nutzen darf. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Verbindungsdaten speichern	Wählen Sie aus, ob die Verbindungsdaten dieser Berechtigungsklasse gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Gebührenübermittlung	Wählen Sie aus, ob die übermittelten Gebühreninformationen an Endgeräte dieser Berechtigungsklasse übermittelt werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

14.2.3 Parallelruf

Im Menü **Nummerierung**->**Benutzereinstellungen**->**Parallelruf** konfigurieren Sie, ob bei kommenden Anrufen auf eine interne Rufnummer an einer weiteren externen Rufnummer parallel signalisiert werden soll.

14.2.3.1 Bearbeiten oder Neu

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

Abb. 86: **Nummerierung->Benutzereinstellungen->Parallelruf->Neu**

Das Menü **Nummerierung->Benutzereinstellungen->Parallelruf->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Interne Rufnummer	Wählen Sie die interne Rufnummer aus, zu der das Leistungsmerkmal Parallelruf eingerichtet werden soll.
Externe Rufnummer	Geben Sie zu **Neue Rufnummer** die externe Telefonnummer ein, auf der ein Anruf parallel signalisiert werden soll. Sind unter **Benutzer->Grundeinstellungen->Externe Rufnummern** eine Mobilnummer und eine Rufnummer privat eingerichtet, werden diese unter **Konfigurierte Rufnummer privat** oder **Konfigurierte Mobilnummer** angezeigt und können ausgewählt werden.
Parallelruf	Wählen Sie aus, ob dieser Parallelruf-Eintrag aktiviert werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

14.3 Gruppen &Teams

In diesem Menü konfigurieren Sie die Teams Ihres Systems.

14.3.1 Teams

Im Menü **Nummerierung**->**Gruppen &Teams**->**Teams** konfigurieren Sie die Teams Ihres Systems.

Teams sind Gruppen von Personen, die gemeinsam an der Umsetzung eines Ziels arbeiten. In der Praxis bedeutet dies, dass alle Personen eines Teams unter einer gemeinsamen Rufnummer für externe und interne Anrufe erreichbar sind. In der TK-Anlage kann somit jedem Team von Telefonen / Endgeräten eine Rufnummer gezielt zugewiesen werden, so dass die Erreichbarkeit bei internen und externen Anrufen gewährleistet ist. Individuelle Strukturen von Unternehmen lassen sich über Teams abbilden. So können Abteilungen wie Service, Verkauf, Entwicklung über Teamrufnummern von intern oder extern gezielt gerufen werden. Innerhalb eines Teams kann der Ruf beispielsweise gleichzeitig an allen oder zunächst an einem Telefon, dann zusätzlich an einem Zweiten, usw. signalisiert werden. In einem Team können auch Anrufbeantworter oder Voice-Systeme genutzt werden.

Jedem Team sind vier Team-Anrufvarianten zugeordnet. Die Umschaltung der Anrufvariante kann manuell oder über einen der Kalender erfolgen.

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um ein neues Team einzurichten.

14.3.1.1 Allgemein

Im Menü **Nummerierung**->**Gruppen &Teams**->**Teams**->**Allgemein** werden die grundlegenden Bedingungen im Team konfiguriert. Dazu gehören der Name des Teams und die interne Teamrufnummer.

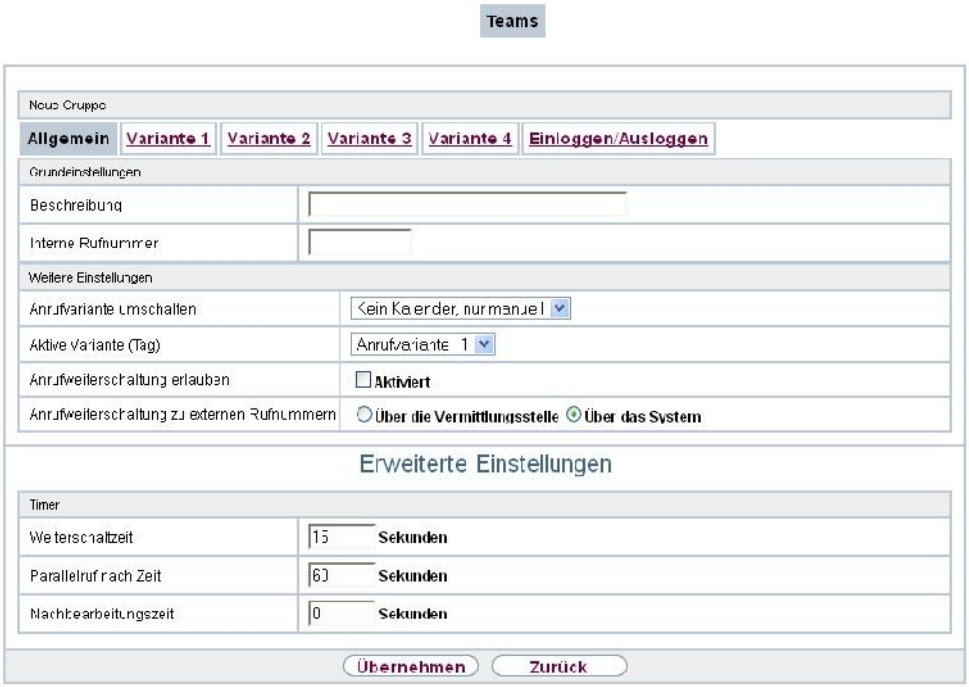


Abb. 87: **Nummerierung->Gruppen &Teams->Teams->Allgemein**

Für interne Teamanrufe kann in der Konfiguration dem Team eine Team-Rufnummer und ein Team-Name zugeordnet werden. Wird eine Teamrufnummer gewählt, sieht der Anrufer solange den Team-Namen, bis ein Team-Teilnehmer das Gespräch angenommen hat. Dann wird der Name des Team-Teilnehmers angezeigt.

Das Menü **Nummerierung->Gruppen &Teams->Teams->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Team ein.
Interne Rufnummer	Geben Sie die interne Rufnummer des Teams ein.

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Anrufvariante umschalten	Legen Sie fest, ob die für das Team eingerichtete Anrufvariante manuell über das Telefon oder über den Kalender eingeschaltet werden soll. Hierzu müssen der Kalender und die Schaltzeiten

Feld	Beschreibung
	zuvor konfiguriert werden. Sie können für jedes Team bis zu vier Anrufvarianten im Menü **Nummerierung**->**Gruppen &Teams**->**Teams**->**Neu**->**Variante1-4** einrichten. Mögliche Werte: • *Kein Kalender, nur manuell*: Die manuelle Umschaltung wird aktiv. • *<Kalender>*: Wählen Sie einen der konfigurierten Kalender aus.
Aktive Variante (Tag)	Wählen Sie die Anrufvariante aus, die zurzeit aktiv sein soll. Ist eine Umschaltung über den Kalender eingerichtet, wird diese Einstellung zeitgerecht wieder umgeschaltet.
Anrufweiterschaltung erlauben	Legen Sie fest, ob ein Anrufweiterschaltung für das Team durchgeführt werden darf. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Anrufweiterschaltung zu externen Rufnummern	Wählen Sie aus, ob eine Anrufweiterschaltung im System selbst (**Über das System**) oder über eine Vermittlungsstelle (Provider, **Über die Vermittlungsstelle**) erfolgen soll. Beachten Sie hierzu, dass bei einer Anrufweiterschaltung im System zwei externe Verbindungen belegt werden.

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

Felder im Menü Timer

Feld	Beschreibung
Weiterschaltzeit	Geben Sie hier die **Weiterschaltzeit** ein, nach der eine Anrufweiterschaltung nach Zeit im Team ausgeführt werden soll. Der Standardwert ist *15* Sekunden.
Parallelruf nach Zeit	Beim Teamruf linear und rotierend besteht die Möglichkeit, dass nach einer eingestellten Zeit alle Teamteilnehmer gleichzeitig gerufen werden. Der Standardwert ist *60* Sekunden.

Feld	Beschreibung
Nachbearbeitungszeit	Diese Einstellung ist nur bei **Signalisierung** *Gleichmäßig* aktiv. Jedem Teilnehmer, der ein Gespräch beendet hat, wird eine für jedes Team eingerichtete **Nachbearbeitungszeit** eingerichtet, in der er keinen weiteren Anruf erhält. Anrufe, die der Teilnehmer nicht über das Team sondern über seine Rufnummer erhält und selbst eingeleitete Gespräche, werden nicht mit in die Zeit eingerechnet. Der Standardwert ist *0* Sekunden, der Bereich *0* - *999* Sekunden.

14.3.1.2 Variante 1 - 4

Im Menü **Nummerierung**->**Gruppen &Teams**->**Teams**->**Variante 1-4** konfigurieren Sie die vier Anrufvarianten eines Teams. Sie können bis zu vier verschiedene Anrufvarianten für jedes Team einrichten. Dazu weisen Sie der Anrufvariante entweder interne Rufnummern oder eine externe Rufnummer zu und definieren, wie ein kommender Anruf innerhalb des Teams signalisiert werdens soll.

Interne Rufnummern eines Teams

Wählen Sie unter **Interne Zuordnung** die internen Teilnehmer aus, die diesem Team angehören sollen. Möchten Sie einen der Team-Teilnehmer vorübergehend von der Anrufsignalisierung ausschließen (z. B. Ein Team-Teilnehmer ist im Urlaub) können Sie diesen **Ausloggen**. Die Teamanrufe werden nicht bei den ausgeloggten Teilnehmern signalisiert. Das Ein- oder Ausloggen kann jeder Teamteilnehmer auch über eine Kennziffer des Systems selbst steuern.

Für interne Teamanrufe kann in der Konfiguration dem Team eine Team-Rufnummer und ein Team-Name zugeordnet werden. Wird eine Teamrufnummer gewählt, sieht der Anrufer solange den Team-Namen, bis ein Team-Teilnehmer das Gespräch angenommen hat. Dann wird der Name des Team-Teilnehmers angezeigt. Der Anruf zu einem Team kann gleichzeitig, linear, rotierend, aufbauend oder parallel nach Zeit erfolgen. Beim Teamruf linear und rotierend besteht die Möglichkeit, dass nach einer eingestellten Zeit (1 - 99 Sekunden) alle Team-Teilnehmer gleichzeitig gerufen werden.

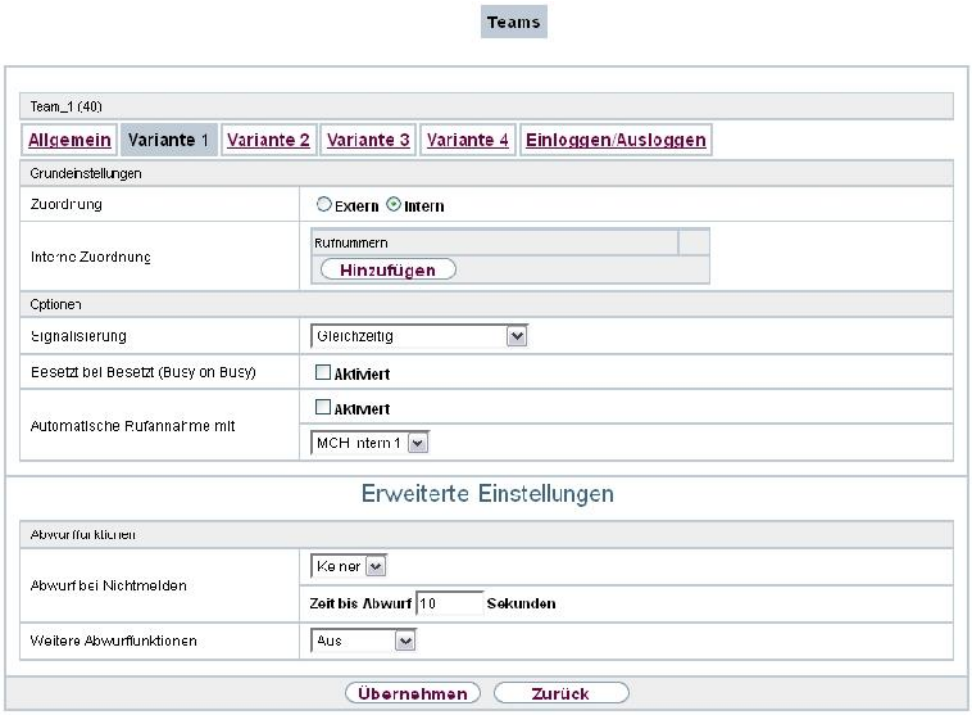


Abb. 88: **Nummerierung->Gruppen &Teams->Teams->Variante**

Das Menü **Nummerierung->Gruppen &Teams->Teams->Variante** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Zuordnung	Sie können jedem Team mehrere interne Rufnummern oder je eine externe Rufnummer zuordnen. Legen Sie fest, ob die Anrufe für ein Team bei den internen Teilnehmern oder bei dem externen Teilnehmer signalisiert werden sollen. Mögliche Werte: • `Extern`: Die eingetragene externe Rufnummer wird gerufen. • `Intern` (Standardwert): Die Teilnehmer, die den ausgewählten Rufnummern zugeordnet sind, werden entsprechend der eingestellten Signalisierung gerufen.
Interne Zuordnung	Nur bei **Zuordnung** = `Intern` Wählen Sie die internen Teilnehmer des Teams aus.

Feld	Beschreibung
	Fügen Sie mit **Hinzufügen** weitere interne Rufnummern hinzu.
Externe Zuordnung	Nur bei **Zuordnung** = *Extern* Geben Sie die Rufnummer des externen Teilnehmers ein.
Zuordnung für Abwurf und Tarife	Nur bei **Zuordnung** = *Extern* Die Kosten für den Anruf und die Belegung eines externen Anschlusses erfolgt über den ausgewählten internen Teilnehmer.

Automatische Rufannahme im Team

Sie möchten dass ein Anrufer während der Rufsignalisierung bereits angenommen wird und nicht den Rufton (Freiton) hört. Kein Problem, wenn Sie die automatische Rufannahme bei Teamanrufen nutzen. Der Anrufer wird in diesem Fall vom System automatisch angenommen und hört eine Ansage oder eine Wartemusik des Systems. Während dieser Zeit erfolgt die Signalisierung des Anrufes bei den eingetragenen Team-Teilnehmern. Nimmt ein Teilnehmer den Ruf an, wird die Verbindung zum Anrufer hergestellt.

Wird ein Team angerufen, kann in der Konfigurierung festgelegt werden, dass der Anruf automatisch angenommen wird und der Anrufer hört eine Ansage oder Musik. Der oder die Zielteilnehmer werden während dieser Zeit weitergerufen. Nach dem Abheben des Hörers werden Ansage oder Musik abgeschaltet und die Teilnehmer sind miteinander verbunden.

Mögliche Einstellungen für die automatische Rufannahme:

- *Gleichzeitig* : Alle zugeordneten Endgeräte werden gleichzeitig gerufen. Ist ein Endgerät besetzt, kann angeklopft werden.
- *Linear*: Alle zugeordneten Endgeräte werden nacheinander in der Reihenfolge des Eintrages in der Konfigurierung gerufen. Wenn ein Endgerät besetzt ist, wird das nächste freie Endgerät gerufen. Je Teilnehmer wird der Anruf ca. 15 Sekunden signalisiert. Diese Zeit ist in der Konfigurierung (je Team) zwischen 1 und 99 Sekunden einstellbar. Wenn Teilnehmer telefonieren oder ausgeloggt sind, erfolgt keine Weiterschaltungszeit für diese Teilnehmer.
- *Rotierend*: Dieser Ruf ist ein Sonderfall des linearen Rufes. Nachdem alle Endgeräte gerufen wurden, beginnt die Rufsignalisierung wieder beim ersten eingetragenen Endgerät. Der Ruf wird solange signalisiert, bis der Anrufer auflegt oder der Ruf von der Vermittlungsstelle beendet wird (nach ca. zwei Minuten).
- *Aufbauend*: Die Endgeräte werden in der Reihenfolge des Eintrages in die Teilnehmerliste gerufen. Jedes bereits gerufene Endgerät wird weiter gerufen, bis alle eingetragenen Endgeräte gerufen werden.

- *Linear, parallel nach Zeit* oder *Rotierend, parallel nach Zeit*: Für den Teamruf ist rotierend oder linear eingerichtet. Nach Ablauf der eingerichteten Zeiten können alle Teamteilnehmer parallel (gleichzeitig) gerufen werden. Beispiel: Voraussetzung ist, dass die Summe der Weiterschaltzeiten größer ist als die Zeit **parallel nach Zeit**. 4 Teilnehmer befinden sich in einem Team. Die Weiterschaltzeit beträgt für jeden Teilnehmer 10 Sekunden, zusammen 40 Sekunden. Die Zeit **parallel nach Zeit** ist auf 38 Sekunden eingestellt. Jeder der Teilnehmer wird gerufen werden. Loggt sich ein Teilnehmer aus dem Team aus oder ist besetzt, beträgt die Weiterschaltzeit nur noch 30 Sekunden. dann wird der Ruf **parallel nach Zeit** nicht mehr ausgeführt.
- *Gleichmäßig*: Die gleichmäßige Verteilung entspricht der **SignalisierungRotierend** und bewirkt, dass alle Teilnehmer eines Teams die gleiche Anzahl von Anrufen erhalten. Jedem Teilnehmer der ein Gespräch beendet hat wird eine für das Team / Teilnehmer eingerichtete **Nachbearbeitungszeit** (0...999 Sekunden) eingerichtet, in der er keinen weiteren Anruf erhält. Anrufe, die der Teilnehmer nicht über das Team sondern über seine Rufnummer erhält und selbst eingeleitete Gespräche, werden nicht mit in die gleichmäßige Verteilung eingerechnet. Die gleichmäßige Verteilung beginnt mit dem Teilnehmer, der am längsten keinen Anruf erhalten hat, beim Neustart mit dem ersten in der Teilnehmerliste eingetragenen Teilnehmer. Ein Teilnehmer, der sich aus dem Team ausgeloggt hat (Kennziffer oder Funktionstaste), wird in der gleichmäßigen Verteilung nicht mehr berücksichtigt. Nach einer Stromunterbrechung des Systems wird die bestehende Berechnung zur **Gleichmäßigen Verteilung** gelöscht und der Vorgang startet neu. Befinden Sich alle Teamteilnehmer in der **Nachbearbeitungszeit**, werden externe Anrufe auf das eingerichtete Abwurfziel geschaltet, interne Anrufer hören den Besetztton. Wird für mehrere Teamteilnehmer die gleiche Zeit nach Beenden des letzten Anrufes errechnet, gilt die Reihenfolge der Einträge in der **Interne Zuordnung**.

Felder im Menü Optionen

Feld	Beschreibung
Signalisierung	Sie können Teilnehmer eines Teams mit dem Sammelruf rufen. Mögliche Werte: • *Gleichzeitig* (Standardwert) • *Linear* • *Rotierend* • *Aufbauend* • *Linear, parallel nach Zeit* • *Rotierend, parallel nach Zeit* • *Gleichmäßig*
Besetzt bei Besetzt (Busy on Busy)	Wählen Sie aus, ob für dieses Anrufvariante das Leistungsmerkmal "Busy on Busy" aktiviert sein soll.

Feld	Beschreibung
	Führt ein Teilnehmer eines Teams ein Gespräch, so können Sie entscheiden, ob weitere Anrufe für dieses Team signalisiert werden sollen. Ist die Funktion "Busy on Busy" für dieses Team eingerichtet, so erhalten weitere Anrufer "besetzt" signalisiert. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Automatische Rufannahme mit	Wählen Sie aus, ob ein kommender Anruf automatisch angenommen werden soll und der Anrufer die gewünschte Wartemusik oder Ansage hören soll. Dabei erfolgt die Signalisierung des Anrufes im Team weiter. Die Kosten für die bereits bestehende Verbindung trägt der Anrufer. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wählen Sie außerdem die gewünschte Wartemusik bzw. Ansage aus. Mögliche Werte: • *<Datei_x>* • *MOH Intern 1* • *MOH Intern 2* • *MoH Wave 1 bis 8*

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

Felder im Menü Abwurffunktionen

Feld	Beschreibung
Abwurf bei Nichtmelden	Wählen Sie aus, ob und auf welches Team ein kommender Anruf bei Nichtmelden abgeworfen werden soll. Mögliche Werte: • *Keiner* • *<Team>* Geben Sie außerdem die Zeit ein, nach der der Abwurf ausgeführt werden soll.

Feld	Beschreibung
Weitere Abwurffunktionen	Wählen Sie aus, ob und auf welche Abwurfvariante ein kommender Anruf geleitet werden soll. Mögliche Werte: • *Aus*: Es werden keine weiteren Abwurfvarianten verwendet. • *Sofort*: Der kommende Anruf wird sofort auf die in **Sofort** ausgewählte Abwurffunktion umgeleitet. • *Bei Besetzt*: Der kommende Anruf wird auf die in **Bei Besetzt** ausgewählte Abwurffunktion umgeleitet.
Sofort	Nur bei **Weitere Abwurffunktionen** = *Sofort* Wählen Sie die Abwurffunktion für sofortigen Abwurf aus. Die Abwurffunktionen konfigurieren Sie in **Anwendungen**->**Abwurf**->**Abwurffunktionen**.
Bei Besetzt	Nur bei **Weitere Abwurffunktionen** = *Bei Besetzt* Wählen Sie die Abwurffunktion für Abwurf bei Besetzt aus. Die Abwurffunktionen konfigurieren Sie in **Anwendungen**->**Abwurf**->**Abwurffunktionen**.
Besetzt beginnend bei	Nur bei **Weitere Abwurffunktionen** = *Bei Besetzt* Wählen Sie aus, ab welcher Anzahl Teilnehmer das Team als besetzt gilt.

14.3.1.3 Einloggen/Ausloggen

Im Menü **Nummerierung**->**Gruppen &Teams**->**Teams**->**Einloggen/Ausloggen** werden die einzelnen Teammitglieder an- oder abgemeldet.

Abb. 89: **Nummerierung->Gruppen &Teams->Teams->Einloggen/Ausloggen**

Das Menü **Nummerierung->Gruppen &Teams->Teams->Einloggen/Ausloggen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Rufnummern	Zeigt die interne Rufnummer der zugewiesenen Teammitglider an.
Status	Wählen Sie aus, ob das Teammitglied am Team angemeldet ist. Mit Auswahl von `Angemeldet` wird das Teammitglied angemeldet.

14.4 Rufverteilung

In diesem Menü konfigurieren Sie die interne Weiterleitung aller kommenden Anrufe.

14.4.1 Anrufzuordnung

Im Menü **Nummerierung->Rufverteilung->Anrufzuordnung** konfigurieren Sie die Zuordnung der kommenden Anrufe zu den gewünschten internen Rufnummern.

Unter Anrufzuordnung ordnen Sie die unter **Externe Rufnummern** eingetragenen Rufnummern z. B. den Teams oder einer internen Rufnummer zu.

14.4.1.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Abb. 90: **Nummerierung->Rufverteilung->Anrufzuordnung->**

Das Menü **Nummerierung->Rufverteilung->Anrufzuordnung->** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
<Name des Rufnummerneintrags>	Zeigt die konfigurierte Rufnummer an.
Externer Anschluss	Zeigt den externen Anschluss an, für den Anrufzuordnung konfiguriert wird.
Zuordnung	Wählen Sie die interne Rufnummer oder die gewünschte Funktion aus, zu der kommende Anrufe über die in **Externer Anschluss** ausgewählte Leitung zugewiesen werden sollen. Mögliche Werte: • *Interne Nummer* (Standardwert): Für die Zuordnung auf ein Team wird die interne Rufnummer für das Team ausgewählt. • *Call Through* • *Abwurfanwendung* • *Fernzugang Telefonie* • *ISDN-Login* • *Service-Login* • *Mini-Callcenter*

Felder im Menü Einstellungen interne Rufnummer und Abwurf

Feld	Beschreibung
Interne Rufnummer	Nur für **Zuordnung** = *Interne Rufnummer* Wählen Sie die interne Rufnummer aus, zu der kommende Anrufe über die in **Externer Anschluss** ausgewählte Leitung zugewiesen werden sollen.
Abwurfanwendung	Nur für **Zuordnung** = *Abwurfanwendung* Wählen Sie die gewünschte Abwurfanwendung, die der Rufnummer zugeordnet werden soll. Abwurfanwendungen konfigurieren Sie im Menü **Anwendungen**->**Abwurf**->**Abwurfanwendungen**.
Aktive Variante (Tag)	Nur für Abwurfanwendung = *<konfigurierte Abwurfanwendung>* Wählen Sie die Variante der Abwurfanwendung aus, die zurzeit aktiv sein soll. Ist eine Umschaltung der Varianten über den Kalender eingerichtet, wird diese Einstellung zeitgerecht wieder umgeschaltet. Mögliche Werte: • *Variante 1* • *Variante 2* • *Variante 3* • *Variante 4*

Felder im Menü Call Through Einstellungen

Feld	Beschreibung
Zugangsberechtigung	Nur für **Zuordnung** = *Call Through* Legen Sie die Berechtigung fest, nach der die Funktion Call Through freigegeben wird. Mögliche Werte: • *Rufnummernüberprüfung*: Nach Überprüfung der eingegebenen Rufnummer mit dem Eintrag im Telefonbuch des Systems oder mit Rufnummerneinträgen des Benutzers (**Mobilnummer** und **Rufnummer privat**) erfolgt die Freigabe der Wahl.

Feld	Beschreibung
	• *Rufnummern und PIN*: Nach Überprüfung der eingegebenen Rufnummer mit dem Eintrag im Telefonbuch des Systems oder mit Rufnummerneinträgen des Benutzers (**Mobilnummer** und **Rufnummer privat**) UND Eingabe der PIN erfolgt die Freigabe der Wahl. • *PIN*: Nach Eingabe der PIN erfolgt die Freigabe der Wahl. • *Rufnummer oder PIN*: Nach Überprüfung der eingegebenen Rufnummer mit dem Eintrag im Telefonbuch des Systems oder mit Rufnummerneinträgen des Benutzers (**Mobilnummer** und **Rufnummer privat**) ODER Eingabe der PIN erfolgt die Freigabe der Wahl.
PIN (6-stellig)	Nur für **Zugangsberechtigung** = *Rufnummern und PIN*, *PIN*, *Rufnummer oder PIN* Das System überprüft die Berechtigung des Anrufers für die Weiterwahl und schaltet einen simulierten externen Wählton für die Wahl an. Die Berechtigung ist gegeben, wenn der Anrufer die richtige 6-stellige PIN eingegeben hat.
Einstellungen interne Rufnummer und Abwurf	Wählen Sie den internen Teilnehmer aus, über den Call Through erfolgen soll. Eine der Telefonnummern des Systems wird in der Konfiguration für Call Through festgelegt. Ein externer Anrufer über diese Telefonnummer erhält zuerst einen Aufmerkton des Systems.

14.4.2 Abwurf bei Falschwahl

Im Menü **Nummerierung**->**Rufverteilung**->**Abwurf bei Falschwahl** legen Sie für jeden externen Anschluss den Teilnehmer oder das Team fest, zu dem der Anruf erfolgen soll, falls

- ein kommender Anruf eine falsche oder unvollständige Rufnummer / Durchwahl besitzt.
- alle Teilnehmer des angewählten Teams oder Callcenters ausgeloggt sind.
- sich alle Teilnehmer des angewählten Callcenters in der Nachbearbeitung befinden.

14.4.2.1 Bearbeiten

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

Abb. 91: **Nummerierung**->**Rufverteilung**->**Abwurf bei Falschwahl**->

Das Menü **Nummerierung**->**Rufverteilung**->**Abwurf bei Falschwahl**-> besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Externer Anschluss	Zeigt den externen Anschluss an, für den Abwurf bei Falschwahl konfiguriert wird.
Abwurf auf Rufnummer	Wählen Sie die Art des Abwurfs aus. Mögliche Werte: • *Keine*: Hier erfolgt kein Abwurf, der Anrufer erhält "besetzt". • *Globale Einstellungen*: Der Abwurf erfolgt wie unter **Systemverwaltung**->**Globale Einstellungen**->**System**->**Abwurf auf Rufnummer** eingetragen. • *<Interne Rufnummer eines Benutzers oder eines Teams>*: Der Abwurf erfolgt auf diesen Benutzer bzw. dieses Team.

Kapitel 15 Endgeräte

15.1 elmeg Systemtelefone

In diesem Menü nehmen Sie die Zuordnung der konfigurierten internen Rufnummern zu den Endgeräten vor und stellen weitere Funktionen je nach Endgerätetyp ein.

Die Endgeräte (bei DECT-System die Basisstationen) sind in der Spalte **Beschreibung** alphabetisch sortiert. Sie können in jeder beliebigen anderen Spalte auf den Spaltentitel klicken und die Einträge in aufsteigender oder in absteigender Reihenfolge sortieren lassen.

Angeschlossene Telefone bzw. DECT-Basisstationen werden automatisch erkannt und in der jeweiligen Übersicht aufgelistet, können aber vor dem Anschließen auch manuell konfiguriert werden.

15.1.1 Systemtelefon

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon** wird eine Liste der Systemtelefone angezeigt. Sie sehen sowohl die manuell konfigurierten als auch die automatisch erkannten Telefone.

Die Grundkonfiguration ist bei allen Telefonen gleich. Unterschiede gibt es im Leistungsumfang und in der Konfiguration einiger Leistungsmerkmale (abhängig vom Typ des Telefons). Können Sie Leistungsmerkmale mit dem ausgewählten Telefon nicht nutzen, werden diese auch nicht zur Konfigurierung angeboten.

Sie können das Systemtelefon je nach Typ am internen ISDN-, S0-, Up0- oder Ethernet-Anschluss des Systems anschließen. Das Systemtelefon stellt Ihnen in Verbindung mit dem System systemtypische Leistungsmerkmale zur Verfügung. Zum Beispiel:

- Wahl aus dem Telefonbuch des Systems
- Durchsage und Wechselsprechen mit anderen Systemtelefonen am System
- Funktionstasten zur Steuerung von Leistungsmerkmalen des Systems (Anrufvarianten schalten, Ein-/Ausloggen in Teams, Linientasten, Leitungstasten). Der Status eingestellter Leistungsmerkmale kann über Leuchtdioden, die den einzelnen Funktionstasten zugeordnet sind, angezeigt werden.
- Zugriff auf das Systemmenü des Systems. In diesem Menü werden weitere Funktionen vom System bereitgestellt.

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

Wählen Sie das Symbol  , um vorhandene Einträge zu kopieren. Das Kopieren eines Eintrags kann nützlich sein, wenn Sie einen Eintrag anlegen wollen, der sich nur in wenigen Parametern von einem bereits vorhandenen Eintrag unterscheidet. In diesem Fall kopieren Sie den Eintrag und ändern Sie die gewünschten Parameter.

Wählen Sie die Schaltfläche **Neu**, um ein neues Systemtelefon manuell einzurichten.

Hinweis

Konfigurationsänderungen werden frühestens 30 Sekunden nach dem Bestätigen der Änderung mit der Schaltfläche **Übernehmen** in die Systemtelefone übertragen.

15.1.1.1 Allgemein

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Allgemein** nehmen Sie die grundlegenden Einstellungen eines Systemtelefons vor.

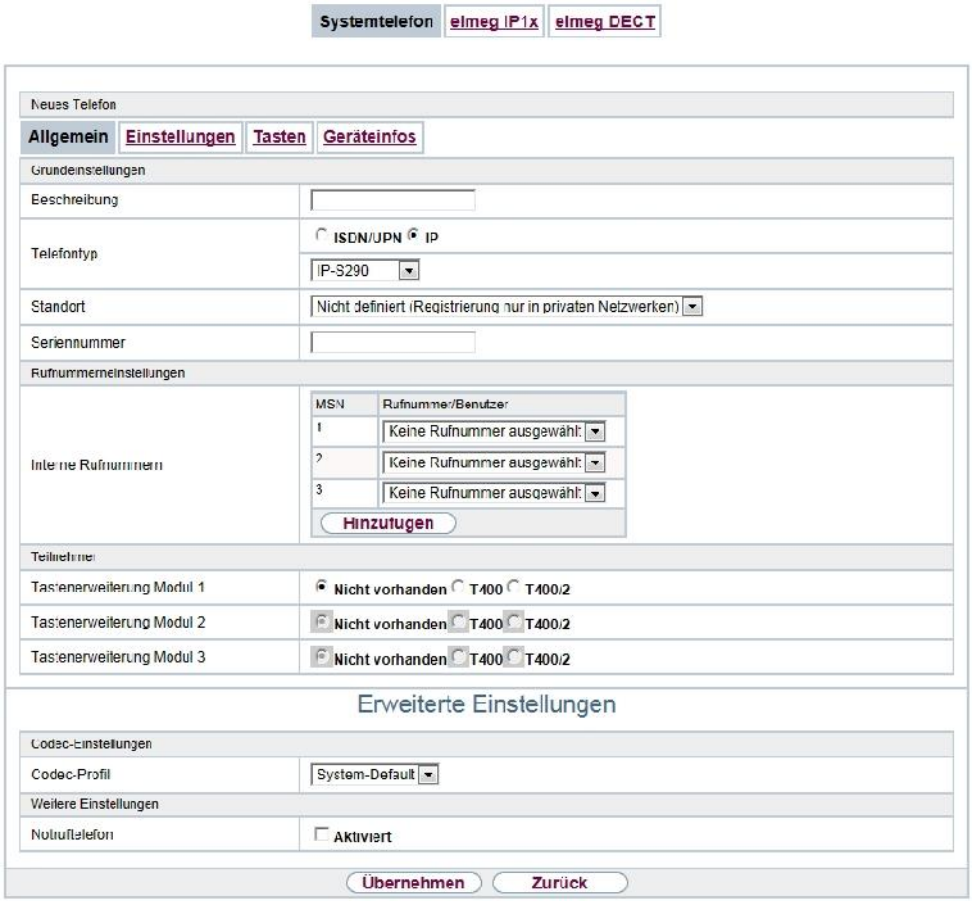


Abb. 92: **Endgeräte->elmeg Systemtelefone->Systemtelefon->Allgemein**

Telefontyp

Es können verschiedene Typen von Telefonen konfiguriert werden.

Werden die Systemtelefone vorab im System mit Typ und Seriennummer konfiguriert, erkennt das System das Systemtelefon nach dem Anschalten an den Anschluss. Dann wird die für dieses Systemtelefon erstellte Konfigurierung vom System in das Systemtelefon übertragen.

Alternativ können Sie ein Systemtelefon in Ihrer Telefonanlage anlegen, den passenden Telefontyp wählen und eine MSN vergeben. Wenn Sie ein Telefon mit Werkseinstellungen an Ihre Telefonanlage anschließen, meldet sich das Telefon mit der Frage nach der Sprache und der ersten MSN. Wenn Sie im Systemtelefon die Sprache eingeben und die MSN, die Sie in der Telefonanlage konfiguriert haben, überträgt die Telefonanlage die Konfiguration zum Telefon.

Wird das Systemtelefon entfernt, erkennt das System dieses und kennzeichnet den Eintrag im System mit einem roten Pfeil. Wird anschließend ein anderes Systemtelefon des gleichen Typs mit dem Anschluss verbunden, erkennt das System dieses und weist dem erkannten Systemtelefon die entsprechende Konfiguration zu. Das Systemtelefon erhält somit die gleiche Konfiguration wie sein Vorgänger, trotz abweichender Seriennummer. Lediglich die erste MSN muss identisch auf dem Systemtelefon und im System eingetragen sein.

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Um das Telefon im System eindeutig zu identifizieren, geben Sie eine Beschreibung für das Telefon ein.
Telefontyp	Zeigt den Typ des angeschlossenen Telefons an. Wenn die Schnittstelle konfiguriert ist, liest das System automatisch den Typ aus. Das Feld ist anschließend nicht mehr editierbar, sofern ein Telefon angeschlossen ist. Mögliche Werte: • *ISDN/UPN* • *IP* Bei **Telefontyp** = *ISDN/UPN*: Zeigt die Produktbezeichnung des Systemtelefons an. Mögliche Werte: • *CS290* • *CS290-U* • *CS400xt* • *CS410* • *CS410-U* • *S530* • *S560* Bei **Telefontyp** = *IP*: Zeigt die Produktbezeichnung des Systemtelefons an. Mögliche Werte:

Feld	Beschreibung
	• *IP-S290* • *IP-S290plus* • *IP-S400*
Standort	Nur für **Telefontyp** = *IP* Wählen Sie den Standort des Telefons aus. Standorte definieren Sie im Menü **VoIP**->**Einstellungen**->**Standorte**. Abhängig von der Einstellung in diesem Menü wird das Standardverhalten für die Registrierung von VoIP-Teilnehmern zur Auswahl angezeigt, für die kein Standort definiert werden soll. Mögliche Werte: • *Nicht definiert (Uneingeschränkte Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer dennoch registriert. • *Nicht definiert (Keine Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nicht registriert. • *Nicht definiert (Registrierung nur in privaten Netzwerken)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nur registriert, wenn er sich im privaten Netzwerk befindet. • *<Standort>*: Es wird ein definierter Standort ausgewählt. Der Teilnehmer wird nur registriert, wenn er sich an diesem Standort befindet.
Schnittstelle	Nur für **Telefontyp** = *ISDN/UPN* Zeigt die Schnittstelle an, an der das Endgerät angeschlossen ist. Wenn die Schnittstelle konfiguriert ist, liest das System automatisch die Schnittstelle aus. Das Feld ist anschließend nicht mehr editierbar, sofern ein Telefon angeschlossen ist. Mögliche Werte: • *Keine* • *<Schnittstellenbezeichnung>*
Seriennummer	Zeigt die Seriennummer des Geräts an. Wenn die Schnittstelle konfiguriert ist, liest das System automatisch die Seriennummer

Feld	Beschreibung
	aus. Das Feld ist anschließend nicht mehr editierbar.

Felder im Menü Rufnummerneinstellungen

Feld	Beschreibung
Interne Rufnummern	Wählen Sie die internen Rufnummern für dieses Endgerät aus. Sie können für 10 MSNs interne Rufnummern zuweisen. Standardmäßig können für Systemtelefone bis zu drei MSNs vergeben werden. Für Endgeräte der Serien 290 sind bis zu drei MSNs verfügbar. Für Endgeräte der Serie S5x0 sind bis zu fünf MSNs verfügbar. Für Endgeräte der Serien CS400 und 4xx sind bis zu 10 MSNs verfügbar. Beachten Sie, dass zum ordnungsgemäßen Betrieb des Telefons mindestens die erste MSN im System eingetragen sein muss. Mögliche Werte: • *Keine freie Leitung verfügbar*: Alle konfigurierten internen Rufnummern sind schon in Verwendung. Konfigurieren Sie zunächst einen weiteren Benutzer mit internen Rufnummern. • *Keine Rufnummer ausgewählt*: Dieser MSN soll keine interne Rufnummer zugewiesen werden. • *<Interne Rufnummer>*: Wählen Sie eine der vorhandenen Rufnummern der konfigurierten Benutzer aus.

Tastenerweiterungen

Die Tastenerweiterung T400 (verfügbar für die Telefone der CS4xx-Serie und für IP-S400) besitzt 20 Tasten mit Leuchtdioden, die Sie in zwei Ebenen als Funktionstasten nutzen können. Die Leuchtdioden sind der ersten Tastenebene zugeordnet. Zwei weitere Leuchtdioden sind für die Anzeige zusätzlicher Informationen realisiert. Sie können bis zu drei Tastenerweiterungen hintereinander (kaskadierend) an Ihrem Telefon anschließen. Ab der zweiten Tastenerweiterung ist der Einsatz eines Steckernetzgerätes notwendig.

Die Tastenerweiterung T400/2 (verfügbar für die Telefone der CS4xx-Serie und für IP-S400) besitzt 10 Tasten mit Leuchtdioden, die Sie in zwei Ebenen als Funktionstasten nutzen können. Die Leuchtdioden sind der ersten Tastenebene zugeordnet. Zwei weitere Leuchtdioden sind für die Anzeige zusätzlicher Informationen realisiert.

Die Tastenerweiterung T500 (verfügbar für die Telefone S530 und S560) besitzt 30 Tasten,

die Sie in zwei Ebenen als Funktionstasten nutzen können. Rechts neben jeder Taste zeigen zwei Leuchtdioden an, welche Ebene aktiv ist. Sie können bis zu drei Tastenerweiterungen hintereinander (kaskadierend) an Ihrem Telefon anschließen. Ab der ersten Tastenerweiterung ist der Einsatz eines Steckernetzgerätes notwendig.

Felder im Menü Teilnehmer

Feld	Beschreibung
Tastenerweiterung Modul 1 - 3	Zeigt an, ob Sie das Systemtelefon mit einem Tastenerweiterungsmodul betreiben. Mögliche Werte (je nach **Telefontyp**): • *Nicht vorhanden* • *T400* • *T400/2* • *T500*

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

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Profil	Wählen Sie das Codec-Profil aus, das verwendet werden soll, wenn über eine VoIP-Leitung verbunden wird. Codec-Profile konfigurieren Sie im Menü **VoIP**->**Einstellungen**->**Codec-Profile**

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Notruftelefon	Systemtelefone Ihres Systems können als Notruftelefone eingerichtet werden. Sie können diese Funktion nur nutzen, wenn ihr System über externe ISDN-Anschlüsse verfügt. Sie können dann sofort mit der externen Wahl beginnen, egal ob der externe ISDN-Anschluss frei oder besetzt ist. Sind die externen Anschlüsse bereits benutzt, wird ein B-Kanal eines Anschlusses freigeschaltet, und auf diesem B-Kanal telefonierende Gesprächspartner hören den Besetztton. Ein bereits bestehender Notruf wird nicht unterbrochen. Dieses Leistungsmerkmal können Sie unabhängig vom Leistungsmerkmal Vorrang für Notrufe nutzen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

15.1.1.2 Einstellungen

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Einstellungen** können Sie bestimmte Leistungsmerkmale und Funktionen für dieses Systemtelefon freischalten.

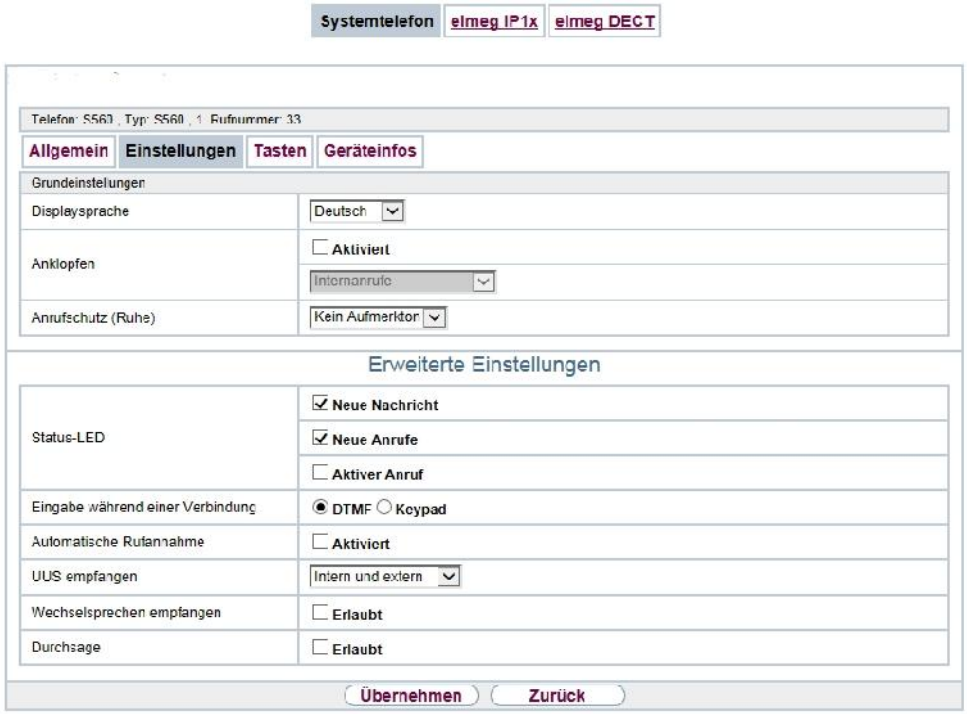


Abb. 93: **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Einstellungen**

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Displaysprache	Wählen Sie die Sprache für das Display Ihres Telefons aus. Mögliche Werte: • *Deutsch*

Feld	Beschreibung
	• *Niederländisch* : Nicht für **S530** und **S560** • *Englisch* • *Italienisch* • *Dänisch*: Nicht für **S530** und **S560** • *Spanisch*: Nicht für **S530** und **S560** • *Schwedisch*: Nicht für **S530** und **S560** • *Französisch*: Nicht für **S530** und **S560** • *Portugues*: Nicht für **S530** und **S560** • *Cesko*: Nicht für **S530** und **S560** • *Norwegisch*: Nicht für **S530** und **S560** • *Griechisch*: Nicht für **S530**, **S560**, **CS290**, **CS290-U**, **IP-S290**, **IP-S290plus** • *Isländisch*: Nicht für **S530**, **S560**, **CS400**, **CS410**, **CS410-U**, **IP-S400** • *Polnisch*: Nicht für **S530** und **S560** • *Ungarisch*: Nicht für **S530** und **S560** • *Russisch*: Nicht für **S530**, **S560**, **CS290**, **CS290-U**, **IP-S290**, **IP-S290plus**
Headset Unterstützung	Nicht für **S530** und **S560**. Wählen Sie aus, ob das Headset Anrufe automatisch entgegennehmen soll. **Hinweis** Wenn Sie ein Headset verwenden wollen, müssen Sie in Ihrer Telefonanlage eine Headset-Taste und eine Taste für die automatische Rufannahme konfigurieren. Am Systemtelefon müssen Sie einen Headset-Typ auswählen und die Taste für die automatische Rufannahme aktivieren.
Anklopfen	Wählen Sie aus, ob ein weiterer Anruf für dieses Telefon durch einen Anklopfton oder eine Displayanzeige signalisiert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv. Wenn **Anklopfen** aktiviert ist, wählen Sie aus, für welche Gespräche Sie Anklopfen zulassen wollen. Mögliche Werte: • *Internanrufe* • *Externanrufe* • *Intern- und Externanrufe* Entscheiden Sie unter **Anklopfwiederholung** außerdem, ob der Anklopfton oder die Displayanzeige nur einmal signalisiert oder so lange wiederholt werden soll, wie der Anruf besteht.
Anrufschutz (Ruhe)	Nur für Telefone der **CS4xx**-Serie, die Telefone **S530** und **S560** und das Telefon **IP-S400**. Für die Telefone **S530** und **S560** konfigurieren Sie hier lediglich die Funktion. Aktivieren Sie sie bei diesen Telefonen über die Funktionstaste *Anrufschutz*. Wählen Sie aus, ob Sie das Leistungsmerkmal Anrufschutz (Ruhe vor der Telefon) nutzen wollen. Mit diesem Leistungsmerkmal können Sie die Signalisierung von Anrufen an Ihrem Endgerät schalten. Wählen Sie aus, für welche Rufnummern Sie das Leistungsmerkmal Anrufschutz nutzen wollen. Mögliche Werte: • *Nur erste Rufnummer* (nur **CS4xx**-Serie): Der Anrufschutz gilt nur für die erste konfigurierte MSN. • *Alle Rufnummern* (nur **CS4xx**-Serie): Der Anrufschutz gilt für alle konfigurierten MSNs. Wählen Sie aus, ob kommende Anrufe signalisiert werden sollen: • *Aus*: Anrufe werden signalisiert. • *Ein* (nur **CS4xx**-Serie): Anrufe werden nicht signalisiert. • *Nur Bestätigungston* (nur **CS4xx**-Serie): Bei einem An-

Feld	Beschreibung
	ruf ist einmalig ein Aufmerkton zu hören. • *Aufmerkton 1* (nur **S530** und **S560**) • *Aufmerkton 2* (nur **S530** und **S560**) • *Aufmerkton 3* (nur **S530** und **S560**) • *Aufmerkton 4* (nur **S530** und **S560**) • *Kein Aufmerkton* (nur **S530** und **S560**)

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Status-LED	Wählen Sie aus, ob und welche Ereignisse die Status-LED am Systemtelefon signalisieren soll. Mögliche Werte: • *Aus*: Die Funktion der Status-LED wird nicht genutzt. • *Anruferliste*: Die Status-LED signalisiert Anrufe und neue Nachrichten. • *Nur Nachrichten*: Die Status-LED signalisiert nur neue Nachrichten (MWI). • *Neue Nachricht* nur (**S5x0**) • *Neue Anrufe* nur (**S5x0**) • *Aktiver Anruf* nur (**S5x0**) Die Optionen *Neue Nachricht*, *Neue Anrufe* und *Aktiver Anruf* können Sie einzeln verwenden oder beliebig kombinieren.
Softkey Telefonbuch	Nur für die Telefone der **CS4xx**-Serie Wählen Sie aus, ob mit dem Softkey Einträge aus dem System-Telefonbuch (*System*) oder aus dem Telefonbuch des Telefons (*Telefon*) aufgerufen werden.
Gesprächsanzeige	Nicht für **S5x0** Wählen Sie aus, welche Informationen während eines Telefonats im Display des Systemtelefons angezeigt werden sollen.

Feld	Beschreibung
	Mögliche Werte: • *Rufnummer und Kosten oder Dauer* • *Rufnummer und Kosten* • *Rufnummer und Dauer* • *Rufnummer und Zeit* • *Nur Rufnummer* • *Nur Datum und Uhrzeit*
Eingabe während einer Verbindung	Wählen Sie aus, ob im Gesprächszustand DTMF-Signale oder Keypad-Funktionen in das System gesendet werden sollen. Während einer Verbindung können Sie durch die Eingabe von Zeichen- und Ziffernfolgen besondere Funktionen nutzen. Diese Eingaben müssen je nach zu steuernder Funktion als Keypad- oder MFV-Sequenz erfolgen. Sie können festlegen, ob in der Grundeinstellung während einer Verbindung MFV- oder Keypad-Sequenzen möglich sind. Mögliche Werte: • *DTMF* (Standardwert) • *Keypad*
Automatische Rufannahme	Wählen Sie aus, nach welcher Zeit Rufe an diesem Systemtelefon automatisch angenommen werden sollen, ohne dass Sie den Hörer abheben oder die Lautsprechertaste betätigen müssen. **Hinweis** Beachten Sie, dass mindestens eine Taste des Telefons mit Automatische Rufannahme belegt sein muss, um diese Funktion nutzen zu können. Nur für **S5x0** Mit *Aktiviert* Schalten Sie die automatische Rufannahme ein. Stellen Sie die entsprechende Zeitdauer im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Tasten**

Feld	Beschreibung
	ein. Nur für **x290xx** und **x4x0xx** Mögliche Werte: • *Sofort* • *Nach 5 Sekunden* • *Nach 10 Sekunden*
Stumm nach Freisprechanwahl	Nicht für **S5x0**, **CS290**, **CS290-U** Sie können die Rufnummer eines Teilnehmers wählen, ohne dabei den Hörer abzuheben (z. B. Freisprechen). Sie haben dabei die Wahl, ob das eingebaute Mikrofon sofort oder erst nach Betätigung des entsprechenden Softkeys eingeschaltet wird. Ist das Mikrofon während der Anwahl ausgeschaltet, muss der entsprechende Softkey gedrückt werden, auch wenn die Verbindung bereits hergestellt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
UUS empfangen	Wählen Sie aus, ob an diesem Telefon das Leistungsmerkmal UUS (User to User Signalling) genutzt werden kann. Mit diesem Leistungsmerkmal können Sie kurze Textnachrichten von anderen Telefonen empfangen. Innerhalb des Systems können Sie auf diese Weise schriftliche Informationen, wie z. B. *Besprechung um 09:30 Uhr* oder *Bin bis zum Montag im Urlaub*, versenden. Mögliche Werte: • *Aus, UUS blockiert*: Das Leistungsmerkmal UUS wird nicht genutzt. • *Nur intern*: Textnachrichten können nur intern empfangen werden. • *Nur extern*: Textnachrichten können nur extern empfangen werden. • *Intern und extern* (Standardwert): Textnachrichten können intern und extern empfangen werden.
Wechselsprechen	Nur sichtbar wenn im Menü **Endgeräte**->**elmeg Systemtelefo-**

Feld	Beschreibung
empfangen	**ne**->**Systemtelefon**->**Allgemein** unter **Interne Rufnummern** eine **Rufnummer/Benutzer** ausgewählt ist. Wählen Sie aus ob die Funktion **Wechselsprechen empfangen** erlaubt sein soll. Standardmäßig ist die Funktion nicht aktiv.
Durchsage	Nur sichtbar wenn im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Allgemein** unter **Interne Rufnummern** eine **Rufnummer/Benutzer** ausgewählt ist. Wählen Sie aus ob die Funktion **Durchsage** erlaubt sein soll. Standardmäßig ist die Funktion nicht aktiv.

15.1.1.3 Tasten / T400 / T400/2 / T500

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Tasten** wird die Konfiguration der Tasten Ihres Systemtelefons angezeigt.

Ihr Telefon verfügt über mehrere Funktionstasten, die Sie in zwei Ebenen mit verschiedenen Funktionen belegen können. Die Funktionen, die auf den Tasten programmiert werden können, sind bei den einzelnen Telefonen unterschiedlich.

Jede Funktionstaste mit automatischen Leuchtdiodenfunktionen (z. B. Leitungstasten, Linientasten) darf nur einmal je System (Telefon und Tastenerweiterungen) programmiert werden.

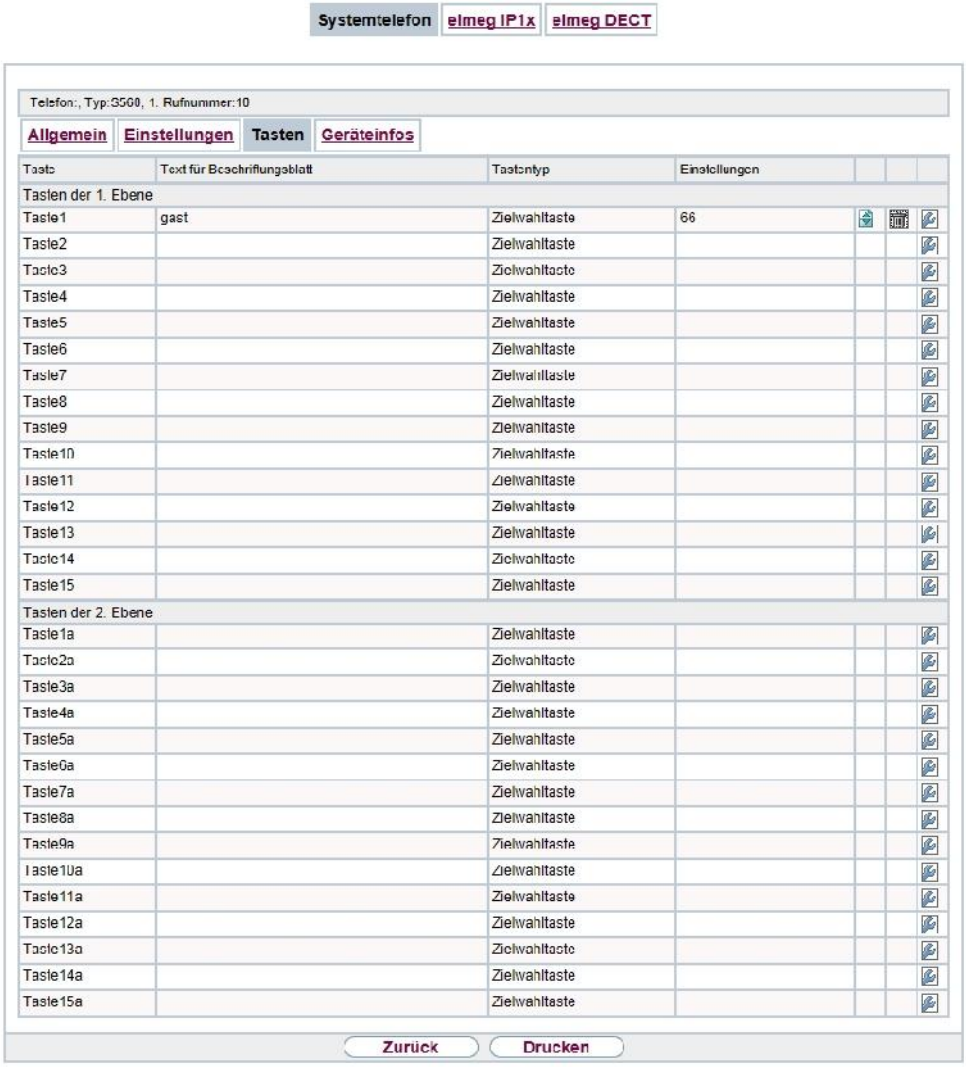


Abb. 94: **Endgeräte->elmeg Systemtelefone->Systemtelefon->Tasten**

Werte in der Liste Tasten

Feld	Beschreibung
Taste	Zeigt die Tastennummer an.
Text für Beschriftungs-blatt	Zeigt den konfigurierten Tastennamen an. Dieser erscheint auf dem Beschriftungsblatt (Beschriftungsstreifen).
Tastentyp	Zeigt den Tastentyp an.

Feld	Beschreibung
Einstellungen	Zeigt die zusätzlichen Einstellungen in einer Zusammenfassung an.

Mithilfe von **Drucken** können Sie ein Beschriftungsblatt für das Beschriftungsfeld Ihres Systemtelefons oder Ihrer Tastenerweiterung drucken.

Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Im Popup-Menü konfigurieren Sie die Funktionen der Tasten Ihres Systemtelefons.

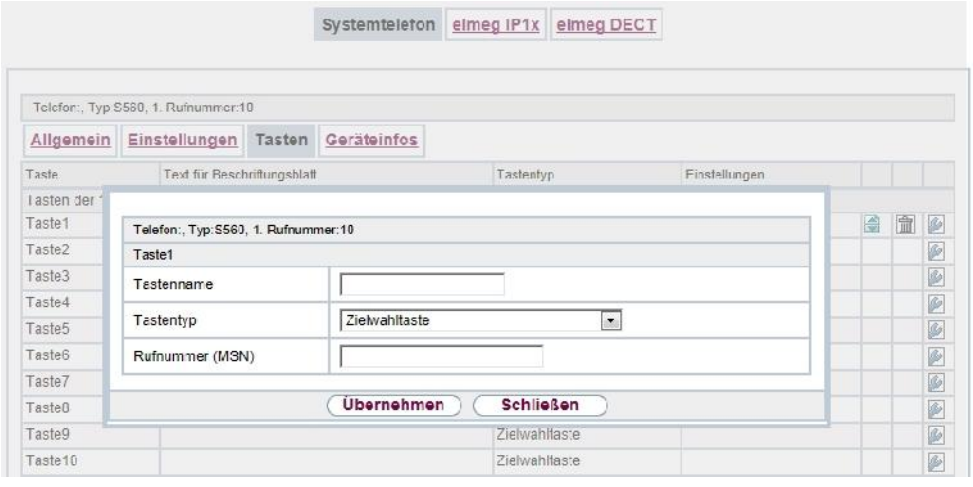


Abb. 95: **Endgeräte->elmeg Systemtelefone->Systemtelefon->Tasten->Bearbeiten**

Folgende Funktionen können Sie mit Systemtelefonen nutzen:

- *MSN-Auswahltaste*: Sie können eine interne oder externe Wahl so durchführen, dass von Ihrem Systemtelefon eine bestimmte Rufnummer (MSN) zum Gesprächspartner übermittelt wird. Diese Rufnummer (MSN) muss vorab in Ihrem Systemtelefon eingetragen sein. Wenn die Leuchtdiode eingeschaltet ist, so besteht eine Verbindung über die Taste.
- *Zielwahltaste*: Sie können auf jeder Funktionstaste eine Rufnummer speichern. Bei Eingabe einer externen Rufnummer muss die Amtskennziffer *0* vorangestellt sein, wenn in Ihrem Telefon **Benutzerklasse** = *keine automatische Amtsholung* eingestellt ist.
- *Zielwahltaste (DTMF)*: Sie können auf jeder Funktionstaste MFV-Sequenz speichern.
- *Zielwahltaste (Keypad)*: Sie können auf jeder Funktionstaste eine Keypadsequenz

speichern.

- *Linientaste Teilnehmer*: Unter einer Linientaste können Sie eine Wahl zu einem internen Teilnehmer einrichten. Nach Betätigen der entsprechenden Taste wird das Freisprechen eingeschaltet und der eingetragene interne Teilnehmer gewählt. Wird ein Anruf an dem eingetragenen internen Teilnehmer signalisiert, können Sie diesen durch Betätigen der Linientaste heranholen.
- *Linientaste Team*: Unter einer Linientaste können Sie eine Wahl zu einem Team einrichten. Nach Betätigen der entsprechenden Taste wird das Freisprechen eingeschaltet und das eingetragene Team wird gemäß seiner aktiven Anrufvariante gerufen. Wird ein Anruf an dem eingetragenen Team signalisiert, können Sie diesen durch Betätigen der Linientaste heranholen.
- *Leitungstaste*: Unter einer Leitungstaste wird ein ISDN-Anschluss oder ein VoIP-Provider eingerichtet. Wird diese Taste betätigt, wird automatisch Freisprechen eingeschaltet und der entsprechende ISDN-Anschluss belegt. Sie hören dann den externen Wählton. Wird ein externer Anruf an einem anderen internen Telefon signalisiert, können Sie diesen durch Betätigen der Leitungstaste heranholen.
- *Durchsage Benutzer*: Sie können eine Verbindung zu einem anderen Telefon aufbauen, ohne dass diese Verbindung aktiv angenommen werden muss. Sobald das Telefon die Durchsage angenommen hat, wird die Verbindung hergestellt und die Leuchtdiode der Durchsage-Taste wird eingeschaltet. Das Beenden der Durchsage ist durch erneutes Betätigen der Durchsage-Taste oder durch Betätigen der Lautsprecher-Taste möglich. Nach Beenden der Durchsage wird die Leuchtdiode wieder ausgeschaltet.
- *Durchsage Team*: Sie können eine Durchsage zu einem Team durch eine eingerichtete Funktionstaste aufbauen. Die Funktionsweise entspricht der oben beschriebenen.
- *Ein-/Ausloggen, Team*: Sind Sie als Teilnehmer in den Anrufvarianten eines oder mehrerer Teams eingetragen, können Sie eine Taste so einrichten, dass Sie die Rufsignalisierung Ihres Telefons kontrollieren können. Sind Sie eingeloggt, werden Teamanrufe an Ihrem Telefon signalisiert. Sind Sie ausgeloggt, werden keine Teamanrufe signalisiert.

  Das Ein-/ Ausloggen aus einem Team durch eine eingerichtete Funktionstaste ist für die im Telefon eingetragenen Rufnummern (**MSN**-1... **MSN**-9) möglich. Vor der Eingabe der Teamrufnummer müssen Sie daher den Index der Rufnummer (MSN) des Telefons wählen,die in der entsprechenden Team-Anrufvarianten eingetragen ist.
- *Durchsage erlauben ein/aus*: Sie können die Durchsage durch eine Funktionstaste gezielt sperren oder erlauben. Um Durchsagen verwenden zu können, müssen sie in der entsprechenden Berechtigungsklasse erlaubt sein.
- *Wechselsprechen*: Sie können eine Taste so einrichten, dass eine Verbindung zu dem angegebenen Telefon aufgebaut wird, ohne dass diese Verbindung aktiv angenommen werden muss.
- *Wechselsprechen erlauben ein/aus*: Sie können eine Taste so einrichten, dass

die Funktion Wechselsprechen erlaubt bzw. untersagt ist. Um Wechselsprechen verwenden zu können, muss die Funktion in der entsprechenden Berechtigungsklasse erlaubt sein.

- *Chef* / *Sekretariat*: Sie können eine Taste als besondere Linien-Taste einrichten. Durch diese Tasten werden in den beiden Telefonen die Eigenschaften Chef-Telefon und Sekretariats-Telefon hinterlegt.
- *Umleitung Sekretariat*: Sie können eine Taste so einrichten, dass kommende Anrufe auf das Chef-Telefon automatisch auf das Sekretariat-Telefon umgeleitet werden.
- *Anrufweiterschaltung verzögert (CFNR)*: Sie können eine Taste so einrichten, dass eine verzögerte Rufumleitung für eine bestimmte Rufnummer (MSN) Ihres Telefons eingerichtet wird. Im Ruhezustand des Telefons wird durch Betätigen der Taste die Rufumleitung ein- oder ausgeschaltet. Das Einrichten einer Rufumleitung über eine programmierte Taste ist nur für die Rufnummern 1 bis 9 (MSN-1...MSN-9) des Telefons möglich. Um die Rufumleitung nutzen zu können, müssen Sie mindestens eine Rufnummer eingerichtet haben.
- *Anrufweiterschaltung sofort (CFU)*: Sie können eine Taste so einrichten, dass eine sofortige Rufumleitung für eine bestimmte Rufnummer (MSN) Ihres Telefons eingerichtet wird. Im Ruhezustand des Telefons wird durch Betätigen der Taste die Rufumleitung ein- oder ausgeschaltet. Das Einrichten einer Rufumleitung über eine programmierte Taste ist nur für die Rufnummern 1 bis 9 (MSN-1...MSN-9) des Telefons möglich. Um die Rufumleitung nutzen zu können, müssen Sie mindestens eine Rufnummer eingerichtet haben.
- *Anrufweiterschaltung bei Besetzt (CFB)*: Sie können eine Taste so einrichten, dass eine Rufumleitung bei Besetzt für eine bestimmte Rufnummer (MSN) Ihres Telefons eingerichtet wird. Im Ruhezustand des Telefons wird durch Betätigen der Taste die Rufumleitung ein- oder ausgeschaltet. Das Einrichten einer Rufumleitung über eine programmierte Taste ist nur für die Rufnummern 1 bis 9 (MSN-1...MSN-9) des Telefons möglich. Um die Rufumleitung nutzen zu können, müssen Sie mindestens eine Rufnummer eingerichtet haben.
- *Makro*: Sie können eine Taste so einrichten, dass bei Betätigen der Taste ein hinterlegtes Makro ausgeführt wird.

  Die Makro-Funktion kann nur am Telefon programmiert werden.
- *Headset* (nicht bei **S5x0**): Haben Sie an Ihrem Telefon ein Headset über eine separate Headsetbuchse angeschlossen und eingerichtet, erfolgt die Bedienung des Headsets über eine Funktionstaste. Zum Einleiten oder Annehmen von Gesprächen betätigen Sie die Headsettaste. Haben Sie bereits eine aktive Verbindung über das Headset, können Sie das Gespräch durch Betätigen der Headsettaste beenden.
- *Automatische Rufannahme*: Ihr Telefon kann Anrufe automatisch annehmen, ohne dass Sie den Hörer abheben oder die Lautsprechertaste betätigen müssen. Die automatische Rufannahme wird durch eine eingerichtete Funktionstaste ein- oder ausgeschaltet. Sie können für jede Rufnummer (»MSN-1«...»MSN-9«) eine separate Funktionstaste

oder eine Funktionstaste für alle Rufnummern einrichten. Die Zeit, nach der Anrufe automatisch angenommen werden, wird einmal für alle Rufnummern des Telefons eingerichtet.

- *Bündelauswahl*: Im System können mehrere externe ISDN- oder IP-Anschlüsse zu Bündeln zusammengefasst werden. Durch eine Bündeltaste können Sie diese Anschlüsse auf einer Funktionstaste hinterlegen. Wird diese Taste betätigt, wird automatisch Freisprechen eingeschaltet und ein freier B-Kanal des entsprechenden Bündels belegt. Sie hören dann den externen Wählton.
- *Verbindungstaste* (nicht bei **S5x0**): Für die Bedienung beim Makeln können zusätzlich zu den Softkeys »Verbindung 1.. « Funktionstasten am Systemtelefon oder der Erweiterung eingerichtet werden. Es müssen mindestens zwei Verbindungstasten eingerichtet werden.
- *Hotelzimmer*: Sie können eine Taste so belegen, dass bei Betätigung der Taste der Gast ein- oder ausgecheckt wird (erste Ebene) oder das ausgewählte Hotelzimmer-Telefon gerufen wird (zweite Ebene). Sie müssen diese Taste auf der ersten Ebene einrichten, die zugehörige Taste auf der zweiten Ebene wird automatisch belegt und ihr Inhalt gegebenenfalls überschrieben.
- *Offene Rückfrage*: Der angerufene Teilnehmer geht in Rückfrage und wählt eine Kennziffer. Das Telefon ist jetzt für andere Bedienungen, z. B. eine Durchsage oder Ansage frei. Ein anderer Teilnehmer kann das Gespräch annehmen, wenn er den Hörer abhebt und die entsprechende Kennziffer für das gehaltene Gespräch wählt. Die von der TK-Anlage vorgegebenen Kennziffern können auch in die Funktionstasten eines oder mehrerer Systemtelefone eingetragen werden. Wird ein Gespräch durch Betätigen der Funktionstaste in die offene Rückfrage gelegt, wird dieses durch Blinken an den LEDs der Funktionstasten der hierfür eingerichteten Systemtelefone angezeigt. Durch Drücken der entsprechenden Funktionstaste wird das Gespräch übernommen. Dieses Leistungsmerkmal ist nur möglich, wenn nur ein Gespräch gehalten wird.
- *Nachbereitungszeit des Agent*: Sie können eine Taste so einrichten, dass beim Betätigen dieser Taste die Nachbearbeitungszeit eines Agents in einem Team Call Center ein- oder ausgeschaltet wird (erste Ebene) oder diese verlängert wird (zweite Ebene).
- *Nachtbetrieb*: Sie können eine Taste so einrichten, dass beim Betätigen dieser Taste der Nachtbetrieb ein oder ausgeschaltet wird.

Hinweis

Um den Nachbetrieb manuell wieder ausschalten zu können, muss für die Berechtigungsklasse **Anrufvarianten manuell umschalten** akiviert sein.

- *Parallelruf* (nur **S5x0**): Wenn ein Parallelruf zu einem anderen Telefon eingerichtet ist, klingelt es bei einem Anruf an beiden Anschlüssen. Das Gespräch wird dort angenommen, wo zuerst abgehoben wird.
- *Umschalttaste* (nur **S5x0**): Mit dieser Taste können Sie die Funktionen der zweiten

Ebene erreichen.

- *Anrufschutz* (nur **S5x0**): Mit dieser Taste schalten Sie die Funktion Ruhe vor dem Telefon ein oder aus, die Sie unter **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Einstellungen** konfiguriert haben.

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Tasten**->**Bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Telefon

Feld	Beschreibung
Tastenname	Geben Sie einen Namen für die Taste ein, der beim Drucken der Beschriftungsschilder als Text für die entsprechende Taste verwendet wird.
Tastentyp	Die Telefone verfügen je nach Ausführung über fünf bis 15 Tasten, die in zwei Ebenen mit Funktionen belegt werden können. Die zweite Ebene der Funktionstasten erreichen Sie durch einen doppelten Tastendruck. Dieser muss in kurzem Abstand ausgeführt werden. Bei S5x0-Geräten können Sie alternativ die Funktionstaste *Umschalttaste* verwenden. Mit den optionalen Tastenerweiterungen stehen Ihnen weitere zweifach belegbare Funktionstasten zur Verfügung. Mögliche Werte: • *MSN-Auswahltaste* • *Zielwahltaste* • *Zielwahltaste (DTMF)* • *Zielwahltaste (Keypad)* • *Linientaste Teilnehmer* • *Linientaste Team* • *Leitungstaste* • *Durchsage Benutzer* • *Durchsage Team* • *Ein-/Ausloggen, Team* • *Durchsage erlauben ein/aus* • *Wechselsprechen* • *Wechselsprechen erlauben ein/aus* • *Chef* • *Sekretariat*

Feld	Beschreibung
	• *Umleitung Sekretariat* • *Anrufweiterschaltung verzögert (CFNR)* • *Anrufweiterschaltung sofort (CFU)* • *Anrufweiterschaltung bei Besetzt (CFB)* • *Makro* • *Headset* • *Automatische Rufannahme* • *Bündelauswahl* • *Verbindungstaste* • *Hotelzimmer* • *Offene Rückfrage* • *Nachbereitungszeit des Agent* • *Nachtbetrieb* • *Umschalttaste* (nur **S5x0**) • *Parallelruf* (nur **S5x0**) • *Anrufschutz (Ruhe)* (nur **S5x0**)
Rufnummer (MSN)	Nur bei **Tastentyp** = *Zielwahltaste*, *Zielwahltaste (DTMF)* und *Zielwahltaste (Keypad)* Sie können auf jeder Funktionstaste eine Rufnummer, eine MFV-Sequenz oder eine Keypadsequenz speichern. Geben Sie die Rufnummer oder die Zeichen für die MFV-/ Keypadsequenz ein.
Interne Rufnummer	Bei **Tastentyp** = *Linientaste Teilnehmer* Wählen Sie die interne Rufnummer eines Benutzers aus, der bei Betätigung dieser Taste gerufen werden soll. Bei **Tastentyp** = *Durchsage Benutzer* Wählen Sie die interne Rufnummer eines Benutzers aus, an dessen Telefon eine Durchsage ertönen soll. Bei **Tastentyp** = *Ein-/Ausloggen, Team* Wählen Sie die interne Rufnummer eines Teams aus, in das bei Betätigung dieser Taste eingeloggt bzw. davon ausgeloggt wer-

Feld	Beschreibung
	den soll. Bei **Tastentyp** = *Wechselsprechen* Wählen Sie die interne Rufnummer eines Benutzers aus, mit dem Sie Wechselgespräche führen wollen. Bei **Tastentyp** = *Anrufweiterschaltung verzögert (CFNR)*, *Anrufweiterschaltung sofort (CFU)*, *Anrufweiterschaltung bei Besetzt (CFB)* Wählen Sie die interne Rufnummer einer MSN des Telefons aus, von der aus an die angegebene Zielrufnummer weitergeleitet werden soll. Bei **Tastentyp** = *Automatische Rufannahme* Wählen Sie die interne Rufnummer dieses Telefons aus, auf der kommende Rufe automatisch angenommen werden sollen. Bei **Tastentyp** = *Hotelzimmer* Wählen Sie die interne Rufnummer eines Hotelgastes aus. Bei **Tastentyp** = *Nachbereitungszeit des Agent* Wählen Sie die interne Rufnummer eines Benutzers aus, dessen Nachbearbeitungszeit bei Betätigung dieser Taste intervallweise verändert werden soll. Bei **Tastentyp** = *Parallelruf* Wählen Sie die interne Rufnummer eines Benutzers aus, bei dem das Telefon ebenfalls klingeln soll, wenn bei Ihnen ein Anruf eingeht. Bei **Tastentyp** = *MSN-Auswahltaste* Wählen die MSN des eigenen Telefons, die Sie verwenden wollen.
Automatische Rufannahme	Bei **Tastentyp** = *Automatische Rufannahme* Wählen Sie aus, wann ein Ruf automatisch beim eingetragenen internen Teilnehmer angenommen werden soll. Mögliche Werte:

Feld	Beschreibung
	• *Sofort*: Der Ruf wird sofort automatisch angenommen. • *Nach 5 Sekunden*: Der Ruf wird nach 5 Sekunden automatisch angenommen. • *Nach 10 Sekunden*: Der Ruf wird nach 10 Sekunden automatisch angenommen. • *Nach 15 Sekunden* (nur **S5x0**): Der Ruf wird nach 15 Sekunden automatisch angenommen. • *Nach 20 Sekunden* (nur **S5x0**): Der Ruf wird nach 20 Sekunden automatisch angenommen. • *Aus* (nur **S5x0**): Der Ruf wird nicht automatisch angenommen.
Team	Bei **Tastentyp** = *Linientaste Team* Wählen Sie die interne Rufnummer eines Teams aus, mit dem bei Betätigung dieser Taste verbunden werden soll. Bei **Tastentyp** = *Durchsage Team* Wählen Sie die interne Rufnummer eines Teams aus, an dessen Telefon eine Durchsage ertönen soll. Bei **Tastentyp** = *Ein-/Ausloggen, Team* Wählen Sie die interne Rufnummer eines Teams aus, bei dem bei Betätigung dieser Taste ein- bzw. ausgeloggt werden soll.
Trunk-Leitung	Nur bei **Tastentyp** = *Leitungstaste* Wählen Sie den externen Anschluss aus, über den bei Betätigung dieser Taste eine externe Verbindung aufgebaut werden soll.
Rufnummer des Sekretariat-Telefones	Nur bei **Tastentyp** = *Chef* Wählen Sie die interne Rufnummer des Sekretariat-Telefons aus. Bei Betätigung dieser Taste wird das Sekretariat-Telefon gerufen.
Rufnummer des Chef-Telefones	Nur bei **Tastentyp** = *Sekretariat* Wählen Sie die interne Rufnummer des Chef-Telefons aus. Bei Betätigung dieser Taste wird das Chef-Telefon gerufen.

Feld	Beschreibung
Zielrufnummer "Bei Nichtmelden"	Nur bei **Tastentyp** = *Anrufweiterschaltung verzögert (CFNR)* Geben Sie die Rufnummer ein, auf die bei Anrufweiterschaltung sofort weitergeleitet werden soll.
Zielrufnummer "Sofort"	Nur bei **Tastentyp** = *Anrufweiterschaltung sofort (CFU)* Geben Sie die Rufnummer ein, auf die bei Anrufweiterschaltung bei Besetzt weitergeleitet werden soll.
Zielrufnummer "Bei besetzt"	Nur bei **Tastentyp** = *Anrufweiterschaltung bei Besetzt (CFB)* Geben Sie die Rufnummer ein, auf die bei Anrufweiterschaltung bei Nichtmelden weitergeleitet werden soll.
Bündelauswahl	Nur bei **Tastentyp** = *Bündelauswahl* Wählen Sie das Bündel aus, über das eine Verbindung nach extern aufgebaut werden soll.
Wartefeld	Nur bei **Tastentyp** = *Offene Rückfrage* Wählen Sie das Wartefeld aus, in dem die aktuelle Verbindung gehalten werden soll.

Taste verschieben

Wählen Sie das Symbol , um konfigurierte Funktionstasten zu verschieben.

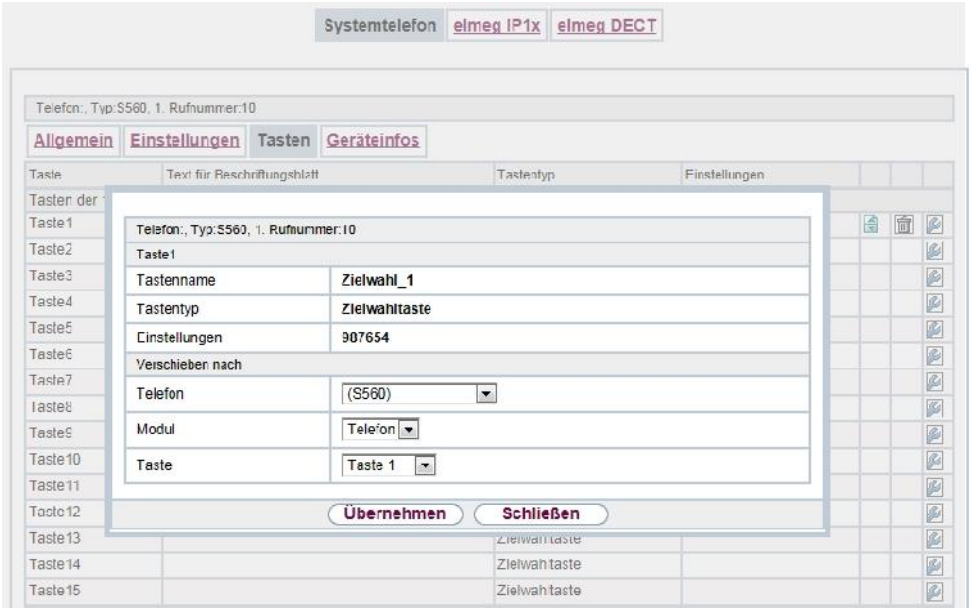


Abb. 96: **Endgeräte->elmeg Systemtelefone->Systemtelefon->Tasten->Verschieben**

Felder im Menü Taste

Feld	Beschreibung
Tastenname	Zeigt den Namen der Taste an.
Tastentyp	Zeigt den Tastentyp an.
Einstellungen	Zeigt die zusätzlichen Einstellungen in einer Zusammenfassung an.

Felder im Menü Verschieben nach

Feld	Beschreibung
Telefon	Wählen Sie eines der angeschlossenen Telefone aus.
Modul	Wählen Sie *Telefon* oder eine Tastenerweiterung aus.
Taste	Wählen Sie die Taste aus, auf die Sie die konfigurierte Funktion verschieben möchten.

15.1.1.4 Geräteinfos

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Geräteinfos** werden die aus dem Systemtelefon ausgelesenen Systemdaten angezeigt.

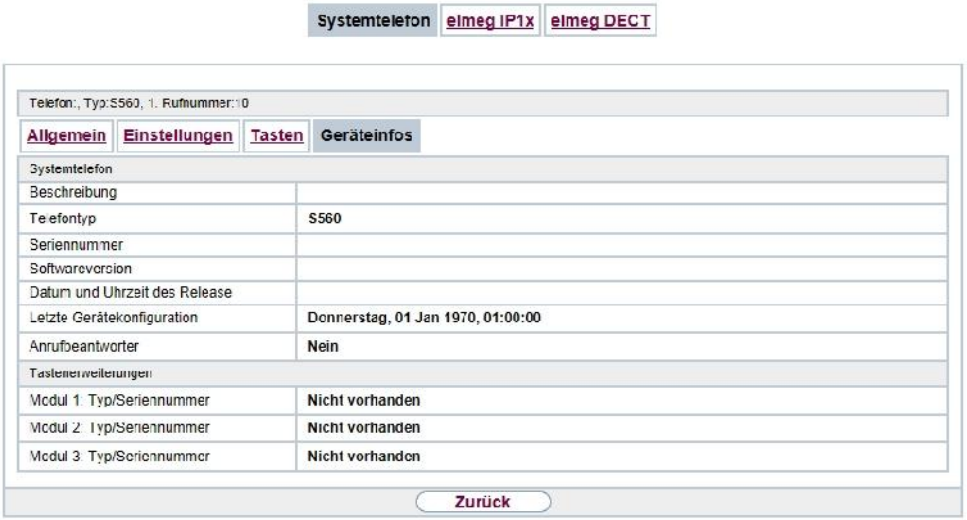


Abb. 97: **Endgeräte->elmeg Systemtelefone->Systemtelefon->Geräteinfos**

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Beschreibung	Zeigt die eingetragene Beschreibung des Telefons an.
Telefontyp	Zeigt den Typ des Telefons an.
Seriennummer	Zeigt die Seriennummer des Telefons an.
Softwareversion	Zeigt den aktuellen Stand der Telefon-Software an.
Datum und Uhrzeit des Release	Zeigt Datum und Uhrzeit des Telefon-Software-Standes an.
Letzte Gerätekonfiguration	Zeigt Datum und Uhrzeit der letzten Konfigurierung des Telefons an.
Anrufbeantworter	Zeigt an, ob ein Anrufbeantwortermodul im Telefon gesteckt ist (Ja) oder nicht (Nein).

Bedeutung der Tastenerweiterungen

Beschreibung	Bedeutung
Modul 1: Typ/ Seriennummer, **Modul 2: Typ/Seriennummer**, **Modul 3: Typ/ Seriennummer**	Zeigt den Typ und die Seriennummer der angeschlossenen Tastenerweiterung an.
Modul 1: Softwareversion, **Modul. 2: Softwareversion**, **Modul 3: Softwareversion**	Zeigt die aktuelle Softwareversion der angeschlossenen Tastenerweiterung an.

15.1.2 elmeg IP1x

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x** wird eine Liste der IP-Telefone angezeigt. Im oberen Abschnitt sehen Sie die manuell konfigurierten, im unteren Abschnitt die automatisch erkannten Telefone. Für das automatische Erkennen empfehlen wir Ihnen, DHCP zu verwenden (Aktivieren Sie im Menü **Assistenten**->**Erste Schritte** die Option *Dieses Gerät als DHCP-Server verwenden*.). Sollten Sie feste IP-Adressen einstellen wollen, so müssen Sie für das automatische Erkennen Ihre Telefonanlage im Telefon als Provisioning-Server eintragen (*http://<IP_Adresse des Provisionierungsservers>/eg_prov*).

Sobald eine **Beschreibung** für ein automatisch erkanntes Gerät eingetragen und mit **OK** übernommen wurde, wird der Eintrag für dieses Gerät in den oberen Abschnitt der Übersicht verschoben.

Hinweis

Tastenerweiterungen werden nicht automatisch erkannt, sondern müssen manuell mit dem GUI konfiguriert werden.

Wird eine konfigurierte Tastenerweiterung gelöscht, so werden die entsprechenden Funktionstasten ebenfalls gelöscht.

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

Wenn Sie auf die Schaltfläche **Übernehmen** klicken, verstreichen einige Sekunden bis die konfigurierten Änderungen in das entsprechende IP-Telefon übertragen sind.

Wählen Sie das Symbol  , um vorhandene Einträge zu kopieren. Das Kopieren eines Eintrags kann nützlich sein, wenn Sie einen Eintrag anlegen wollen, der sich nur in wenigen Parametern von einem bereits vorhandenen Eintrag unterscheidet. In diesem Fall kopieren Sie den Eintrag und ändern Sie die gewünschten Parameter.

Wählen Sie das Symbol  , um zum Web-Konfigurator des **elmeg IP1x**-Telefons zu gelangen. Dieser wird in der Bedienungsanleitung zum Telefon beschrieben.

Wählen Sie die Schaltfläche **Neu**, um ein neues IP-Telefon manuell einzurichten.

Verwenden Sie die automatische Provisionierung, um mithilfe der Telefonanlage elementare Telefonie-Parameter an ein IP-Telefon zu übertragen. Wenn Sie dazu den Assistenten **Erste Schritte** verwenden wollen, aktivieren Sie unter **Assistenten**->**Erste Schritte**->**Erweiterte Einstellungen**->**Hinzufügen** im Feld **Übertrage Provisionierungsserver für** den Wert *elmeg IP1x/DECT*. Sie können stattdessen auch unter **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu**->**Erweiterte Einstellungen** unter **DHCP-Optionen** mit **Hinzufügen** einen neuen Eintrag erzeugen und die Felder **Option** = *URL (Provisionierungsserver)* und **Wert** = *http://<IP_Adresse des Provisionierungsservers>/eg_prov* setzen.

15.1.2.1 Allgemein

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Allgemein** nehmen Sie die grundlegenden Einstellungen eines IP-Telefons vor.

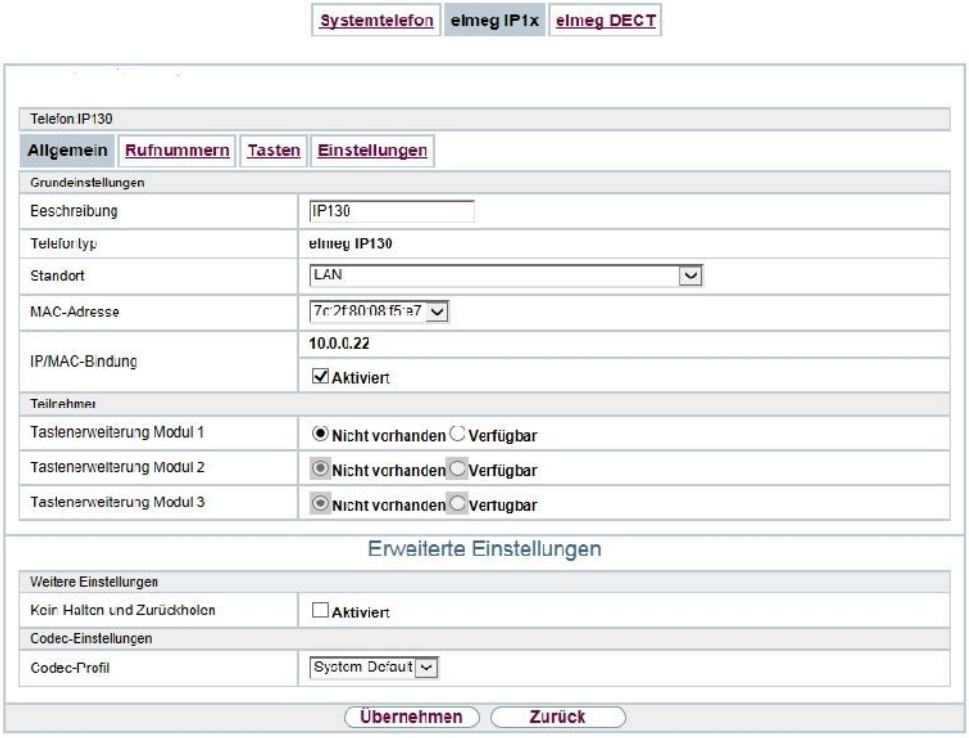


Abb. 98: **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Allgemein**

Das Menü **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Um das Telefon im System eindeutig zu identifizieren, geben Sie eine Beschreibung für das Telefon ein.
Telefontyp	Zeigt den Typ Ihres IP-Telefons an. Mögliche Werte: • *Eine auswählen* • *elmeg IP120* • *elmeg IP130* • *elmeg IP140*
Standort	Wählen Sie den Standort des Telefons aus. Standorte definie-

Feld	Beschreibung
	ren Sie im Menü **VoIP**->**Einstellungen**->**Standorte**. Abhängig von der Einstellung in diesem Menü wird das Standardverhalten für die Registrierung von VoIP-Teilnehmern zur Auswahl angezeigt, für die kein Standort definiert werden soll. Mögliche Werte: • *Nicht definiert (Uneingeschränkte Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer dennoch registriert. • *Nicht definiert (Keine Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nicht registriert. • *Nicht definiert (Registrierung nur in privaten Netzwerken)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nur registriert, wenn er sich im privaten Netzwerk befindet. • *<Standort>*: Es wird ein definierter Standort ausgewählt. Der Teilnehmer wird nur registriert, wenn er sich an diesem Standort befindet.
MAC-Adresse	Zeigt die MAC-Adresse des Telefons an.
IP/MAC-Bindung	Zeigt die per DHCP automatisch zugewiesene IP-Adresse an. Hier haben Sie die Möglichkeit, dem Gerät mit der angezeigten MAC-Adresse die angezeigte IP-Adresse fest zuzuweisen. Um eine schnelle Wiederanmeldung nach einer Funktionsstörung zu ermöglichen, sollte diese Option aktiviert werden.

Tastenerweiterungen

Die Tastenerweiterung **elmeg T100** (verfügbar für die Telefone **elmeg IP120**, **IP130** und **IP140**) besitzt 14 Tasten mit Leuchtdioden, die Sie als Funktionstasten nutzen können. Bei **elmeg IP120** können Sie bis zu zwei Tastenerweiterungen, bei **elmeg IP130** und **IP140** bis zu drei Tastenerweiterungen hintereinander (kaskadierend) an Ihrem Telefon anschließen. Für die dritte Tastenerweiterung ist der Einsatz eines Steckernetzgerätes notwendig.

Felder im Menü Teilnehmer

Feld	Beschreibung
Tastenerweiterung Modul 1 - 3 (je nach **Telefontyp**)	Zeigt an, ob Sie das IP-Telefon mit einem Tastenerweiterungsmodul betreiben. Es wird nur die jeweils für den Telefontyp unterstützte Anzahl von Modulen zur Konfiguration angezeigt. Mögliche Werte: • **Nicht vorhanden** • **Verfügbar**

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

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Kein Halten und Zurückholen	Die Leistungsmerkmale Halten eines Gesprächs und Zurückholen eines gehaltenen Gesprächs stehen bei bestimmten Telefonen nicht zur Verfügung. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Profil	Wählen Sie das Codec-Profil aus, das verwendet werden soll. Codec-Profile konfigurieren Sie im Menü **VoIP**->**Einstellungen**->**Codec-Profile**

15.1.2.2 Rufnummern

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Rufnummern** weisen Sie einem IP-Telefon mit **Hinzufügen** bis zu zwölf interne Rufnummern zu.

Die verfügbaren internen Rufnummern werden unter **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Neu** angelegt.

Mit  können Sie zugewiesene Rufnummern aus der Liste löschen.

Abb. 99: **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Rufnummern**

Werte in der Liste Rufnummerneinstellungen

Feld	Beschreibung
Verbindungs-Nr.	Zeigt die laufende Nummer der Verbindung an.
Interne Rufnummer	Zeigt die zugewiesene interne Rufnummer an.
Angezeigte Beschreibung	Zeigt die Beschreibung an, die auf dem Display des IP-Telefons angezeigt wird.
Benutzer	Zeigt den Namen des Benutzers an.

15.1.2.3 Tasten / T100

Im Menü **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Tasten** wird die Konfiguration der Tasten Ihres IP-Telefons angezeigt.

Hinweis

Sie können die Tastenbelegung über Ihre Telefonanlage oder im Gerät selbst konfigurieren. Wir empfehlen Ihnen, für diese Aufgabe Ihre Telefonanlage zu verwenden, da die Telefonanlage die Konfiguration im Telefon überschreibt.

Für einzelne, bereits im Gerät konfigurierte Tasten können Sie das Überschreiben verhindern, indem Sie für diese Taste in der Telefonanlage `Nicht konfiguriert` eintragen.

Ihr Telefon verfügt über mehrere Funktionstasten, die Sie mit verschiedenen Funktionen belegen können. Die Funktionen, die auf den Tasten programmiert werden können, sind

bei den einzelnen Telefonen unterschiedlich.

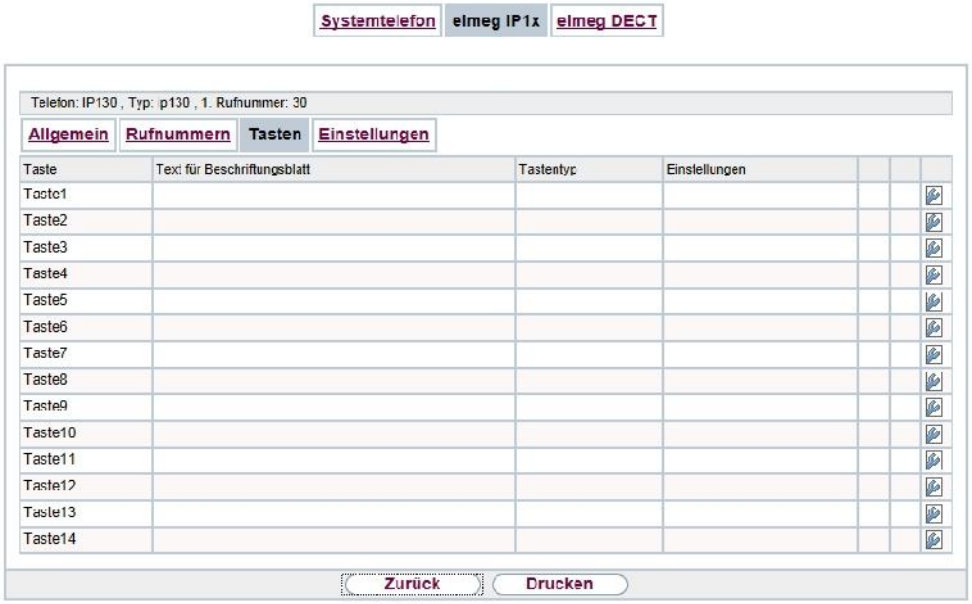


Abb. 100: **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Tasten**

Werte in der Liste Tasten

Feld	Beschreibung
Taste	Zeigt die Tastennummer an.
Text für Beschriftungs-blatt	Zeigt den konfigurierten Tastennamen an. Dieser erscheint auf dem Beschriftungsblatt (Beschriftungsstreifen).
Tastentyp	Zeigt den Tastentyp an.
Einstellungen	Zeigt die zusätzlichen Einstellungen in einer Zusammenfassung an.

Mithilfe von **Drucken** können Sie ein Beschriftungsblatt für das Beschriftungsfeld Ihres IP-Telefons oder Ihrer Tastenerweiterung drucken.

Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Im Popup-Menü konfigurieren Sie die Funktionen der Tasten Ihres IP-Telefons.

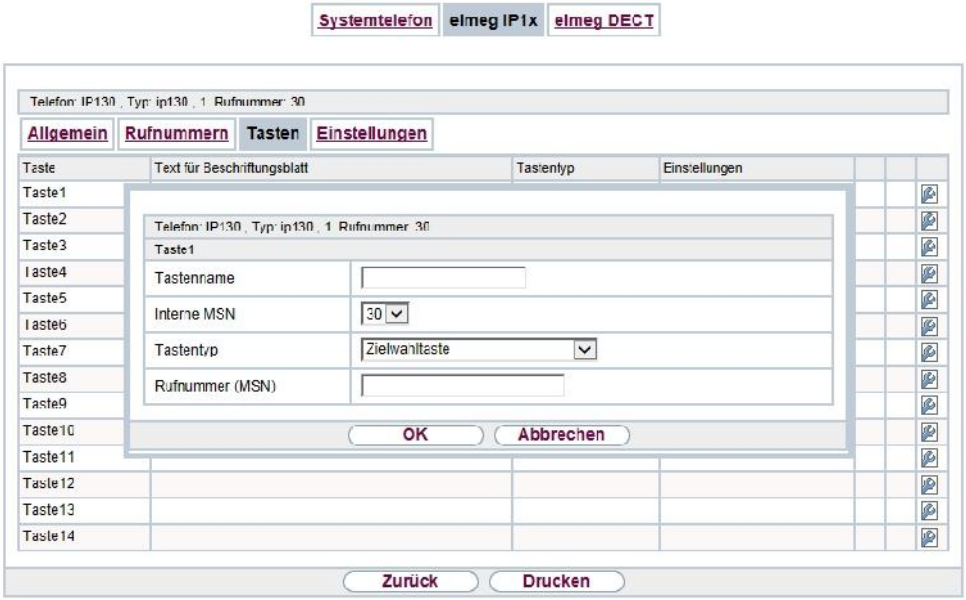


Abb. 101: **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Tasten->Bearbeiten**

Folgende Funktionen können Sie mit IP-Telefonen nutzen:

- *Zielwahltaste*: Sie können auf jeder Funktionstaste eine Rufnummer speichern. Bei Eingabe einer externen Rufnummer muss die Amtskennziffer *0* vorangestellt sein, wenn in Ihrem Telefon **Benutzerklasse** = *keine automatische Amtsholung* eingestellt ist.
- *Zielwahltaste (DTMF)*: Sie können auf jeder Funktionstaste MFV-Sequenz speichern.
- *Linientaste Teilnehmer*: Unter einer Linientaste können Sie eine Wahl zu einem internen Teilnehmer einrichten. Nach Betätigen der entsprechenden Taste wird das Freisprechen eingeschaltet und der eingetragene interne Teilnehmer gewählt. Wird ein Anruf an dem eingetragenen internen Teilnehmer signalisiert, können Sie diesen durch Betätigen der Linientaste heranholen.
- *MSN-Auswahltaste*: Ordnet der Funktionstaste eine bestimmte Verbindung (d.h. einen bestimmten SIP Account) zu. Über die Taste leiten Sie einen Anruf über diese Verbindung ein oder nehmen einen eingehenden Anruf für diese Verbindung an. Die Taste blinkt, wenn ein Anruf eingeht, sie leuchtet, wenn die Leitung besetzt ist. Wählen Sie die gewünschte Verbindung aus. Alle konfigurierten Verbindungen werden zur Auswahl angeboten. Konfigurieren Sie diese SIP Accounts ausschließlich über Ihre Telefonanlage.
- *Anrufweiterschaltung (ein/aus)*: Ordnet der Funktionstaste das Ein- bzw. Ausschalten einer Anrufweiterschaltung zu, die im Endgerät hinterlegt ist. Sie können im Endgerät nur eine einzige Weiterschaltungsvariante einrichten. Die dort hinterlegte Anruf-

weiterschaltung gilt für alle Anrufe.

- *Offene Rückfrage*: Der angerufene Teilnehmer geht in Rückfrage und wählt eine Kennziffer. Das Telefon ist jetzt für andere Bedienungen, z. B. eine Durchsage oder Ansage frei. Ein anderer Teilnehmer kann das Gespräch annehmen, wenn er den Hörer abhebt und die entsprechende Kennziffer für das gehaltene Gespräch wählt. Die von der TK-Anlage vorgegebenen Kennziffern können auch in die Funktionstasten eines oder mehrerer Systemtelefone eingetragen werden. Wird ein Gespräch durch Betätigen der Funktionstaste in die offene Rückfrage gelegt, wird dieses durch Blinken an den LEDs der Funktionstasten der hierfür eingerichteten Systemtelefone angezeigt. Durch Drücken der entsprechenden Funktionstaste wird das Gespräch übernommen. Dieses Leistungsmerkmal ist nur möglich, wenn nur ein Gespräch gehalten wird.
- *XML-Daten*: Ordnet der Funktionstaste eine URL zu. Sie können zum Beispiel auf einem Server kundenspezifische Menüs hinterlegen und diese temporär auf das Display Ihres Telefons laden. Diese Funktion wird zur Zeit von Ihrer Telefonanlage nicht unterstützt.
- *Nächster Anruf anonym*: Bei Ihrem nächsten Anruf wird die eingegebene Rufnummer gewählt. Dem angerufenen Teilnehmer wird Ihre Rufnummer nicht übermittelt.
- *Menu - Anrufweiterschaltung* : Ordnet der Funktionstaste den Menüpunkt **Anrufweiterschaltung** im Display-Menü Ihres Telefons zu. Sie können die Bedingungen für die Anrufweiterschaltung konfigurieren.
- *Menu - Media-Pool*: Ordnet der Funktionstaste den Menüpunkt **Media-Pool** im Display-Menü Ihres Telefons zu. Sie können Bilder, die Sie als Bildschirmschoner verwenden, Anruferbilder für Telefonbucheinträge und Klingeltöne verwalten. Außerdem können Sie die Kapazität des Pools überwachen.
- *Menu - Internet-Radio*: Ordnet der Funktionstaste den Menüpunkt **Internet-Radio** im Display-Menü Ihres Telefons zu. Sie können eine Verbindung zum zuletzt eingestellten Internet-Radiosender herstellen oder einen anderen Sender auswählen.
- *Nicht konfiguriert*: Die Funktionstaste wird vom Endgerät selbst und nicht von der Telefonanlage verwaltet. Mit dieser Einstellung sperren Sie die Taste für eine Provisionierung über Ihre Telefonanlage.

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Tasten**->**Bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Telefon

Feld	Beschreibung
Tastenname	Geben Sie einen Namen für die Taste ein, der beim Drucken der Beschriftungsschilder als Text für die entsprechende Taste verwendet wird.
Tastentyp	Die Telefone verfügen je nach Ausführung über sieben oder 14 Tasten, die mit Funktionen belegt werden können. Mit den optionalen Tastenerweiterungen stehen Ihnen weitere Funktions-

Feld	Beschreibung
	tasten zur Verfügung. Mögliche Werte: • *Zielwahltaste* • *Zielwahltaste (DTMF)* • *Linientaste Teilnehmer* • *MSN-Auswahltaste* • *Anrufweiterschaltung (ein/aus)* • *Offene Rückfrage* • *XML-Daten* • *Nächster Anruf anonym* • *Menu - Anrufweiterschaltung* • *Menu - Media-Pool* • *Menu - Internet-Radio* • *Nicht konfiguriert*
Interne MSN	Nur bei **Tastentyp** = *Zielwahltaste*, *Linientaste Teilnehmer*, *MSN-Auswahltaste*, *Anrufweiterschaltung (ein/aus)* oder *Offene Rückfrage* Sie können eine der internen MSNs wählen, die im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Rufnummern** konfiguriert sind.
Rufnummer (MSN)	Nur bei **Tastentyp** = *Zielwahltaste* oder *Zielwahltaste (DTMF)* Sie können auf jeder Funktionstaste eine Rufnummer oder eine MFV-Sequenz speichern. Geben Sie die Rufnummer oder die Zeichen für die MFV-Sequenz ein.
Interne Rufnummer	Nur bei **Tastentyp** = *Linientaste Teilnehmer* Wählen Sie die interne Rufnummer des Benutzers aus, der bei Betätigung dieser Taste gerufen werden soll.
Kennziffer für Rufannahme	Nur bei **Tastentyp** = *Linientaste Teilnehmer* Die Kennziffer wird für das Besetztlampenfeld (BLF) benötigt,

Feld	Beschreibung
	damit Sie auf einem IP-Telefon einen Ruf bei blinkender LED annehmen können. Der Standardwert ist *#0*.
Wartefeld	Nur bei **Tastentyp** = *Offene Rückfrage* Wählen Sie das Wartefeld aus, in dem die aktuelle Verbindung gehalten werden soll.
URL	Nur bei **Tastentyp** = *XML-Daten* Sie können für die Funktion *XML-Daten* eine URL zu einem Server angeben, auf dem die gewünschten Informationen hinterlegt sind. Diese Funktion wird zur Zeit von Ihrer Telefonanlage nicht unterstützt.

Taste verschieben

Wählen Sie das Symbol , um konfigurierte Funktionstasten zu verschieben.

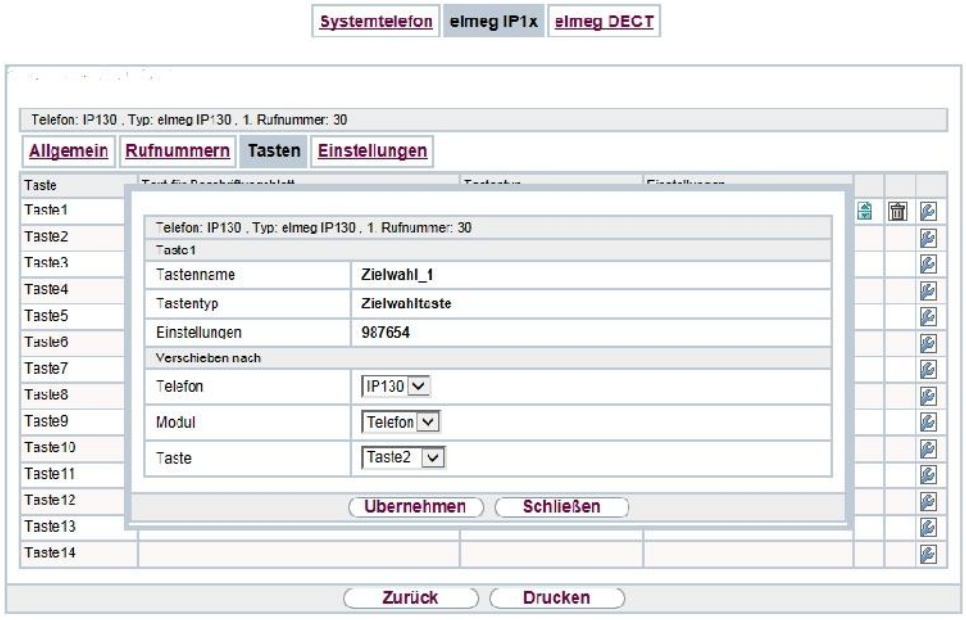


Abb. 102: **Endgeräte->elmeg Systemtelefone->elmeg IP1x->Tasten->Verschieben**

Felder im Menü Taste

Feld	Beschreibung
Tastenname	Zeigt den Namen der Taste an.
Tastentyp	Zeigt den Tastentyp an.
Einstellungen	Zeigt die zusätzlichen Einstellungen in einer Zusammenfassung an.

Felder im Menü Verschieben nach

Feld	Beschreibung
Telefon	Wählen Sie eines der angeschlossenen Telefone aus.
Modul	Wählen Sie die Telefonbasis (eingebaute Tasten) oder eine Tastenerweiterung aus.
Taste	Wählen Sie die Taste aus, auf die Sie die konfigurierte Funktion verschieben möchten.

15.1.2.4 Einstellungen

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Einstellungen** können Sie das Administratorpasswort des Telefons zurücksetzen und die Displaysprache des Telefons festlegen.

Abb. 103: **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Einstellungen**

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg IP1x**->**Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Systemtelefon

Feld	Beschreibung
Administratorpasswort	Wählen Sie aus, ob das Administratorpasswort zurückgesetzt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Sobald Sie das Schaltfläche **OK** wählen, wird das Passwort auf die Standardeinstellung zurückgesetzt.
Displaysprache	Wählen Sie die Sprache für das Display Ihres Telefons aus. Mögliche Werte: • *Deutsch* • *Niederländisch* • *Englisch* • *Italienisch* • *Spanisch* • *Französisch* • *Portugues* • *Cesko* • *Griechisch* • *Polnisch* • *Romanian* • *Slovak*

15.1.3 elmeg DECT

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT** wird eine Liste der Basisstationen der angeschlossenen DECT SingleCell- und MultiCell-Systeme angezeigt.

Im oberen Abschnitt sehen Sie die manuell konfigurierten, im unteren Abschnitt die automatisch erkannten Geräte. Für das automatische Erkennen empfehlen wir Ihnen, DHCP zu verwenden (Aktivieren Sie im Menü **Assistenten**->**Erste Schritte** die Option *Dieses Gerät als DHCP-Server verwenden*.). Sollten Sie feste IP-Adressen einstellen wollen, so müssen Sie für das automatische Erkennen Ihre Telefonanlage im Telefon als Provisioning-Server eintragen (*http://<IP_Adresse des Provisionierungsservers>/eg_prov*).

Sobald eine **Beschreibung** für eine Basisstation eingetragen und mit **OK** übernommen ist, wird der Eintrag für dieses Gerät in den oberen Abschnitt der Übersicht verschoben.

Nach einer kurzen Zeitspanne werden die Symbole und für dieses Gerät angezeigt.

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Wenn Sie auf die Schaltfläche **Übernehmen** klicken, verstreichen einige Sekunden bis die konfigurierten Änderungen in das entsprechende Gerät übertragen sind.

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

Wählen Sie das Symbol , um zum Web-Konfigurator der Basisstation zu gelangen. Dieser wird in der Bedienungsanleitung des jeweiligen DECT-Systems beschrieben.

Um die automatische Provisionierung verwenden zu können, klicken Sie erneut auf das Symbol und fügen die entsprechenden Rufnummern hinzu.

Verwenden Sie die automatische Provisionierung, um mithilfe der Telefonanlage elementare Telefonie-Parameter an das DECT-System zu übertragen. Wenn Sie dazu den Assistenten **Erste Schritte** verwenden wollen, aktivieren Sie unter **Assistenten**->**Erste Schritte**->**Erweiterte Einstellungen**->**Hinzufügen** im Feld **Übertrage Provisionierungsserver für** den Wert *elmeg IP1x/DECT*. Sie können stattdessen auch unter **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu**->**Erweiterte Einstellungen** unter **DHCP-Optionen** mit **Hinzufügen** einen neuen Eintrag erzeugen und die Felder **Option** = *URL (Provisionierungsserver)* und **Wert** = *http://<IP_Adresse des Provisionierungsservers>/eg_prov* setzen.

Zum Anmelden der Mobilteile versetzen Sie zuerst die Basisstation in den Anmeldemodus. Danach nehmen Sie die Anmeldung der Mobilteile an den Mobilteilen selbst vor. Eine weitergehende Konfiguration der Basisstation müssen Sie über den Web-Konfigurator des DECT-Systems durchführen.

Wählen Sie die Schaltfläche , um ein Update der Provisionierung des Geräts anzustoßen. Bei einem erfolgreichen Update wird der aktualisierte Wert in der Spalte **Zuletzt gesehen** innerhalb von 10 Sekunden angezeigt.

Hinweis

Wenn Sie testen wollen, ob Ihre Basisstation korrekt konfiguriert und erreichbar ist, wählen Sie die Schaltfläche und kontrollieren Sie, ob innerhalb von 10 Sekunden in der Spalte **Zuletzt gesehen** ein aktualisierter Wert angezeigt wird.

Hinweis

Wenn Sie bei einem DECT SingleCell-System die aktuell verwendete Sprache ändern wollen, muss das System mit dem Provisionierungsserver der Telefonanlage verbunden sein. Sie benötigen eine installierte SD-Karte. Alle verwendeten Sprachen müssen auf der SD-Karte gespeichert sein. SingleCell-Systeme laden die gewünschte Sprache bei Bedarf von der SD-Karte.

15.1.3.1 Allgemein

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Allgemein** nehmen Sie die grundlegenden Einstellungen der Basisstationen vor.

Abb. 104: **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Allgemein**

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Um die Basisstation im System eindeutig zu identifizieren, geben Sie eine Beschreibung für die Basisstation ein.

Feld	Beschreibung
Telefontyp	Zeigt den Typ der Basisstation an. Mögliche Werte: • *elmeg DECT150* • *elmeg DECT200*
Standort	Wählen Sie den Standort der Basisstation aus. Standorte definieren Sie im Menü **VoIP**->**Einstellungen**->**Standorte**. Abhängig von der Einstellung in diesem Menü wird das Standardverhalten für die Registrierung von VoIP-Teilnehmern zur Auswahl angezeigt, für die kein Standort definiert werden soll. Mögliche Werte: • *Nicht definiert (Uneingeschränkte Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer dennoch registriert. • *Nicht definiert (Keine Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nicht registriert. • *Nicht definiert (Registrierung nur in privaten Netzwerken)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nur registriert, wenn er sich im privaten Netzwerk befindet. • *<Standort>*: Es wird ein definierter Standort ausgewählt. Der Teilnehmer wird nur registriert, wenn er sich an diesem Standort befindet.
MAC-Adresse	Zeigt die MAC-Adresse der Basisstation an.
IP/MAC-Bindung	Zeigt die per DHCP automatisch zugewiesene IP-Adresse an. Hier haben Sie die Möglichkeit, der Basisstation mit der angezeigten MAC-Adresse die angezeigte IP-Adresse fest zuzuweisen. Um eine schnelle Wiederanmeldung nach einer Funktionsstörung zu ermöglichen, sollte diese Option aktiv sein.

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

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Kein Halten und Zurückholen	Die Leistungsmerkmale Halten eines Gesprächs und Zurückholen eines gehaltenen Gesprächs stehen bei bestimmten Telefonen nicht zur Verfügung. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Profil	Wählen Sie das Codec-Profil aus, das verwendet werden soll. Codec-Profile konfigurieren Sie im Menü **VoIP**->**Einstellungen**->**Codec-Profile**.

15.1.3.2 Rufnummern

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Rufnummern** weisen Sie den Mobilteilen **Interne Rufnummern** zu. Sie können aus den Rufnummern wählen, die Sie unter **Nummerierung**->**Benutzereinstellungen**->**Benutzer** für diesen Zweck angelegt haben.

Jedem Mobilteil wird vom System automatisch eine laufende Nummer, die **Mobilnummer**, zugeteilt, über die Sie das Gerät identifizieren können. Danach können Sie einem Mobilteil mit **Hinzufügen** genau eine **Interne Rufnummer** aus der Liste zuweisen.

Mit  können Sie zugewiesene Rufnummern löschen.

Abb. 105: **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Rufnummern**

Werte in der Liste Rufnummern

Feld	Beschreibung
Mobilnummer	Zeigt die laufende Nummer des Mobilteils an. Diese Nummer ist dem Mobilteil fest zugeordnet, um es eindeutig identifizieren zu können.
Interne Rufnummer	Zeigt die zugewiesene interne Rufnummer an.
Angezeigte Beschreibung	Zeigt die Beschreibung an, die für die interne Rufnummer eingetragen ist. Diese Beschreibung wird im Ruhemodus auf dem Display des Mobilteils angezeigt.
Benutzer	Zeigt den Namen des Benutzers an.

15.1.3.3 Einstellungen

Im Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Einstellungen** können Sie das Administratorpasswort der Basisstation zurücksetzen.

Abb. 106: **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Einstellungen**

Das Menü **Endgeräte**->**elmeg Systemtelefone**->**elmeg DECT**->**Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Administratorpasswort	Wählen Sie aus, ob das Administratorpasswort zurückgesetzt werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
	Sobald Sie die Schaltfläche **OK** wählen, wird das Passwort auf die Standardeinstellung zurückgesetzt.

15.2 Andere Telefone

In diesem Menü nehmen Sie die Zuordnung der konfigurierten internen Rufnummern zu den Endgeräten vor und stellen weitere Funktionen je nach Endgerätetyp ein.

Die Endgeräte der jeweiligen Kategorie (VoIP, ISDN oder analog) sind in der Spalte **Beschreibung** alphabetisch sortiert. Sie können in jeder beliebigen anderen Spalte auf den Spaltentitel klicken und die Einträge in aufsteigender oder in absteigender Reihenfolge sortieren lassen.

15.2.1 VoIP

Im Menü **Endgeräte**->**Andere Telefone**->**VoIP** konfigurieren Sie die angeschlossenen VoIP-Endgeräte. Sie nehmen z. B. die Zuweisung einer konfigurierten internen Rufnummer vor.

15.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere VoIP-Endgeräte hinzuzufügen.

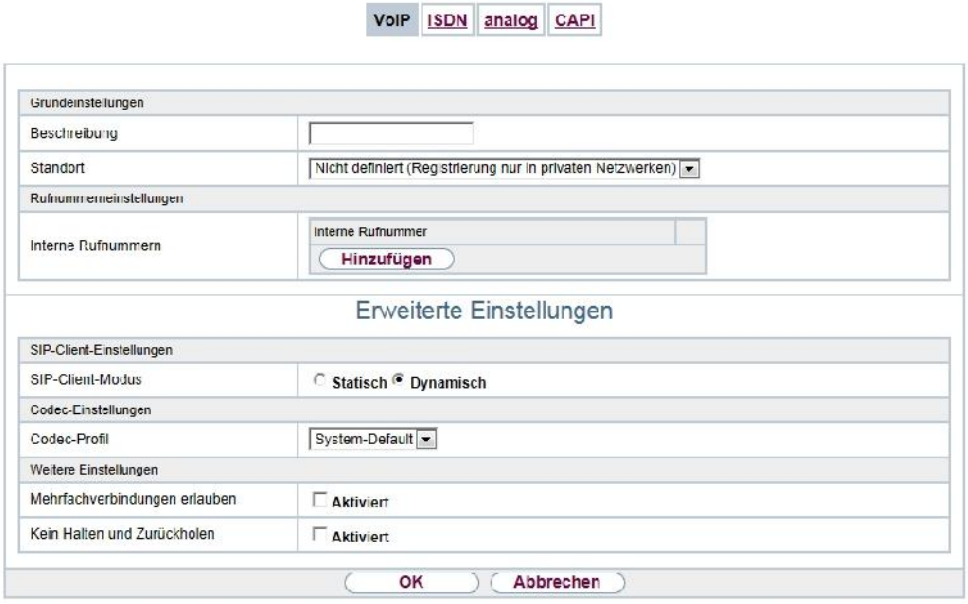


Abb. 107: **Endgeräte->Andere Telefone->VoIP->Neu**

Das Menü **Endgeräte->Andere Telefone->VoIP->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das IP-Telefon ein.
Standort	Wählen Sie den Standort des Telefons aus. Standorte definieren Sie im Menü **VoIP->Einstellungen->Standorte**. Abhängig von der Einstellung in diesem Menü wird das Standardverhalten für die Registrierung von VoIP-Teilnehmern zur Auswahl angezeigt, für die kein Standort definiert werden soll. Mögliche Werte: • *Nicht definiert (Uneingeschränkte Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer dennoch registriert. • *Nicht definiert (Keine Registrierung)*: Es wird kein Standort definiert. Laut festgelegtem Standardverhalten wird der Teilnehmer nicht registriert. • *Nicht definiert (Registrierung nur in privaten Netzwerken)*: Es wird kein Standort definiert. Laut

Feld	Beschreibung
	festgelegtem Standardverhalten wird der Teilnehmer nur registriert, wenn er sich im privaten Netzwerk befindet. • *<Standort>*: Es wird ein definierter Standort ausgewählt. Der Teilnehmer wird nur registriert, wenn er sich an diesem Standort befindet.

Felder im Menü Rufnummerneinstellungen

Feld	Beschreibung
Interne Rufnummern	Wählen Sie die internen Rufnummern für dieses Endgerät aus. Sie können mehrere interne Rufnummern definieren. Mögliche Werte: • *Keine freie Leitung verfügbar*: Alle konfigurierten internen Rufnummern sind schon in Verwendung. Konfigurieren Sie zunächst einen weiteren Benutzer mit internen Rufnummern. • *<Interne Rufnummer>*: Wählen Sie eine der vorhandenen Rufnummern der konfigurierten Benutzer aus.

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

Felder im Menü SIP-Client-Einstellungen

Feld	Beschreibung
SIP-Client-Modus	Wählen Sie aus, ob ein *dynamischer* SIP Client oder ein *statischer* SIP Client verwendet werden soll. Mögliche Werte: • *Dynamisch* (Standardwert): Ihr Gerät (z. B. ein Standard-SIP-Telefon) führt eine SIP-Registrierung durch, um dem System seine (dynamische) IP-Adresse mitzuteilen. • *Statisch* : Ein eingehender Ruf eines (statisch konfigurierten) SIP Clients wird vom System akzeptiert ohne dass sich dieser Client vorher registriert haben muss, wenn die IP-Adresse des Clients mit der eingegebenen IP-Adresse unter **IP-Adresse des SIP-Clients** übereinstimmt. Dieser Modus wird zum Beispiel vom MIcrosoft Office Communications Server und anderen Unified Communication Servern verwendet.
IP-Adresse des SIP-	Nur für **SIP-Client-Modus** = *Statisch*:

Feld	Beschreibung
Clients	Geben Sie die statische lokale IP-Adresse des SIP-Clients ein.
Portnummer	Nur für **SIP-Client-Modus** = *Statisch*: Geben Sie die Nummer des Ports ein, der für die Verbindung genutzt werden soll. Möglich ist eine 5-stellige Ziffernfolge. Für die Anbindung an einen Microsoft Exchange Communication Server ist z. B. der Port *5065* anzugeben.
Transportprotokoll	Nur für **SIP-Client-Modus** = *Statisch*: Wählen Sie das Transportprotokoll für die Verbindung aus. Mögliche Werte: • *UDP* (Standardwert) • *TCP* Für die Anbindung an einen Microsoft Exchange Communication Server ist z. B. das Protokoll *TCP* anzugeben.

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Profil	Wählen Sie das Codec-Profil aus, das verwendet werden soll, wenn über eine VoIP-Leitung verbunden wird. Codec-Profile konfigurieren Sie im Menü **VoIP**->**Einstellungen**->**Codec-Profile**.

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Mehrfachverbindungen erlauben	Wählen Sie aus, ob von diesem Endgerät aus Mehrfachverbindungen gestattet werden sollen. Betrieb als Unteranlage: Nur bei Anschaltung einer Unteranlage an ein System. Hier ist bei ausgeschaltetem Leistungsmerkmal nur eine Verbindung über die Teilnehmer SIP-Registrierung möglich. Erfolgt ein zweiter Anruf, wird dieser angenommen und das bestehende Gespräch gehalten. Bei eingeschaltetem Leistungsmerkmal sind mehrere SIP-Verbindungen über dieselbe Registrierung möglich. Wird das Leistungsmekmal bei einem

Feld	Beschreibung
	System ohne Unteranlage eingeschaltet, werden z. B. zwei gleichzeitig am Telefon bestehende Gespräche, nach Auflegen des Hörers, nicht miteinander verbunden sondern ausgelöst. Hier sollte das Leistungsmerkmal nicht gesetzt werden. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Kein Halten und Zurückholen	Die Leistungsmerkmale „Halten eines Gesprächs“ und „Zurückholen eines gehaltenen Gesprächs“ stehen bei bestimmten Telefonen nicht zur Verfügung. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

15.2.2 ISDN

Im Menü **Endgeräte**->**Andere Telefone**->**ISDN** konfigurieren Sie die angeschlossenen ISDN-Endgeräte. Sie nehmen z. B. die Zuweisung einer konfigurierten internen Rufnummer vor.

15.2.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um eine weiteres ISDN-Endgerät hinzuzufügen.

Abb. 108: **Endgeräte**->**Andere Telefone**->**ISDN**->**Neu**

Das Menü **Endgeräte**->**Andere Telefone**->**ISDN**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das ISDN-Telefon ein.
Schnittstelle	Wählen Sie die Schnittstelle aus, an der das ISDN-Telefon angeschlossen ist.

Felder im Menü Grundlegende Telefoneinstellungen

Feld	Beschreibung
Endgerätetyp	Wählen Sie den Endgeräte-Typ aus. Mögliche Werte: • *Telefon* (Standardwert) • *Anrufbeantworter* • *Voice Mail* • *Notruftelefon*
Interne Rufnummern	Wählen Sie die internen Rufnummern für dieses Endgerät aus. Sie können mehrere interne Rufnummern definieren. Mögliche Werte: • *Keine freie Leitung verfügbar*: Alle konfigurierten internen Rufnummern sind schon in Verwendung. Konfigurieren Sie zunächst einen weiteren Benutzer mit internen Rufnummern. • *<Interne Rufnummer>* : Wählen Sie eine der vorhandenen Rufnummern der konfigurierten Benutzer aus.

15.2.3 Analog

Im Menü **Endgeräte**->**Andere Telefone**->**Analog** konfigurieren Sie die angeschlossenen analogen Endgeräte. Sie nehmen z. B. die Zuweisung einer konfigurierten internen Rufnummer vor.

15.2.3.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Wählen Sie das Symbol , um vorhandene Einträge zu kopieren. Das Kopieren eines Eintrags kann nützlich sein, wenn Sie einen Eintrag anlegen wollen, der sich nur in wenigen Parametern von einem bereits vorhandenen Eintrag unterscheidet. In diesem Fall kopieren Sie den Eintrag und ändern Sie die gewünschten Parameter.

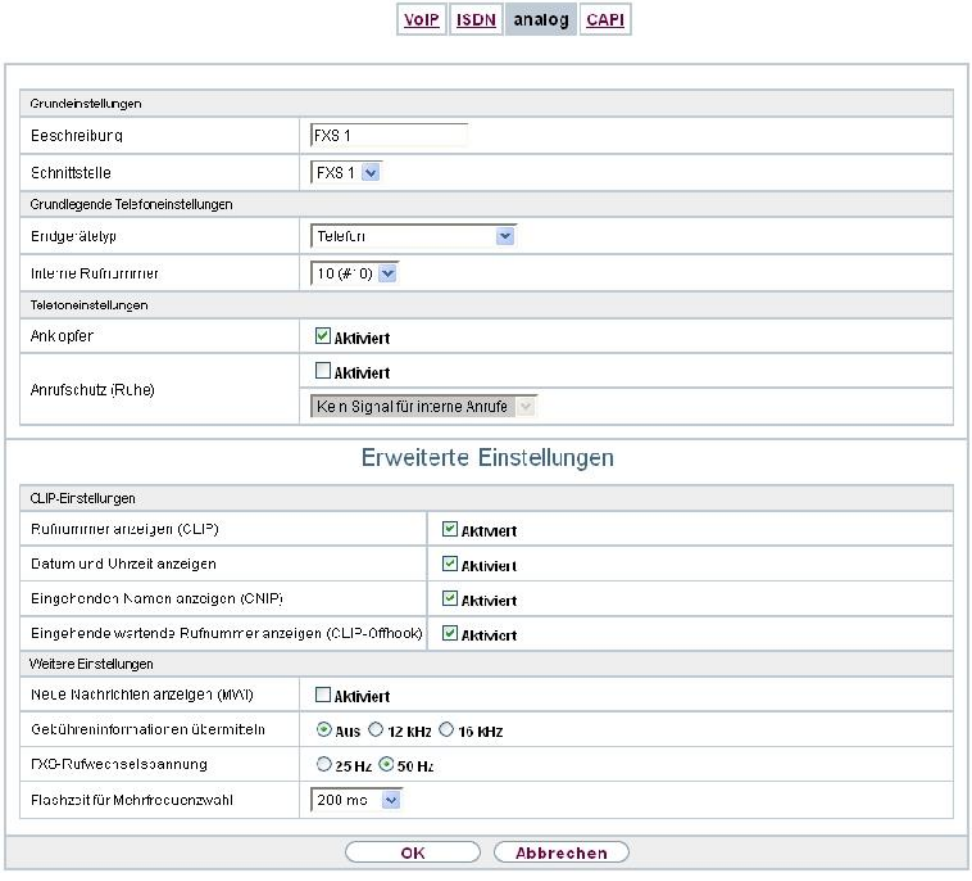


Abb. 109: **Endgeräte->Andere Telefone->Analog->Bearbeiten**

Das Menü **Endgeräte->Andere Telefone->Analog->Bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das analoge Telefon ein.
Schnittstelle	Wählen Sie die Schnittstelle aus, an der das Telefon angeschlossen ist.

Felder im Menü Grundlegende Telefoneinstellungen

Feld	Beschreibung
Endgerätetyp	Wählen Sie den Endgeräte-Typ aus. Mögliche Werte: • *Multifunktionsgerät/Telefax* • *Telefon* • *Modem* • *Anrufbeantworter* • *Notruftelefon*
Interne Rufnummer	Wählen Sie die interne Rufnummer für dieses Endgerät aus. Mögliche Werte: • *Keine freie Leitung verfügbar*: Die konfigurierte interne Rufnummer ist schon in Verwendung. Konfigurieren Sie zunächst einen weiteren Benutzer mit internen Rufnummern. • *<Interne Rufnummer>* : Wählen Sie eine der vorhandenen Rufnummern der konfigurierten Benutzer aus.

Felder im Menü Telefoneinstellungen

Feld	Beschreibung
Anklopfen	Wählen Sie aus, ob für dieses Endgerät Anklopfen erlaubt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Anrufschutz (Ruhe)	Wählen Sie aus, ob Sie das Leistungsmerkmal Anrufschutz (Ruhe vor der Telefon) nutzen wollen. Mit diesem Leistungsmerkmal können Sie die Signalisierung von Anrufen an Ihrem Endgerät schalten. Analoge Endgeräte nutzen dafür Kennziffern des Systems. Mögliche Werte: • *Kein Signal für interne Anrufe* • *Kein Signal für externe Anrufe* • *Keine Anrufe*

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

Felder im Menü CLIP-Einstellungen

Feld	Beschreibung
Rufnummer anzeigen (CLIP)	Wählen Sie aus, ob die Rufnummer des Teilnehmers übertragen werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Datum und Uhrzeit anzeigen	Nur für **Rufnummer anzeigen (CLIP)** *Aktiviert* Wählen Sie aus, ob Datum und Uhrzeit aus Ihrer Telefonanlage übernommen und am Telefon angezeigt werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Eingehenden Namen anzeigen (CNIP)	Nur für **Rufnummer anzeigen (CLIP)** *Aktiviert* Wählen Sie aus, ob der Name des Anrufers angezeigt werden soll. Der Name des Anrufers kann angezeigt werden, wenn im System-Telefonbuch ein Eintrag vorhanden ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Eingehende wartende Rufnummer anzeigen (CLIP-Offhook)	Nur für **Rufnummer anzeigen (CLIP)** *Aktiviert* Wählen Sie aus, ob die Rufnummer eines Anrufers angezeigt werden soll, der während eines bestehenden Anrufs anklopft. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Neue Nachrichten anzeigen (MWI)	Nur für **Rufnummer anzeigen (CLIP)** *Aktiviert* Wählen Sie aus, ob neue Nachrichen auf einem Voice Mail System signalisiert werden sollen.

Feld	Beschreibung
	Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Gebühreninformationen übermitteln	Wählen Sie aus, ob das System aus den Gebühreninformationen des ISDN-Netzes Gebührenimpulse für das Endgerät erzeugen soll. Hierfür können Sie einstellen, ob der Gebührenimpuls 12 kHz oder 16 kHz betragen soll. Mögliche Werte: • *Aus*: Gebühreninformationen aus dem ISDN-Netz werden nicht übermittelt. • *12 kHz* • *16 kHz*
FXS-Rufwechselspannung	Die Signalisierung von Anrufen bei analogen Endgeräten erfolgt über das Anlegen einer Rufwechselspannung an den gerufenen analogen Anschlüssen. Diese Rufwechselspannung wird von dem analogen Endgerät in einen eigenen Tonruf umgewandelt. Im System können Sie für die analogen Anschlüsse eine Rufwechselspannung mit einer Frequenz von *25 Hz* oder *50 Hz* einstellen. Der Standardwert ist *50* Hz.
Flashzeit für Mehrfrequenzwahl	Bei der Nutzung von analogen Endgeräten mit Mehrfrequenzwahlverfahren können Sie die Flashzeit einstellen die das System als maximale Flashlänge erkennt. Ist der Flash vom Endgerät länger als die eingestellte Zeit wird "Hörer aufgelegt“ erkannt. Einstellbar sind Werte von *100 ms* (Standardwert) bis *1000 ms*.

15.2.4 CAPI

Sofern Ihr Gerät CAPI unterstützt, konfigurieren Sie die angeschlossenen CAPI-Endgeräte im Menü **Endgeräte**->**Andere Telefone**->**CAPI**. Sie nehmen z. B. die Zuweisung einer konfigurierten internen Rufnummer vor.

15.2.4.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um eine weiteres CAPI-Endgerät hinzuzufügen.

Abb. 110: **Endgeräte->Andere Telefone->CAPI->Neu**

Das Menü **Endgeräte->Andere Telefone->CAPI->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das CAPI-Telefon ein.

Felder im Menü Grundlegende Telefoneinstellungen

Feld	Beschreibung
Interne Rufnummern	Mit **Hinzufügen** wählen Sie die internen Rufnummern für dieses Endgerät aus. Sie können mehrere interne Rufnummern definieren. Mögliche Werte: • *Keine freie Leitung verfügbar*: Alle konfigurierten internen Rufnummern sind schon in Verwendung. Konfigurieren Sie zunächst einen weiteren Benutzer mit internen Rufnummern. • *<Interne Rufnummer>* : Wählen Sie eine der vorhandenen Rufnummern der konfigurierten Benutzer aus.

15.3 Übersicht

15.3.1 Übersicht

Im Menü **Endgeräte**->**Übersicht**->**Übersicht** sehen Sie eine Übersicht über alle konfigurierten Endgeräte.

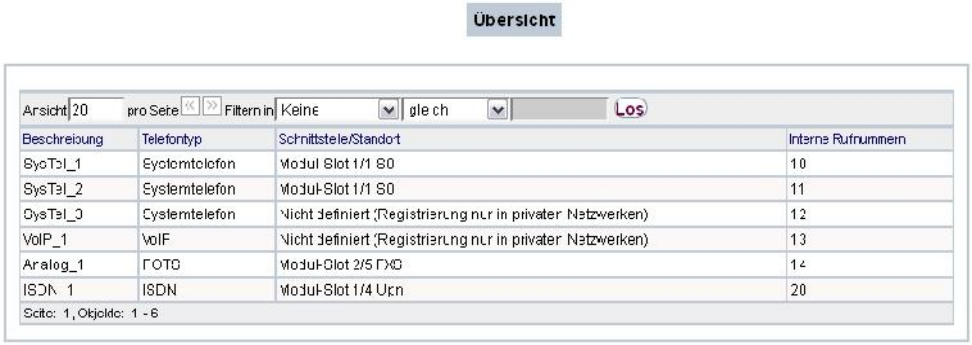


Abb. 111: **Endgeräte->Übersicht->Übersicht**

Werte in der Liste Übersicht

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Endgeräts an.
Telefontyp	Zeigt den Telefontyp an.
Schnittstelle/Standort	Zeigt bei ISDN-, System- und analogen Endgeräten die Schnittstelle an, an der sie am System angeschlossen sind. Bei IP-Endgeräten wird der konfigurierte Standort angezeigt.
Interne Rufnummern	Zeigt die konfigurierten internen Rufnummern an.

Kapitel 16 Anrufkontrolle

In der Anrufkontrolle werden die Funktionen für externe Anrufe, externe Gespräche und die Wahlregeln für externe Gespräche festgelegt.

16.1 Ausgehende Dienste

Im Menü **Anrufkontrolle**->**Ausgehende Dienste** können Sie die Leistungsmerkmale **Direktruf**, **Anrufweiterschaltung (AWS)**, **Wahlkontrolle** und **Vorrangrufnummern** konfigurieren.

16.1.1 Direktruf

Im Menü **Anrufkontrolle**->**Ausgehende Dienste**->**Direktruf** konfigurieren Sie Rufnummern, die direkt gewählt werden, ohne dass der Teilnehmer am Telefon selber eine Nummer wählen muss.

Sie möchten ein Telefon einrichten, bei dem die Verbindung zu einer bestimmten Rufnummer auch ohne die Eingabe der Rufnummer aufgebaut wird (z. B. Notruftelefon). Sie befinden sich außer Haus. Es gibt jedoch jemanden zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Haben Sie für ein oder mehrere Telefone die Funktion "Direktruf" eingerichtet, braucht nur der Hörer des entsprechenden Telefons abgehoben zu werden. Nach einer in der Konfigurierung eingestellten Zeit ohne weitere Eingaben wählt das System automatisch die festgelegte Direktrufnummer.

Wählen Sie nach dem Abheben des Hörers nicht innerhalb der vorgegebenen Zeit, wird die automatische Wahl eingeleitet.

Die Zeit für den Direktruf wird unter **Systemverwaltung**->**Globale Einstellungen**->**Timer**->**Direktruf** eingestellt.

Hinweis

Im System lassen sich bis zu 10 Direktruf-Ziele vom Administrator mit Namen und Telefonnummer einrichten. Diese Ziele müssen dann nur vom Benutzer über die Benutzer-Konfigurationsoberfläche den Endgeräten zugewiesen werden. In der Konfiguration kann dann der System-Direktruf oder ein eigens für das Endgerät eingerichteter Direktruf vom Benutzer eingestellt werden.

16.1.1.1 Bearbeiten oder Neu

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

Abb. 112: **Anrufkontrolle->Ausgehende Dienste->Direktruf->Neu**

Das Menü **Anrufkontrolle->Ausgehende Dienste->Direktruf->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.
Direktrufnummer	Geben Sie die Rufnummer ein, die automatisch gewählt werden soll, wenn nach Abheben des Hörers für eine bestimmte Zeit keine andere Rufnummer gewählt wird.

16.1.2 Anrufweiterschaltung (AWS)

Im Menü **Anrufkontrolle->Ausgehende Dienste->Anrufweiterschaltung (AWS)** konfigurieren Sie Anrufweiterschaltungen von externen Anrufen für einen internen Teilnehmer.

Sie sind vorübergehend nicht in Ihrem Büro und möchten dennoch keinen Anruf verpassen. Mit einer Anrufweiterschaltung zu einer anderen Rufnummer, z. B. Ihr Handy, können Sie Ihre Anrufe auch annehmen, wenn Sie nicht am Platz sind. Sie können Anrufe für Ihre Rufnummer zu einer beliebigen Rufnummer weiterschalten. Sie kann `Sofort`, `Bei Nichtmelden` oder `Bei Besetzt` erfolgen. Anrufweiterschaltungen `Bei Nichtmelden` und `Bei Besetzt` können gleichzeitig bestehen. Sind Sie z. B. nicht in der Nähe Ihres Telefons, wird der Anruf nach einer kurzen Zeit zu einer anderen Rufnummer (z. B. Ihr Handy) weitergeschaltet. Führen Sie bereits ein Telefongespräch an Ihrem Arbeitsplatz, erhalten weitere Anrufer möglicherweise "besetzt". Diese Anrufer können Sie mit einer Anrufweiterschaltung bei besetzt z. B. zu einem Kollegen oder dem Sekretariat weiterschalten.

Jeder interne Teilnehmer des Systems kann seine Anrufe zu einer anderen Rufnummer weiterschalten. Die Anrufweiterschaltung kann dabei zu internen Teilnehmer-Rufnummern, internen Team-Rufnummern oder externen Rufnummern erfolgen. Bei der Eingabe der Rufnummer, zu der die Anrufe weitergeschaltet werden sollen, prüft das System automatisch, ob es sich um eine interne oder um eine externe Rufnummer handelt.

Bei einem Team kann die Anrufweiterschaltung für einen Teilnehmer im Team eingerichtet sein. Bei den anderen Teilnehmern im Team wird dieser Anruf weiterhin signalisiert. Die Anrufweiterschaltung zu einem internen oder externen Teilnehmer wird dabei im System ausgeführt.

Die Anrufweiterschaltung zu einer internen Rufnummer wird im System ausgeführt. Soll ein interner Anruf zu einer externen Rufnummer weitergeleitet werden, wird die Weiterleitung ebenfalls im System ausgeführt. Die Verbindung wird dabei über das Bündel aufgebaut, welches für den einrichtenden Teilnehmer freigegeben ist. Erfolgt die Anrufweiterschaltung über einen ISDN-Anschluss, bleibt ein oder bei einer Weiterschaltung von extern nach extern auch beide B-Kanäle belegt. Für die Anrufweiterschaltung eines externen Anrufes zu einer externen Rufnummer gibt es zwei Möglichkeiten:

- Anrufweiterschaltung in der Vermittlungsstelle: Die Anrufweiterschaltung wird in der Vermittlungsstelle ausgeführt, wenn bei einem externen Anruf nur ein interner Teilnehmer in der Anrufverteilung eingetragen ist. Für eine Anrufweiterschaltung in der Vermittlungsstelle müssen für die betreffenden ISDN-Anschlüsse beim Netzbetreiber die Leistungsmerkmale Call Deflection (Mehrgeräteanschluss) oder Partial Rerouting (Anlagenanschluss) aktiviert sein.
- Anrufweiterschaltung im System: Die Anrufweiterschaltung wird im System ausgeführt, wenn für die betreffenden ISDN-Anschlüsse die notwendigen Leistungsmerkmale für eine Anrufweiterschaltung in der Vermittlungsstelle nicht verfügbar sind. Werden bei einem externen Anruf mehrere Telefone (z. B. ein Team) gerufen, von denen einzelne eine Anrufweiterschaltung eingerichtet haben, wird die entsprechende Anrufweiterschaltung im System ausgeführt. Die externe Verbindung wird dabei über den B-Kanal eines Bündels aufgebaut, welches für den einrichtenden Teilnehmer freigegeben ist. Für die Dauer einer aktiven Anrufweiterschaltung bleibt dieser B-Kanal belegt.

Hinweis

Ist das System an das externe ISDN angeschlossen, versucht das System bei Extern-zu-extern-Verbindungen grundsätzlich die Anrufweiterschaltung über die Vermittlungsstelle einzuleiten. Für Teams kann manuell in der Konfiguration festgelegt werden, ob die Anrufweiterschaltung über die Vermittlungsstelle oder das System erfolgen soll. Besitzt das System keine ISDN-Anschlüsse oder ist Call Deflection (Mehrgeräteanschluss) oder Partial Rerouting (Anlagenanschluss) nicht beim Netzbetreiber beauftragt, erfolgt die Anrufweiterschaltung nur im System.

16.1.2.1 Bearbeiten oder Neu

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

Abb. 113: **Anrufkontrolle->Ausgehende Dienste->Anrufweiterschaltung (AWS) ->Neu**

Das Menü **Anrufkontrolle->Ausgehende Dienste->Anrufweiterschaltung (AWS) ->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Interne Rufnummer	Wählen Sie die interne Rufnummer aus, für die kommende Anrufe weitergeschaltet werden sollen.
Art der Anrufweiterschaltung	Wählen Sie aus, wann kommende Anrufe auf die angegebene interne Rufnummer weitergeschaltet werden sollen. Mögliche Werte: • *Sofort* • *Bei Besetzt* • *Bei Nichtmelden* (Standardwert) • *Bei Besetzt / Bei Nichtmelden*
Zielrufnummer "Bei Nichtmelden"	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei Nichtmelden weitergeschaltet werden sollen.
Zielrufnummer "Bei besetzt"	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei besetzt weitergeschaltet werden sollen.
Zielrufnummer "Sofort"	Geben Sie die Rufnummer ein, auf die kommende Anrufe sofort weitergeschaltet werden sollen.

16.1.3 Wahlkontrolle

Im Menü **Anrufkontrolle**->**Ausgehende Dienste**->**Wahlkontrolle** sperren Sie bestimmte Rufnummern/Teilrufnummern oder Sie geben diese frei.

Sie möchten die Wahl bestimmter Rufnummern im System verhindern, z. B. die Rufnummern von teuren Mehrwertdiensten. Tragen Sie diese Rufnummern oder Teilrufnummern in die Liste der gesperrten Rufnummern der Wahlkontrolle ein. Alle Teilnehmer, die der Wahlkontrolle unterliegen, können diese Rufnummern nicht wählen. Sollten Sie bestimmte Rufnummern aus einem gesperrten Bereich dennoch benötigen, können Sie diese über die Liste der freigegebenen Rufnummern der Wahlkontrolle freigeben.

Mit der Liste der gesperrten Rufnummern können Sie bestimmte Rufnummern oder Vorwahlen sperren. Mit der Liste der freigegebenen Rufnummern können Sie gesperrte Rufnummern oder Vorwahlen freigeben. Ist eine Rufnummer, die als freigegebene Rufnummer eingetragen ist, länger als eine Rufnummer, die als gesperrte Rufnummer eingetragen ist, kann diese Rufnummer gewählt werden. Wenn Sie eine Rufnummer wählen, wird die Wahl nach der gesperrten Ziffer abgebrochen und Sie hören den Besetztton. In den Benutzereinstellungen können Sie jeden Benutzer einzeln der Wahlkontrolle zuordnen.

Beispiel: Gesperrte Rufnummer *01*, alle externen Rufnummern die mit *01* beginnen sind gesperrt. Freigegebene Rufnummer *012345*, die Wahl kann erfolgen. Alle externen Rufnummern, die mit *012345* beginnen können gewählt werden. Sind zwei gleiche Rufnummern (gleiche Ziffernfolge und gleiche Anzahl von Ziffern, z. B. *01234* und *01234*) sowohl in der Liste der freigegebene Rufnummern als auch die der gesperrten Rufnummern eingetragen, wird die Wahl der Rufnummer verhindert.

Hinweis

Über die Liste der freigegebenen Rufnummern werden Teilnehmer, die halbamtsberechtigt oder nichtamtsberechtigt sind (keine externe Wahlberechtigung besitzen), zur externen Wahl der freigegebenen Rufnummer berechtigt.

Beachten Sie, dass die Ortsnetzkennzahl in der Konfigurierung eingetragen ist, sonst kann die gesperrte Rufnummer im Ortsnetz durch die Vorwahl der Ortsnetzkennzahl umgangen werden.

16.1.3.1 Bearbeiten oder Neu

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

Abb. 114: **Anrufkontrolle->Ausgehende Dienste->Wahlkontrolle->Neu**

Das Menü **Anrufkontrolle->Ausgehende Dienste->Wahlkontrolle->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Gesperrte Rufnummer	Geben Sie die Nummer ein, deren Wahl verhindert werden soll.
Freigegebene Rufnummer	Geben Sie die Nummer ein, deren Wahl explizit erlaubt sein soll.

16.1.4 Vorrangrufnummern

Im Menü **Anrufkontrolle->Ausgehende Dienste->Vorrangrufnummern** konfigurieren Sie Rufnummern mit bestimmten Sonderfunktionen z. B. Notruffunktionen.

Sie können in der Konfiguration Ihres Systems Rufnummern eintragen, die im Notfall erreichbar sein müssen. Wählen Sie nun eine dieser Vorrangrufnummern, wird dieses vom System erkannt und automatisch ein ISDN-B-Kanal freigeschaltet. Sind die externen ISDN-B-Kanäle bereits benutzt, wird ein ISDN-B-Kanal freigeschaltet und die telefonierenden Teilnehmer hören den Besetztton. Ein bereits bestehender Vorrangruf wird nicht unterbrochen.

16.1.4.1 Bearbeiten oder Neu

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

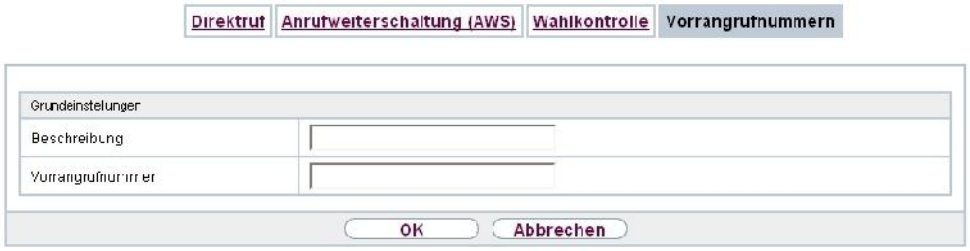


Abb. 115: **Anrufkontrolle->Ausgehende Dienste->Vorrangrufnummern ->Neu**

Das Menü **Anrufkontrolle->Ausgehende Dienste->Vorrangrufnummern ->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.
Vorrangrufnummer	Geben Sie die Nummer ein, die auch gewählt werden kann, wenn alle B-Kanäle des Systems besetzt sind. Es wird dann ein externer B-Kanal für diese Verbindung getrennt und für den Vorrrangruf neu belegt. Ein bereits bestehender Vorrrangruf wird nicht unterbrochen.

16.2 Wahlregeln

Im Menü **Anrufkontrolle->Wahlregeln** können Sie zusätzlich zur konfigurierten Leitungsbelegung Routen für die Wahl nach extern einrichten. Hierbei können gezielt für die Benutzer freigegebene Bündel je nach gewählter Rufnummer für gehende Gespräche belegt werden, oder neue Provider mit deren Netzzugangsvorwahl eingetragen werden. Das Routing legen Sie dann für individuell angelegte Zonen für jeden Wochentag einzeln fest.

16.2.1 Allgemein

Im Menü **Anrufkontrolle->Wahlregeln->Allgemein** aktivieren Sie die Funktion ARS - Automatic Route Selection - und wählen die gewünschte Routing-Stufe.

Abb. 116: **Anrufkontrolle->Wahlregeln->Allgemein**

Das Menü **Anrufkontrolle->Wahlregeln->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
ARS	Wählen Sie aus, ob Sie das Leistungsmerkmal ARS (Automatic Route Selection) aktivieren möchten. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Routingstufe	Wählen Sie aus, ob bei Nichterreichbarkeit eines eingetragenen Providers oder Bündels auf weitere Routen zurückgegriffen werden soll. Mögliche Werte: • *1 (Kein Fallback)*: Ist der eingetragene Provider oder das ausgewählte Bündel (**Anrufkontrolle->Wahlregeln->Zonen &Routing-> Bearbeiten/Hinzufügen -> Mo-So ->Routing-Stufe 1**) nicht verfügbar, wird der Verbindungsaufbau abgebrochen. • *2*: Ist der eingetragene Provider oder das ausgewählte Bündel (**Anrufkontrolle->Wahlregeln->Zonen &Routing-> Bearbeiten/Hinzufügen -> Mo-So ->Routing-Stufe 1**) nicht verfügbar, wird versucht, die Verbindung über die zusätzlich eingetragene Routing-Variante (**Anrufkontrolle->Wahlregeln->Zonen &Routing-> Bearbeiten/Hinzufügen -> Mo-So ->Routing-Stufe 2**) einzuleiten. • *3* (Standardwert): Ist keiner der beiden eingetragenen Provider oder Bündel (**Anrufkontrolle->Wahlregeln->Zonen &Routing-> Bearbeiten/Hinzufügen -> Mo-So ->Routing-Stufe 1** und **Routing-Stufe 2**) verfügbar, wird über den für den Benutzer als Standard eingetragenen Provider (**Nummerie-**

Feld	Beschreibung
	rung->**Berechtigungsklasse**->**Hinzufügen**->**Grundeinstellungen**->**Leitungsbelegung mit Amtskennziffer**) gewählt.

16.2.2 Schnittstellen/Provider

Im Menü **Anrufkontrolle**->**Wahlregeln**->**Schnittstellen/Provider** tragen Sie die Routen bzw. Provider und deren Netzzugangsvorwahl ein.

16.2.2.1 Bearbeiten oder Neu

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

Abb. 117: **Anrufkontrolle**->**Wahlregeln**->**Schnittstellen/Provider**->**Neu**

Das Menü **Anrufkontrolle**->**Wahlregeln**->**Schnittstellen/Provider**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.
Routing-Modus	Wählen Sie aus, wie eine Wahl nach extern geroutet werden soll. Mögliche Werte: • `Standard` (Standardwert): Das Standardverfahren sieht vor, dass beim Wählen nach extern die unter **Provider-Vorwahl** eingegebene Vorwahl vorangestellt wird. • `Route`: Die Wahl nach extern wird über das in **Route** ausgewählte Bündel aufgebaut.

Feld	Beschreibung
Provider-Vorwahl	Geben Sie die Rufnummer ein, die als Vorwahl beim Ruf nach extern vorangestellt werden soll, um z. B. über einen Call-by-Call-Anbieter eine Verbindung aufzubauen.
Route	Nur bei **Routing-Modus** = `Route`. Wählen Sie das Bündel aus, über das die Wahl nach extern erfolgen soll.

16.2.3 Zonen &Routing

Im Menü **Anrufkontrolle**->**Wahlregeln**->**Zonen &Routing** definieren Sie die Zonen, über die mittels bestimmter Routen oder Provider gewählt werden soll.

Die Konfiguration der Routingtabellen erfolgt für die eingerichteten Zonen jeweils für jeden Wochentag einzeln. Je zwei Routingtabellen, Routing-Stufe 1 und Routing-Stufe 2 als Fallback können eingerichtet werden.

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

16.2.3.1 Rufnummern

Im Bereich **Rufnummern** tragen Sie die Rufnummern oder Teilrufnummern der Zonen ein, für die Sie die Routingtabellen einrichten wollen.

Abb. 118: **Anrufkontrolle->Wahlregeln->Zonen & Routing->Rufnummern**

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein.
Zonen	Konfigurieren Sie die gewünschten externen Zonen, zu denen über die gewünschten eingetragenen Provider/Routen gewählt werden soll. Mögliche Werte: • *Rufnummer/Teilrufnummer*: Geben Sie die Rufnummer oder den Teil der Rufnummer ein, die eine Zone kennzeichnet. • *Name*: Geben Sie einen Namen für diese Zone ein.

16.2.3.2 Mo - So

Im Bereich **Mo** - **So** wählen Sie für jede Routing-Stufe die gewünschten Uhrzeiten aus und die gewünschte Route bzw. den gewünschten Provider, über den gehende Rufe ab der eingetragenen Uhrzeit geroutet werden sollen.

Abb. 119: **Anrufkontrolle->Wahlregeln->Zonen & Routing->Mo**

Felder im Menü <Wochentag>

Feld	Beschreibung
Routing-Stufe 1	Konfigurieren Sie für die Routing-Stufe 1 die Umschaltzeiten. Wählen Sie dazu zunächst die **Startzeit** aus, ab wann über eine bestimmte Schnittstelle oder einen bestimmten Netzbetreiber geroutet werden soll und wählen Sie diesen unter **Schnittstelle/Netzbetreiber** aus.

Feld	Beschreibung
Routing-Stufe 2	Konfigurieren Sie für die Routing-Stufe 2 die Umschaltzeiten. Wählen Sie dazu zunächst die **Startzeit** aus, ab wann über eine bestimmte Schnittstelle oder einen bestimmten Netzbetreiber geroutet werden soll und wählen Sie diesen unter **Schnittstelle/Netzbetreiber** aus.

Kapitel 17 Anwendungen

Unter **Anwendungen** werden interne Telefon-Leistungsmerkmale des Systems eingerichtet.

17.1 Kalender

Im Menü **Anwendungen**->**Kalender** können Sie entscheiden, ob sie neue Einträge oder Änderungen im Kalender vornehmen möchten.

In jedem Unternehmen gibt es feste Geschäftszeiten. Diese Zeiten können Sie in den internen Kalendern des Systems speichern. So können zum Beispiel alle Anrufe außerhalb der Geschäftszeiten an einem Vermittlungsplatz oder einem Anrufbeantworter signalisiert werden. Ihre Mitarbeiter können in dieser Zeit andere Aufgaben erledigen, ohne von Telefonanrufen unterbrochen zu werden. Die einzelnen Anrufvarianten eines Teams werden automatisch durch die Kalender umgeschaltet.

Sie möchten nach Feierabend für bestimmte Teilnehmer die Berechtigungen für externe Gespräche ändern. In der Konfiguration des Systems können Sie für jeden Benutzer separat festlegen, ob die Berechtigung für Externgespräche automatisch umgeschaltet werden soll. Die Umschaltung erfolgt gemäß den Daten im zugewiesenen Kalender.

Sie können im System fünf Arten von Kalendern einrichten. Die Kalender "Berechtigungsklasse“ und "Nachtbetrieb“ sind für zentrale Umschaltungen vorgesehen und können nur einmal eingerichtet werden. Die Kalender "Team-Signalisierung“, "TFE-Signalisierung“ und "Abwurf auf interne/externe Rufnummer“ können mehrfach eingerichtet werden. Für jeden Wochentag können mehrere unterschiedliche Umschaltzeiten gewählt werden.

Allen Leistungsmerkmalen, bei denen mehrere Varianten eingerichtet werden können (z. B. Teams), kann in der Konfiguration ein Kalender zugewiesen werden. Die Umschaltung zwischen den einzelnen Anrufvarianten erfolgt dann zu den Schaltzeiten des zugewiesenen Kalenders.

17.1.1 Kalender

Im Menü **Anwendungen**->**Kalender**->**Kalender** können Sie einen bereits eingerichteten Kalender ansehen, ändern oder kopieren sowie neue Kalender erstellen.

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

17.1.1.1 Allgemein

Im Bereich **Allgemein** legen Sie den Namen des zu erstellenden Kalenders fest.

Abb. 120: **Anwendungen->Kalender->Kalender->Allgemein**

Das Menü **Anwendungen->Kalender->Kalender->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Kalender ein.
Anwendung	Wählen Sie aus, für welche Anwendung der Kalender verwendet werden soll. Beachten Sie, dass dieses Feld bei bestehenden Einträgen nicht editiert werden kann. Soll eine andere Anwendung konfiguriert werden, ist es notwendig, einen neuen Eintrag anzulegen und den bestehenden zu löschen. Mögliche Werte: • *Team-Signalisierung* (Standardwert): Hier können mehrere Kalender eingerichtet werden. • *TFE-Signalisierung*: Hier können mehrere Kalender eingerichtet werden. • *Nachtbetrieb*: Hier kann nur ein Kalender eingerichtet werden. • *Berechtigungsklasse*: Hier kann nur ein Kalender eingerichtet werden. • *Abwurf auf interne/externe Rufnummer*: Hier kön-

Feld	Beschreibung
	nen mehrere Kalender eingerichtet werden. • *Voice Mail System*: Hier können mehrere Kalender eingerichtet werden. • *Meldeeingang*: Hier können mehrere Kalender eingerichtet werden.

17.1.1.2 Mo - So / Ausnahme

Mo - So

Im Bereich **Mo - So** richten die Schalttage und Schaltzeiten für diesen Kalender ein.

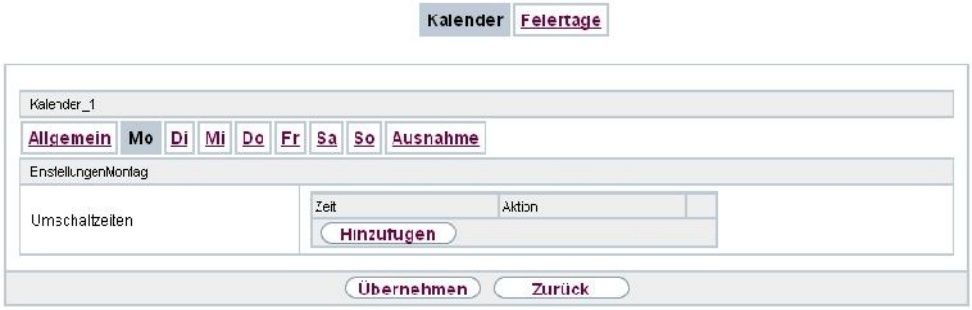


Abb. 121: **Anwendungen->Kalender->Kalender->Mo - So**

Das Menü **Anwendungen->Kalender->Kalender->Mo - So** besteht aus folgenden Feldern:

Felder im Menü <Wochentag>

Feld	Beschreibung
Umschaltzeiten	Geben Sie die gewünschten Umschaltzeiten ein. Wählen Sie hierzu für jeden Wochentag unter **Zeit** die gewünschten Schaltpunkte aus, an denen von einer ggf. abweichenden aktiven Schaltvariante in die unter **Aktion** ausgewählte gewünschte Schaltvariante umgeschaltet werden soll. Folgende Schaltvarianten stehen je nach Anwendung zur Verfügung: • *Team-Signalisierung* : Anrufvariante 1 bis Anrufvariante 4

Feld	Beschreibung
	• *TFE-Signalisierung*: TFE-Anrufvariante 1 und TFE-Anrufvariante 2 • *Nachtbetrieb*: Nachtbetrieb an und Nachtbetrieb aus • *Berechtigungsklasse*: Berechtigungsklasse Standard und Berechtigungsklasse Optional • *Abwurf auf interne/externe Rufnummer*: Abwurfvariante 1 bis Abwurfvariante 4 • *Voice Mail System*: Aktion Im Büro und Außer Haus • *Meldeeingang*: Nachtbetrieb an und Nachtbetrieb aus.
Einstellungen übernehmen von	Nur wenn schon Einstellungen für einen Wochentag vorgenommen wurden. Wählen Sie aus, von welchem Wochentag die Einstellungen übernommen werden sollen. Wenn Sie für diesen Tag spezifische Einstellungen benötigen, wählen Sie die Option *Individuell* aus.

Ausnahme

Im Bereich **Ausnahme** wählen Sie aus, ob und wie Feiertage berücksichtigt werden sollen.

Abb. 122: **Anwendungen->Kalender->Kalender->Ausnahme**

Das Menü **Anwendungen->Kalender->Kalender->Ausnahme** besteht aus folgenden Feldern:

Felder im Menü Einstellungen Feiertage

Feld	Beschreibung
Feiertage berücksichtigen	Wählen Sie aus, ob die im Menü **Anwendungen**->**Kalender**->**Feiertage** eingetragenen Termine in diesem Kalender ebenfalls berücksichtig werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Einstellungen übernehmen von	Nur wenn **Feiertage berücksichtigen** aktiviert. Wählen Sie aus, von welchem Wochentag die Einstellungen für Feiertage übernommen werden sollen. Die Wochentage konfigurieren Sie im Menü **Anwendungen**->**Kalender**->**Kalender**->**Mo - So** Wenn Sie für Feiertage spezifische Einstellungen benötigen, wählen Sie die Option *Individuell* aus.
Umschaltzeiten	Nur für **Einstellungen übernehmen von** = *Individuell*. Geben Sie die gewünschten Umschaltzeiten ein. Wählen Sie hierzu unter **Zeit** die gewünschten Schaltpunkte aus, an denen von einer ggf. abweichenden aktiven Schaltvariante in die unter **Aktion** ausgewählte gewünschte Schaltvariante umgeschaltet werden soll. Folgende Schaltvarianten stehen je nach Anwendung zur Verfügung: • *Team-Signalisierung* : Anrufvariante 1 bis Anrufvariante 4 • *TFE-Signalisierung*: TFE-Anrufvariante 1 und TFE-Anrufvariante 2 • *Nachtbetrieb*: Nachtbetrieb und Nachtbetrieb aus • *Berechtigungsklasse*: Berechtigungsklasse Standard und Berechtigungsklasse Optional • *Abwurf auf interne/externe Rufnummer*: Abwurfvariante 1 bis Abwurfvariante 4 • *Voice Mail System*: Aktion Im Büro und Außer Haus • *Meldeeingang*: Nachtbetrieb an und Nachtbetrieb aus.

17.1.2 Feiertage

Im Menü **Anwendungen**->**Kalender**->**Feiertage** können Sie Feiertage oder beliebige besondere Tage eintragen, an denen über den Kalender abweichende Einstellungen erfolgen sollen. Die Feiertagseinträge werden nach Datum sortiert!

17.1.2.1 Bearbeiten oder Neu

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

Abb. 123: **Anwendungen**->**Kalender**->**Feiertage**->**Neu**

Das Menü **Anwendungen**->**Kalender**->**Feiertage**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Feiertag ein.
Datum (TT-MM)	Geben Sie das Datum mit Tag und Monat in zweistelliger Schreibweise ein. Fehlerhafte Eintragungen, z. B. der 31.02., werden angenommen und gespeichert, aber vom System nicht ausgeführt.

17.2 Abwurf

Im Menü **Anwendungen**->**Abwurf** konfigurieren Sie, wie im System mit kommenden Anrufen standardmäßig verfahren werden soll.

17.2.1 Abwurffunktionen

Im Menü **Anwendungen**->**Abwurf**->**Abwurffunktionen** können Sie verschiedene Abwurfvarianten einrichten für *Direkt*, *Bei Besetzt*, *Bei Nichtmelden* oder *Bei Besetzt und Bei Nichtmelden*. Diese Abwurfvarianten weisen Sie dann im Menü **Nummerierung**->**Rufverteilung**->**Anrufzuordnung** den externen Anschlüssen zu.

17.2.1.1 Bearbeiten oder Neu

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

Abb. 124: **Anwendungen**->**Abwurf**->**Abwurffunktionen**->**Neu**

Das Menü **Anwendungen**->**Abwurf**->**Abwurffunktionen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die Abwurffunktion ein.
Typ der Abwurffunktion	Wählen Sie die gewünschte Vermittlungsfunktion aus. Mögliche Werte: • *Direkt* (Standardwert) • *Bei Besetzt*

Feld	Beschreibung
	• *Bei Nichtmelden* • *Bei Besetzt und Bei Nichtmelden*

Felder im Menü Einstellungen bei Besetzt

Feld	Beschreibung
Anzahl der Teilnehmer in der Warteschleife	Nur für **Typ der Abwurffunktion** = *Bei Besetzt* oder *Bei Besetzt und Bei Nichtmelden*: In diesem Feld können Sie die max. Anzahl von Teilnehmern in der Warteschlange einrichten. Die Warteschlange kann bis zu 10 Teilnehmer umfassen. Weitere Anrufer erhalten "besetzt" signalisiert. Mögliche Werte sind *0* (keine Warteschlange) bis *10*. Der Standardwert ist *0*.
Wartende Anrufe annehmen mit	Nur für **Typ der Abwurffunktion** = *Bei Besetzt* oder *Bei Besetzt und Bei Nichtmelden*: Stellen Sie ein, was Anrufer in der Warteschlange hören (interne oder konfigurierte Wartemusik, Ansage). Mögliche Werte: • *MoH Wave 1* bis *MoH Wave 8* • *MoH Intern 1* (Standardwert) • *MoH Intern 2* • *Aus*
Max. Wartezeit in Warteschleife	Nur für **Typ der Abwurffunktion** = *Bei Besetzt* oder *Bei Besetzt und Bei Nichtmelden*: Stellen Sie die Zeit ein, die ein Anrufer maximal in der Warteschlange verbringt. Nach Ablauf dieser Zeit wird der Anrufer zu dem eingestellten Abwurfziel weitervermittelt. Belassen Sie *Endlos* für eine endlose Warteschlange (entspricht dem Wert 0). Deaktivieren Sie *Endlos*, um den gewünschten Wert einzugeben.

Felder im Menü Einstellungen bei Nichtmelden

Feld	Beschreibung
Zeit für Rerouting bei Nichtmelden	Stellen Sie die Zeit ein, die ein Anrufer maximal in der Warteschlange verbringt, wenn er die Zielrufnummer nicht erreicht. Nach Ablauf dieser Zeit wird der Anrufer zu dem eingestellten Abwurfziel weitervermittelt. Der Standardwert ist *30* Sekunden.

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Ansage	Wählen Sie aus, ob der kommende Anruf auf eine Ansage abgeworfen werden soll. Mögliche Werte: • *Aus* (Standardwert): Der kommende Anruf wird nicht auf eine Ansage abgeworfen. • *MoH Wave 1* bis *MoH Wave 8*
Zielrufnummer	Wählen Sie die interne Rufnummer aus, auf die der kommende Anruf abgeworfen werden soll. Mögliche Werte: • *Keine Rufnummer (Verbindungsunterbrechung)*: Der Anruf wird abgebrochen, die Verbindung getrennt. • *<Rufnummer>*: Ist eine Zielrufnummer eingetragen, wird weitervermittelt.
Weitervermitteln mit	Der Anrufer hört die hier eingestellte Ansage oder Musik während sein Gespräch weitervermittelt wird. Mögliche Werte: • *Freiton* • *MoH Wave 1* bis *MoH Wave 8* • *MoH Intern 1* • *MoH Intern 2* • *<Wave-Datei>*

Ansage vor Abfrage

Sie haben eine allgemeine Info-Rufnummer eingerichtet, auf der Kunden mit den verschiedensten Problemen oder Anliegen anrufen. Natürlich kann nicht ein Mitarbeiter oder ein Team zu allen Themengebieten Auskunft erteilen. Der Anrufer müsste dann zu den einzelnen Fachabteilungen weitervermittelt werden. Wenn Sie bereits vorher wüssten, welches Anliegen (Themengebiet) ein Anrufer hat, könnten Sie ihn sofort zu der richtigen Fachabteilung vermitteln. Auf diese Weise müssen Ihre Anrufer nicht erst von einem Vermittlungsplatz angenommen und weitervermittelt werden. Jeder Anrufer entscheidet selbst, mit welchem Mitarbeiter / Ansprechpartner er verbunden werden möchte.

Mit dem Leistungsmerkmal **Ansage vor Abfrage mit DISA** werden Anrufe automatisch vom System angenommen. Der Anrufer hört dann eine Ansage mit Informationen, welche Eingaben während oder nach der Ansage möglich sind. Mit erfolgter Eingabe ist die Ansage beendet und der Anrufer wird zu einem internen Teilnehmer oder Team weitervermittelt. Gibt der Anrufer keine oder eine falsche Eingabe ein, wird er zu dem eingerichteten Abwurfziel (interner Teilnehmer oder Team) weitervermittelt. Während der Weitervermittlung hört der Anrufer den Freiton oder eine Wartemusik des Systems.

Hinweis

DISA - Direct Inward System Access. Nachdem ein Anruf vom System angenommen wurde, wird der Anrufer nach Eingabe einer Kennziffer automatisch weitervermittelt. Diese Kennziffer ist im System einer internen Rufnummer zugeordnet. Die Eingabe einer Rufnummer oder einer Kennziffer muss während der Ansage erfolgen. Ist die Ansage (die Wave-Datei) bereits beendet, werden keine weiteren Eingaben akzeptiert. Es erfolgt dann ein Abwurf auf das eingerichtete Abwurfziel. Das Leistungsmerkmal **Ansage vor Abfrage mit DISA** ist Bestandteil des Systems und kann gleichzeitig bis zu 28 Anrufe annehmen.

Felder im Menü Ansage/Einstellungen des Auto Attendants

Feld	Beschreibung
Vermittlung	Wählen Sie aus, wie der kommende Anruf vermittelt werden soll. Mögliche Werte: • *Ansage ohne DISA* (Standardwert): Die konfigurierte Ansage wird abgespielt. Danach folgt entweder die Weitervermittlung auf die konfigurierte interne Rufnummer oder die Verbindung wird unterbrochen und der Anrufer hört den Besetztton. • *DISA, interne Rufnummern werden gewählt*: Der Anrufer wird aufgefordert, eine interne Rufnummer einzugeben. Anschließend wird er an diese weitervermittelt.

Feld	Beschreibung
	• *DISA, Codenummern werden gewählt*: Der Anrufer wird aufgefordert, eine Kennziffer von 0 bis 9 einzugeben. Den Kennziffern sind die gewünschten internen Rufnummern zugeordnet. Der Anrufer wird anschließend auf die konfigurierte interne Rufnummer weitervermittelt.
Anzahl der Wiedergaben	Wählen Sie aus, wie oft die Ansage hintereinander wiederholt werden soll. Der Anrufer hört nach Ablauf den Besetztton.
Ansage vor Abfrage mit DISA	Nur bei **Vermittlung** = *DISA, Codenummern werden gewählt* Wählen Sie zu jeder gewünschten DISA-Code Kennziffer die gewünschte interne Rufnummer aus, an die der Anrufer weitervermittelt werden soll.

17.2.2 Abwurfanwendungen

Im Menü **Anwendungen**->**Abwurf**->**Abwurfanwendungen** können Sie konfigurieren, wann welche Abwurfvariante aktiv sein soll. Sie können die verschiedenen Varianten entweder über einen Kalender oder manuell umschalten.

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

17.2.2.1 Allgemein

Im Bereich **Allgemein** nehmen Sie grundlegende Einstellungen einer Abwurfanwendung vor.

Abb. 125: **Anwendungen**->**Abwurf**->**Abwurfanwendungen**->**Neu**

Das Menü **Anwendungen**->**Abwurf**->**Abwurfanwendungen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die Abwurfanwendung ein.
Typ der Abwurfanwendung	Wählen Sie das Ziel aus, auf das eine eingehender Ruf abgeworfen werden soll. Mögliche Werte: • *Anschlussrufnummer* (Standardwert) • *Interner Teilnehmer* • *Global*
Anrufvariante umschalten	Wählen Sie aus, wie zwischen den Varianten umgeschaltet werden soll. Mögliche Werte: • *Kein Kalender, nur manuell* • *<Kalender>*

17.2.2.2 Variante 1 - 4

Im Bereich **Variante** richten Sie die Abwurfvarianten ein. Sie können bis zu vier Varianten einrichten.

Abb. 126: **Anwendungen**->**Abwurf**->**Abwurfanwendungen**->**Variante**

Das Menü **Anwendungen**->**Abwurf**->**Abwurfanwendungen**->**Variante** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Zuordnung	Wählen Sie die Abwurffunktion, die Sie der gewählten Variante zuordnen wollen.

17.3 Voice-Applikationen

Im Menü **Anwendungen**->**Voice-Applikationen** konfigurieren Sie die Wave-Dateien Ihres Systems.

Die Visitenkarte eines Unternehmens stellt gerade am Telefon die professionelle Begrüßung dar. Sie ist mit Voice-Applikationen in jedem Unternehmen möglich. Mehr noch, während der Weitervermittlung und das noch individuell z. B. nach Abteilungen unterschiedlich, wird der Anrufer informiert oder einfach nur mit angenehmer Wartemusik unterhalten.

Sie möchten besondere Musik als Wartemusik oder eigene Ansagen für Ihre Kunden nutzen. Sie können Ihre selbst erstellten Wave-Dateien in das System einspielen.

Im System können benutzerspezifische Sprach- und Musikdaten gespeichert werden. In der Grundeinstellung des Systems steht Speicherplatz für 2 MoH-Melodien zur Verfügung. Durch Einsatz einer SD-Card kann der verfügbare Speicherplatz erweitert werden. Die Länge der speicherbaren Sprach- und Musikdaten richtet sich dabei nach der Größe der eingesetzten SD-Card. Die Speicherung der Sprach- und Musikdaten erfolgt im Wave-Format.

Folgende Voice-Applikationen können im System eingestellt werden:

- Ansage vor Abfrage
- Ansage ohne Abfrage/Infobox
- Weckruf
- Wartemusik/Music on Hold

Weitere Hinweise zur Funktion, Konfiguration und Bedienung finden Sie in der Beschreibung der einzelnen Leistungsmerkmale.

Grundeinstellungen der Voice-Applikationen

Die Voice-Applikationen können den einzelnen Leistungsmerkmalen auf zwei verschiedenen Arten zugewiesen werden.

Jeder Anwender, der eine Voice-Applikation mit dieser Anschaltung nutzt, hört die entsprechende Sprachansage oder Musikeinspielung immer von Beginn an. Ein neu hinzugekom-

mener Anwender hört die Sprachansage oder Musikeinspielung von Beginn an. Die Anzahl der Anwender, die eine solche Voice-Applikation gleichzeitig nutzen können, ist auf 28 begrenzt.

Beachten Sie, dass die externe eingespielte Musik oder die Musiken der Voice-Applikation frei von Schutzrechten Dritter sind (GEMA frei). In anderen Formaten vorhandene Dateien müssen vor dem Speichern im System auf das firmenspezifische Wave-Format konvertiert werden.

Hinweis

Bitte beachten Sie, dass die Wave-Dateien in folgendem Format vorliegen müssen:

- Bitrate: 128 kbit/s
- Abtastgröße: 16 bit
- Kanäle: 1 (Mono)
- Abtastrate: 8 kHz
- Audioformat: PCM

17.3.1 Wave-Dateien

Im Menü **Anwendungen**->**Voice-Applikationen**->**Wave-Dateien** können Sie Ihre Ansage-/ Melodie-Dateien laden und die Lautstärke einrichten. Außerdem haben Sie die Möglichkeit, Voice-Mail-Nachrichten abzuspielen oder auf ihren PC herunterzuladen. Zum Speichern einer Nachricht klicken Sie auf das -Symbol. Daraufhin öffnet sich der Download-Dialog. Um die Voice-Mail-Nachricht anzuhören, klicken Sie auf das -Symbol.

17.3.1.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie , um einen bestehenden Eintrag zu löschen.

MoH Intern 1 und *MoH Intern 2* sind im System vorgegebene Dateien und können daher nicht gelöscht werden.

Abb. 127: **Anwendungen->Voice-Applikationen->Wave-Dateien-> Bearbeiten**

Das Menü **Anwendungen->Voice-Applikationen->Wave-Dateien-> Bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die Wave-Datei ein.
Datei auswählen	Klicken Sie **Durchsuchen...** und wählen Sie über das Explorer-Fenster die Wave-Datei aus, die in das System geladen werden soll.
Lautstärke	Wählen Sie die Lautstärke aus, mit der die Wave-Datei standardmäßig abgespielt werden soll. Wählen Sie *0*, um die Datei in einer vordefinierten Standardlautstärke abzuspielen. Mit den negativen Werten können Sie die Lautstärke stufenweise verringern, mit den positiven erhöhen. Mögliche Werte: • *-5* • *-4* • *-3* • *-2* • *-1* • *0* (Standardwert) • *+1* • *+2* • *+3*

17.4 System-Telefonbuch

Im Menü **Anwendungen**->**System-Telefonbuch** können Sie Rufnummern in das Telefonbuch des Systems eintragen und diese verwalten.

In Ihrem Unternehmen müssen die Mitarbeiter mit vielen Kunden telefonieren. Hier bietet sich das Telefonbuch des Systems an. Sie müssen nicht die Rufnummer des Kunden eingeben, sondern können den Namen über das Display des Systemtelefons heraussuchen und die Wahl kann beginnen. Die Kundennamen und Telefonnummern können von einem Mitarbeiter zentral verwaltet werden. Ruft ein Kunde an, dessen Name im Telefonbuch eingetragen ist, wird sein Name im Display des Systemtelefons angezeigt. Das System verfügt über ein integriertes Telefonbuch, in dem Sie Telefonbucheinträge von bis zu 24-stelligen Rufnummern (Ziffern) und bis zu 20-stelligen Namen (Text) speichern können.

Beim Erstellen eines Telefonbucheintrages wird jedem Eintrag eine **Kurzwahl** zugeordnet. Über diese Kurzwahlrufnummer können berechtigte Telefone eine Kurzwahl aus dem Telefonbuch einleiten.

Systemtelefone

Systemtelefone können über ein besonderes Menü aus dem Telefonbuch des Systems wählen. Um einen Eintrag im Telefonbuch zu suchen, geben Sie die ersten Buchstaben (maximal 8) des gesuchten Namens ein und bestätigen Sie die Eingabe. Es werden immer 8 Einträge des Telefonbuches vom System zur Verfügung gestellt, die Sie sich nacheinander ansehen können. Wählen Sie den gewünschten Eintrag aus und bestätigen Sie mit **OK**. Sie müssen jetzt die Wahl innerhalb von 5 Sekunden beginnen. In der Wahlwiederholungs-Liste des Systemtelefons wird anstelle der Rufnummer der Name des gewählten Teilnehmers angezeigt. Erhält ein Systemtelefon einen Anruf, dessen Rufnummer und Name im Telefonbuch des Systems gespeichert ist, wird im Display des Systemtelefons der Name des Anrufers angezeigt.

Hinweis

Die zusätzlichen Rufnummern eines Benutzers (**Mobilnummer** und **Rufnummer privat**) werden nur im Telefonbuch-Menü des Systemtelefons. Sie werden nicht im Menü **System-Telefonbuch** der Benutzeroberfläche angezeigt. Einträge im Telefonbuch-Menü des Systemtelefons mit dem Vermerk (M) verweisen auf eine eingetragene **Mobilnummer** eines Benutzers, solche mit dem Vermerk (H) auf die **Rufnummer privat**.

Hinweis

Ihre Telefonanlage unterstützt LDAP (Lightweight Directory Access Protocol), um die Einträge des System-Telefonbuchs anderen Geräten bzw. Anlagen bereitzustellen. Name, Rufnummer (MSN) sowie mobile und private Rufnummer können auf diese Weise transferiert werden.

17.4.1 Einträge

Im Menü **Anwendungen**->**System-Telefonbuch**->**Einträge** werden alle eingerichteten Telefonbucheinträge mit der zugehörigen Kurzwahl angezeigt. In der Spalte **Beschreibung** sind die Einträge alphabetisch sortiert. Sie können in jeder beliebigen Spalte auf den Spaltentitel klicken und die Einträge in aufsteigender oder in absteigender Reihenfolge sortieren lassen.

17.4.1.1 Bearbeiten oder Neu

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

Abb. 128: **Anwendungen**->**System-Telefonbuch**->**Einträge**->**Neu**

Das Menü **Anwendungen**->**System-Telefonbuch**->**Einträge**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Telefonbucheintrag

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein. Die spätere Sortierung im Telefonbuch erfolgt nach den ersten Buchstaben des Eintrags.

Feld	Beschreibung
Telefonnummer	Geben Sie die Telefonnummer ein (intern oder extern).
Kurzwahl	Geben Sie eine Kurzwahl ein. Wird keine Kurzwahl eingegeben, wird automatisch weitergezählt, d.h. eine Kurzwahl wird automatisch zugeordnet. Möglich sind Zahlen von *0* bis *999*.
Call Through	Wählen Sie aus, ob die Telefonnummer für die Funktion **Call Through** freigegeben werden soll. Wenn eine Telefonnummer dafür freigegeben ist und ein Anrufer diese Nummer für die Funktion **Call Through** nutzt, wird seine Berechtigung zur Nutzung anhand des Telefonbucheintrags überprüft. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

17.4.2 Import / Export

Im Menü **Anwendungen**->**System-Telefonbuch**->**Import / Export** können Sie Telefonbuchdaten importieren und exportieren. So können z. B. aus Microsoft Oulook exportierte Daten importiert werden. Beim Export der in Ihrem Gerät gespeicherten Telefonbuchdaten wird eine Textdatei erzeugt.

Abb. 129: **Anwendungen**->**System-Telefonbuch**->**Import / Export**

Das Menü **Anwendungen**->**System-Telefonbuch**->**Import / Export** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Aktion	Wählen Sie die gewünschte Aktion aus. Mögliche Werte:

Feld	Beschreibung
	• *Exportieren* (Standardwert): Sie können die in **Anwendungen->System-Telefonbuch ->Einträge** gespeicherten Namen (mit Angabe von Telefonnummern, Kurzwahl, Call Through) in eine Textdatei exportieren. • *Importieren* : Sie können eine Textdatei im folgenden Format importieren: Die zu importierende Datei muss aus einzelnen Zeilen im Format Beschreibung,Telefonnummer,Kurzwahl,Call Through (1 = Aktiviert, 2 = Nicht aktiviert) bestehen. Beispiel: Name,Phone Number,Speeddial Number,Call Through Hans,123456,1,1 Klaus,234567,2,2 Max,345678,3,1
Trennzeichen	Nur für **Aktion** = *Importieren* und **Standard-Dateiformat** nicht *Aktiviert* Geben Sie das in der zu importierenden Datei verwendete Tennzeichen an. Mögliche Werte: • *Komma* (Standardwert) • *Semikolon* • *Leertaste* • *Tabulator*
Datei auswählen	Nur für **Aktion** = *Importieren* Wählen Sie die Datei aus, die importiert werden soll.

Sie haben ebenso die Möglichkeit eine CSV-Datei zu importieren.

```
"Anrede","Vorname","Nachname","Telefon geschäftlich","Telefon privat"
"Herr","Hans","Meier","+49 (911) 111111","+49 (911) 222222"
"Frau","Emma","Will","+49 (911) 333333","+49 (911) 444444"
```

Abb. 130: Beispiel einer importierbaren CSV-Datei

Sofern der Datensatz aus mehreren Spalten besteht, haben Sie beim Import die Möglichkeit, aus dem Datensatz zwei Adressbucheinträge zu generieren (z. B. einen geschäftlichen und einen privaten Eintrag). Dazu spezifizieren Sie in einem weiteren Importschritt die Daten, die jeweils als Name und Telefonnummer übernommen werden sollen. Wollen Sie nur einen Adressbucheintrag generieren, wählen Sie die leere Option in allen Auswahlfeldern des zweiten Eintrags **Telefonbuchimport**.

Abb. 131: **Anwendungen->System-Telefonbuch ->Import / Export->Telefonbuchimport**

Felder im Menü Telefonbuchimport

Feld	Beschreibung
Telefonnummer	Wählen Sie aus, welche Daten aus einem Datensatz als Telefonnummer übernommen werden soll.
Name	Wählen Sie aus, welche Spalten aus dem Datensatz als Name übernommen werden sollen. Sie haben dabei die Möglichkeit, zwei Elemente zu übernehmen (z. B. den Vor- und Nachnamen). Dabei kann mithilfe des mittleren Eingabefelds eine Zeichenkette zwischen den beiden Elementen platziert werden. Das Standardtrennzeichen ist ein Komma.

Die Kurzwahl wird automatisch zugewiesen. Call Through ist standardmäßig deaktiviert.

17.4.3 Allgemein

Im Menü **Anwendungen->System-Telefonbuch ->Allgemein** legen Sie den Benutzernamen und das Passwort zur Administration des System-Telefonbuchs fest. Der Administrator kann im Bereich Telefonbuch das Telefonbuch einsehen, ändern und Daten importieren sowie exportieren.

Abb. 132: **Anwendungen->System-Telefonbuch ->Allgemein**

Das Menü **Anwendungen->System-Telefonbuch ->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Benutzername für Webzugang	Geben Sie einen Benutzernamen für den System-Telefonbuch-Administrator ein.
Passwort für Webzugang	Geben Sie ein Passwort für den System-Telefonbuch-Administrator ein.
Telefonbuch löschen	Wenn Sie das vorhandene System-Telefonbuch mit allen Einträgen entfernen möchten, aktivieren Sie die Option **Löschen**. Daraufhin erscheint die Sicherheitsabfrage **Wollen Sie wirklich alle Einträge des Telefonbuchs löschen?** Bestätigen Sie Ihre Eingaben, indem Sie auf **OK** klicken.

17.5 Verbindungsdaten

Im Menü **Anwendungen->Verbindungsdaten** konfigurieren Sie die Erfassung der kommenden und gehenden Verbindungen.

Die Erfassung der Verbindungsdatensätze verschafft Ihnen einen Überblick über das Telefonieverhalten in Ihrem Unternehmen.

Im Gerät können alle externen Gespräche in Form von Verbindungsdatensätzen gespeichert werden. In diesen Datensätzen finden Sie wichtige Informationen über die einzelnen Gespräche wieder.

Sie müssen die Erfassung der Verbindungsdaten im Menü **Nummerierung->Benutzereinstellungen->Berechtigungsklassen->Anwendungen** aktivieren. Im Auslieferungszustand ist die Funktion deaktiviert.

17.5.1 Gehend

Das Menü **Anwendungen**->**Verbindungsdaten**->**Gehend** enthält Informationen, die das Überwachen der gehenden Aktivitäten ermöglichen.

Abb. 133: **Anwendungen**->**Verbindungsdaten**->**Gehend**

Das Menü **Anwendungen**->**Verbindungsdaten**->**Gehend** besteht aus folgenden Feldern:

Felder im Menü Gehend

Feld	Beschreibung
Datum	Zeigt das Datum der Verbindung an.
Zeit	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
Dauer	Zeigt die Dauer der Verbindung an.
Benutzer	Zeigt den Benutzer an, der angerufen hat.
Int. Rufnr.	Zeigt die interne Rufnummer des Benutzers an.
Gewählte Rufnummer	Zeigt die gewählte Rufnummer an.
Projektnummer	Zeigt ggf. die Projektnummer des Gesprächs an.
Schnittstelle	Zeigt die Schnittstelle an, über die die Verbindung nach Extern geleitet wurde.
Kosten	Zeigt die Kosten der Verbindung an, jedoch nur, wenn der Provider die ensprechenden Informationen übermittelt.

17.5.2 Kommend

Im Menü **Anwendungen**->**Verbindungsdaten**->**Kommend** enthält Informationen, die das Überwachen der kommenden Aktivitäten ermöglichen.

Abb. 134: **Anwendungen**->**Verbindungsdaten**->**Kommend**

Das Menü **Anwendungen**->**Verbindungsdaten**->**Kommend** besteht aus folgenden Feldern:

Felder im Menü Kommend

Feld	Beschreibung
Datum	Zeigt das Datum der Verbindung an.
Zeit	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
Dauer	Zeigt die Dauer der Verbindung an.
Benutzer	Zeigt den Benutzer an, der angerufen wurde.
Int. Rufnr.	Zeigt die interne Rufnummer des Benutzers an.
Externe Rufnummer	Zeigt die Rufnummer des Anrufers an.
Projektnummer	Zeigt ggf. die Projektnummer des Gesprächs an.
Schnittstelle	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.

17.5.3 Allgemein

Im Menü **Anwendungen**->**Verbindungsdaten**->**Allgemein** können Sie einrichten, wie die Verbindungsdaten im System gespeichert werden.

Abb. 135: **Anwendungen->Verbindungsdaten->Allgemein**

Das Menü **Anwendungen VerbindungsdatenAllgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Benutzername für Webzugang	Geben Sie einen Benutzernamen für den Verbindungsdaten-Administrator ein.
Passwort für Webzugang	Geben Sie ein Passwort für den Verbindungsdaten-Administrator ein.
Gehende Verbindungen speichern	Wählen Sie aus, welche gehenden Verbindungen gespeichert werden sollen. Mögliche Werte: • *Keine* (Standardwert) • *Alle* • *Nur mit Projekt-Nummer*
Kommende Verbindungen speichern	Wählen Sie aus, welche kommenden Verbindungen gespeichert werden sollen. Mögliche Werte: • *Keine* (Standardwert)

Feld	Beschreibung
	• *Alle* • *Nur mit Projekt-Nummer*
Rufnummernverkürzung	Wählen Sie aus, ob die Rufnummer verkürzt gespeichert werden soll. Soll aus Datenschutzgründen die Anzeige der Rufnummer nur unvollständig erfolgen, können Sie hier die Anzahl der Stellen, die nicht angezeigt werden sollen, festlegen. Sie können für **Gehende Verbindungen** und für **Kommende Verbindungen** getrennt die Anzahl der ausgeblendeten Ziffern eingeben. Das Ausblenden der Ziffern erfolgt von rechts nach links. Mögliche Werte: • *Nein* (Standardwert) • *Alle* • *1* bis *9*
Verbindungsdaten über Serial 2 ausgeben	Nur für modulare Telefonanlagen Wählen Sie, ob die Verbindungsdaten für jedes Gespräch über die serielle Schnittstelle (Serial 2) ausgegeben werden sollen. Sie können auf diese Weise eine externe Softwarelösung zur Gebührenerfassung (Hotel-Applikation) anbinden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Aktionen

Feld	Beschreibung
Verbindungsdaten exportieren	Wenn Sie den aktuellen Verbindungsdatenbestand in eine externe Datei speichern möchten, klicken Sie **Exportieren** und speichern die Datei unter dem gewünschten Speicherort und Dateinamen ab.
Verbindungsdaten löschen	Wenn Sie den aktuellen Verbindungsdatenbestand aus dem Systemspeicher entfernen möchten, klicken Sie **Löschen**.

17.6 Mini-Callcenter

Das Mini-Callcenter ist eine im System integrierte Callcenter-Lösung für bis zu 16 Agents. Sie stellt eine ideale Lösung für kleine Gruppen mit hohem dynamischen Telekommunikations-Aufkommen (z. B. Vertriebsinnendienst, Support, Auftragsannahme/ -abwicklung, Kundendienst) dar. Hier ist im System eine eigene Lösung mit eigenem Administator integriert worden. Das Mini-Callcenter zeichnet sich aus durch:

- Flexible Zuordnung von Agents und Leitungen
- Dynamische Anpassung je nach Anrufaufkommen
- Rufverteilung mit Ruhezeiten für den Agent
- Statistische Angaben zu Agents und Leitungen.

17.6.1 Status

Im Menü **Anwendungen**->**Mini-Callcenter**->**Status** können Sie den derzeitigen Stand der Leitungen und angemeldeten Agents sowie den Leitungen zugeordneten Teilnehmer in einem Block einsehen.

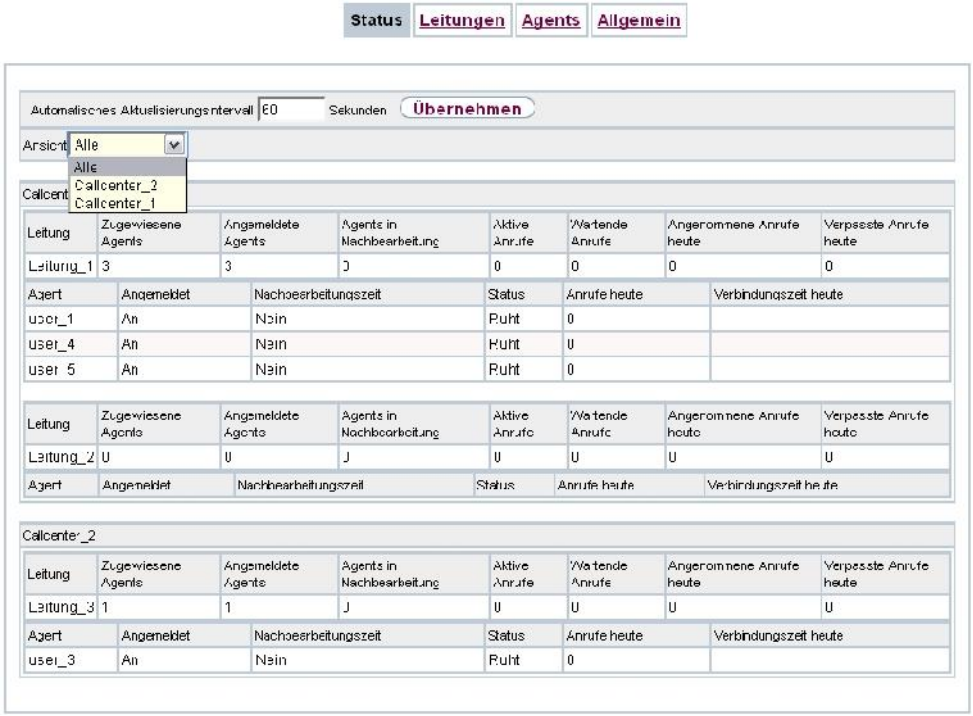


Abb. 136: **Anwendungen->Mini-Callcenter->Status->Leitungen**

Das Menü **Anwendungen->Mini-Callcenter->Status** besteht aus folgenden Feldern:

Werte in der Liste Status

Feld	Beschreibung
Ansicht	Mithilfe von **Ansicht** können Sie bestimmen, welche Callcenter angezeigt werden.
Leitung	Zeigt die Mini-Callcenter-Leitung an.
Zugewiesene Agents	Zeigt die Anzahl der Agents an, die dieser Leitung zugewiesen sind.
Angemeldete Agents	Zeigt die Anzahl der Agents an, die an dieser Leitung angemeldet sind.
Agents in Nachbearbeitung	Zeigt die Anzahl der Agents an, die sich in der Nachbearbeitungszeit befinden.
Aktive Anrufe	Zeigt die Anzahl aktiver Verbindungen an.

Feld	Beschreibung
Wartende Anrufe	Zeigt die Anzahl wartender eingehender Anrufe an.
Angenommene Anrufe heute	Zeigt die aktuelle Anzahl der angenommenen Anrufe für diesen Tag an.
Verpasste Anrufe heute	Zeigt die aktuelle Anzahl der verpassten Anrufe für diesen Tag an.

17.6.2 Leitungen

Im Menü **Anwendungen**->**Mini-Callcenter**->**Leitungen** werden die Leitungen den externen und internen Rufnummern zugeordnet, und die Namen des Callcenters zu dem die Leitung gehört angezeigt..

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

17.6.2.1 Allgemein

Im Bereich **Allgemein** nehmen Sie grundlegende Einstellungen einer Leitung vor.

Abb. 137: **Anwendungen**->**Mini-Callcenter**->**Leitungen**->**Allgemein**

Das Menü **Anwendungen**->**Mini-Callcenter**->**Leitungen**->**Allgemein** besteht aus folgen-

den Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die Leitung ein.
Externe Rufnummer	Wählen Sie eine der als Mini-Callcenter konfigurierten Rufnummern für den externen Anschluss dieser Callcenter-Leitung aus.
Interne Rufnummer	Geben Sie die gewünschte interne Rufnummer für diese Leitung ein.
Beschreibung des Call Centers	Wählen Sie *Neu* und geben Sie einen Namen für das neue Mini-Callcenter ein. Oder wählen Sie den Namen eines zuvor erzeugten Mini-Callcenters aus.

Felder im Menü Weitere Einstellungen

Feld	Beschreibung
Anrufvariante umschalten	Wählen Sie aus, ob die Anrufvarianten für diese Leitung über einen konfigurierten Kalender umgeschaltet werden sollen und, wenn ja, über welchen. Mögliche Werte: • *Kein Kalender, nur manuell* • *<Kalender>*
Aktive Anrufvariante	Wählen Sie aus, welche Anrufvariante standardmäßig für diese Leitung nach der Konfiguration aktiviert sein soll.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Weiterschaltzeit	Geben Sie die Zeit ein, nach der eine Anrufweiterschaltung auf den nächsten freien Agent, der dieser Leitung zugeordnet ist, ausgeführt werden soll.

17.6.2.2 Variante 1 - 4

Im Bereich **Variante** richten Sie die Anrufvarianten des Mini-Callcenters ein.

Abb. 138: **Anwendungen->Mini-Callcenter->Leitungen->Variante**

Das Menü **Anwendungen->Mini-Callcenter->Leitungen->Variante** besteht aus folgenden Feldern:

Felder im Menü Einstellungen

Feld	Beschreibung
Automatische Rufannahme mit	Wählen Sie aus, ob ein kommender Ruf automatisch und wenn ja mit welcher Ansage bzw. Melodie angenommen werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wählen Sie die Wave-Datei aus, die für die Rufannahme verwendet werden soll. Zur Auswahl stehen alle im System voreingestellten und zusätzlich geladenen Wave-Dateien.

Felder im Menü Abwurffunktionen

Feld	Beschreibung
Abwurf bei Nichtmelden	Wählen Sie aus, ob und wenn ja mit welcher Variante ein kommender Ruf nach einer eingetragenen Zeit abgeworfen werden soll.

Feld	Beschreibung
	Mögliche Werte: • *Keine*: Es soll kein Abwurf bei Nichtmelden ausgeführt werden. • *<Team>*: Der kommende Anruf wird nach der in **Zeit bis Abwurf** spezifizierten Zeit an das ausgewählte Team weitervermittelt.
Weitere Abwurffunktionen	Wählen Sie weitere Abwurffunktionen aus. Diese müssen Sie zunächst in **Anwendungen**->**Abwurf**->**Abwurffunktionen** einrichten. Dann stehen folgende Werte zur Auswahl: • *Aus*: Keine weiteren Abwurffunktionen. • *Sofort*: Vermittelt den Ruf laut einer konfigurierten Abwurffunktion Sofort. • *Bei Besetzt*: Vermittelt den Ruf laut einer konfigurierten Abwurffunktion bei Besetzt.
Abwurffunktion	Nur für **Weitere Abwurffunktionen** = *Sofort* oder **Weitere Abwurffunktionen** = *Bei Besetzt* Wählen Sie eine konfigurierte Abwurfvariante für Abwurf Sofort bzw. für Abwurf bei Besetzt aus.
Besetzt wenn	Nur für **Weitere Abwurffunktionen** = *Bei Besetzt* Wählen Sie aus, ab wie vielen besetzten Agents die Leitung als besetzt gilt.

17.6.2.3 Einloggen/Ausloggen

Im Bereich **Einloggen/Ausloggen** wählen Sie aus, welche der zugewiesenen Agents für die Leitung angemeldet werden sollen.

Abb. 139: **Anwendungen->Mini-Callcenter->Leitungen->Einloggen/Ausloggen**

Das Menü **Anwendungen->Mini-Callcenter->Leitungen->Einloggen/Ausloggen** besteht aus folgenden Feldern:

Felder im Menü Einloggen/Ausloggen

Feld	Beschreibung
Rufnummern	Zeigt die interne Rufnummer und die Beschreibung des zugewiesenen Agents an.
Status	Wählen Sie aus, ob der Agent an der Leitung angemeldet ist. Mit Auswahl von `Angemeldet` wird der Agent angemeldet.

17.6.3 Agents

Im Menü **Anwendungen->Mini-Callcenter->Agents** werden die Leitungen den Agents zugeordnet. Ein Agent kann eine oder auch mehrere Mini-Callcenter-Leitungen bedienen.

17.6.3.1 Bearbeiten oder Neu

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

Abb. 140: **Anwendungen->Mini-Callcenter->Agents->Neu**

Das Menü **Anwendungen->Mini-Callcenter->Agents->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Benutzer	Wählen Sie den konfigurierten Benutzer aus, der als Agent des Callcenters tätig sein soll. Die notwendigen Benutzer konfigurieren Sie im Menü **Nummerierung->Benutzereinstellungen->Benutzer**.
Interne Rufnummer	Wählen Sie die interne Rufnummer des Benutzers aus, die für das Callcenter verwendet werden soll.

Felder im Menü Zugewiesene Leitungen

Feld	Beschreibung
Leitungen auswählen	Wählen Sie die Leitungen aus, für die der Agent tätig sein soll. Bei der Auswahl der Leitungen wird noch der Name des zugehörigen Callcenters zur besseren Übersicht angezeigt. Wählen Sie unter **Zuweisen** aus, ob der Eintrag aktiv sein soll.

Felder im Menü Einstellungen Nachbearbeitungszeit

Feld	Beschreibung
Nachbearbeitungszeit	Geben Sie die Zeit ein, die diesem Agent nach einem erledigten Telefonat zur Nachbearbeitung zur Verfügung steht. In dieser Zeit kann dem Agent kein weiteres Telefonat zugewiesen werden. Der Agent hat die Möglichkeit, die Zeit temporär über eine Telefonprozedur zu verlängern.

17.6.4 Allgemein

Im Menü **Anwendungen**->**Mini-Callcenter**->**Allgemein** können Sie einen HTML-Weboberflächen-Zugang für den Mini-Callcenter-Leiter einrichten. Dieser kann dann den Status der Leitungen und Agents überwachen und die Einstellungen der Leitungen und Agents ändern.

Abb. 141: **Anwendungen**->**Mini-Callcenter**->**Allgemein**

Das Menü **Anwendungen**->**Mini-Callcenter**->**Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Benutzername für Webzugang	Geben Sie einen Benutzernamen für den Mini-Callcenter-Administrator ein. Wenn sich ein Benutzer mit diesem Namen in die Benutzeroberfläche einloggt, steht ihm die Benutzeroberfläche mit ausgewählten Parametern für die Verwaltung des Callcenters zur Verfügung.
Passwort für Webzugang	Geben Sie ein Passwort für den Mini-Callcenter-Administrator ein.

17.7 TFE-Adapter

Eine Türfreisprecheinrichtung können Sie als TFE-Adapter an einem analogen Anschluss Ihres Systems anschließen.

Ist an Ihr System ein TFE-Adapter 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 wäh-

rend eines Türgespräches betätigt werden. Eine Betätigung ohne Türgespräch ist nicht möglich.

Hinweis

Alle Funktionen der Türfreisprecheinrichtung (TFE-Adapter) werden über die Kennziffern, die in der Bedienungsanleitung der TFE angegeben sind, gesteuert. Das System unterstützt die TFE nicht mit eigenen Kennziffern.

17.7.1 TFE-Adapter

Im Menü **Anwendungen**->**TFE-Adapter**->**TFE-Adapter** wählen Sie den internen analogen Anschluss (FXS) aus, an dem ein TFE-Adapter angeschlossen werden sollen. Weiterhin wählen Sie die interne Rufnummer für den Anschluss und optional die Kennziffern für die Rufannahme.

17.7.1.1 Bearbeiten oder Neu

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

Abb. 142: **Anwendungen**->**TFE-Adapter**->**TFE-Adapter**->**Neu**

Das Menü **Anwendungen**->**TFE-Adapter**->**TFE-Adapter**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, an die ein TFE-Adapter angeschlossen ist. Zur Verfügung stehen alle freien FXS-Schnittstellen.

Feld	Beschreibung
Interne Rufnummer	Wählen Sie die konfigurierte interne Rufnummer aus, die dem TFE-Adapter zugewiesen werden soll. Die Rufnummer wird im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer** eingerichtet.
Kennziffer für TFE-Rufannahme	Durch Betätigen eines Klingeltasters am TFE-Adapter wird ein Ruf im System ausgelöst. Um eine Gesprächsverbindung zwischen einem gerufenen Teilnehmer und dem TFE-Adapter herzustellen, muss dieser Teilnehmer den Hörer abheben und die Kennziffer zur Rufannahme wählen. Tragen Sie diese Kennziffer für die Rufannahme ein. Nimmt ein Teilnehmer einen Ruf vom TFE-Adapter an, wählt die TK-Anlage automatisch die notwendige Kennziffer zum Herstellen der Gesprächsverbindung. Der Teilnehmer muss dann keine weiteren Eingaben vornehmen.

17.7.2 TFE-Signalisierung

Im Menü **Anwendungen**->**TFE-Adapter**->**TFE-Signalisierung** konfigurieren Sie die Signalisierungsvarianten für die Rufannahme über einen TFE-Adapter. Es stehen zwei TFE-Anrufvarianten zur Verfügung.

Die Kennziffer für die Klingeltaster ist die Rufnummer, die der TFE-Adapter beim Betätigen des Klingeltasters in das System wählt. Hierüber können Sie für jeden Klingeltaster eine interne Rufverteilung realisieren. Beachten Sie, dass die Vorgaben für die Anschaltung des TFE-Adapters vom jeweiligen Hersteller abhängig sind. Lesen Sie hierzu die Bedienungsanleitung des Herstellers der TFE-Adapter.

17.7.2.1 Allgemein

Im Bereich **Allgemein** richten Sie grundlegende Merkmale der TFE-Signalisierung ein.

Abb. 143: **Anwendungen->TFE-Adapter->TFE-Signalisierung->Allgemein**

Das Menü **Anwendungen->TFE-Adapter->TFE-Signalisierung->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Wählen Sie eine der konfigurierten TFE-Einrichtungen aus, die vorher im Menü **Anwendungen->TFE-Adapter->TFE-Adapter** angelegt wurde.
Klingelkennziffer	Geben Sie eine eindeutige vierstellige Kennziffer für die Klingel ein. Durch Betätigen eines Klingeltasters am TFE-Adapter werden die in der zugewiesenen TFE-Anrufvariante eingetragenen Endgeräte gerufen.
Klingelname	Geben Sie einen Namen für die Klingel ein.
Variante umschalten	Wählen Sie aus, ob die TFE-Anrufvarianten für diese Klingel über einen konfigurierten Kalender umgeschaltet werden sollen und, wenn ja, über welchen. Sie können für jede Klingel bis zu zwei TFE-Anrufvarianten im Menü **Anwendungen->TFE-Adapter->TFE-Signalisierung->Neu->Variante** einrichten. Mögliche Werte: • *Kein Kalender, nur manuell*

Feld	Beschreibung
	• *<Kalender>*
Aktive TFE-Variante	Wählen Sie aus, welche TFE-Anrufvariante standardmäßig für diese Klingel nach der Konfigurierung aktiviert sein soll.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Anrufsignalisierungs-zeit	Geben Sie die Zeit in Sekunden an, wie lange der Türstellenruf signalisiert werden soll. Der Standardwert ist *40* Sekunden.
Weiterschaltzeit	Geben Sie hier die **Weiterschaltzeit** ein, nach der eine Anrufweiterschaltung nach Zeit ausgeführt werden soll. Der Standardwert ist *15* Sekunden.
Parallelruf nach Zeit	Es besteht die Möglichkeit, dass nach einer eingestellten Zeit alle Rufnummern, die dieser TFE-Signalisierung zugewiesen wurden, gleichzeitig gerufen werden. Der Standardwert ist *60* Sekunden.

17.7.2.2 TFE-Anrufvariante 1 und 2

Im Bereich **TFE-Anrufvariante** konfigurieren Sie die beiden TFE-Anrufvarianten für dieses Signalisierungs-Profil.

Abb. 144: **Anwendungen->TFE-Adapter->TFE-Signalisierung->TFE-Anrufvariante**

Das Menü **Anwendungen**->**TFE-Adapter**->**TFE-Signalisierung**->**TFE-Anrufvariante** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Zuordnung	Wählen Sie aus, wo ein Betätigen der Türklingel signalisiert werden soll. Mögliche Werte: • *Intern*: Die Signalisierung erfolgt an einer internen Rufnummer. • *Extern*: Die Signalisierung erfolgt an einer externen Rufnummer.
Interne Zuordnung	Wählen Sie die internen Rufnummern aus, an denen ein Betätigen der Türklingel signalisiert werden soll. Fügen Sie mit **Hinzufügen** eine weitere interne Rufnummer hinzu.
Externe Zuordnung	Geben Sie die externe Telefonnummer ein, an der das Betätigen der Türklingel signalisiert werden soll.
Signalisierung	Sie können die internen Rufnummern mit dem Sammelruf rufen. Mögliche Werte: • *Gleichzeitig* (Standardwert): Alle zugeordneten Endgeräte werden gleichzeitig gerufen. Ist ein Telefon besetzt, kann angeklopft werden. • *Linear*: Alle zugeordneten Endgeräte werden nacheinander in der Reihenfolge des Eintrages in der Konfigurierung gerufen. Wenn ein Endgerät besetzt ist, wird das nächste freie Endgerät gerufen. Je Teilnehmer wird der Anruf ca. 15 Sekunden signalisiert. Diese Zeit ist in der Konfigurierung (je Klingel) zwischen 1 und 99 Sekunden einstellbar. Wenn Teilnehmer telefonieren oder ausgeloggt sind, erfolgt keine Weiterschaltungszeit für diese Teilnehmer. • *Rotierend*: Dieser Ruf ist ein Sonderfall des linearen Rufes. Nachdem alle Endgeräte gerufen wurden, beginnt die Rufsignalisierung wieder beim ersten eingetragenen Endgerät. Der Ruf wird solange signalisiert, bis der Anrufer auflegt oder der Ruf vom TFE-Adapter beendet wird (nach ca. zwei Minuten). • *Aufbauend*: Die Endgeräte werden in der Reihenfolge des

Feld	Beschreibung
	Eintrages in die Teilnehmerliste der Konfigurierung gerufen. Jedes bereits gerufene Endgerät wird weiter gerufen, bis alle eingetragenen Endgeräte gerufen werden. Über die Konfigurierung ist einrichtbar, wann das jeweils nächste Endgerät gerufen wird. • *Linear, parallel nach Zeit*: Sie haben für den TFE-Ruf linear eingerichtet. Nach Ablauf der eingerichteten Zeiten können Sie zusätzlich in der Konfigurierung einrichten, dass anschließend alle Teamteilnehmer parallel (gleichzeitig) gerufen werden. • *Rotierend, parallel nach Zeit*: Sie haben für den TFE-Ruf rotierend eingerichtet. Nach Ablauf der eingerichteten Zeiten können Sie zusätzlich in der Konfigurierung einrichten, dass anschließend alle TFE-Teilnehmer parallel (gleichzeitig) gerufen werden.

17.8 Melderufe

Die FXS-Schnittstelle der Telefonanlagen kann als Meldeeingang konfiguriert werden. So kann z. B. ein Meldeknopf an eine dieser Schnittstellen angeschlossen werden: Wenn der Knopf gedrückt wird, wird ein Melderuf an entweder bis zu acht interne oder eine von zwei externen Rufnummern ausgelöst. Während eines Melderuf kann ggf. einer der Schaltkontakte aktiviert werden. Optional kann die Funktion über einen Kalender geschaltet bzw. zwischen den beiden möglichen Signalisierungsvarianten umgeschaltet werden.

17.8.1 Melderufe

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

17.8.1.1 Allgemein

Im Bereich **Allgemein** richten Sie grundlegende Merkmale der Meldeeingänge ein.

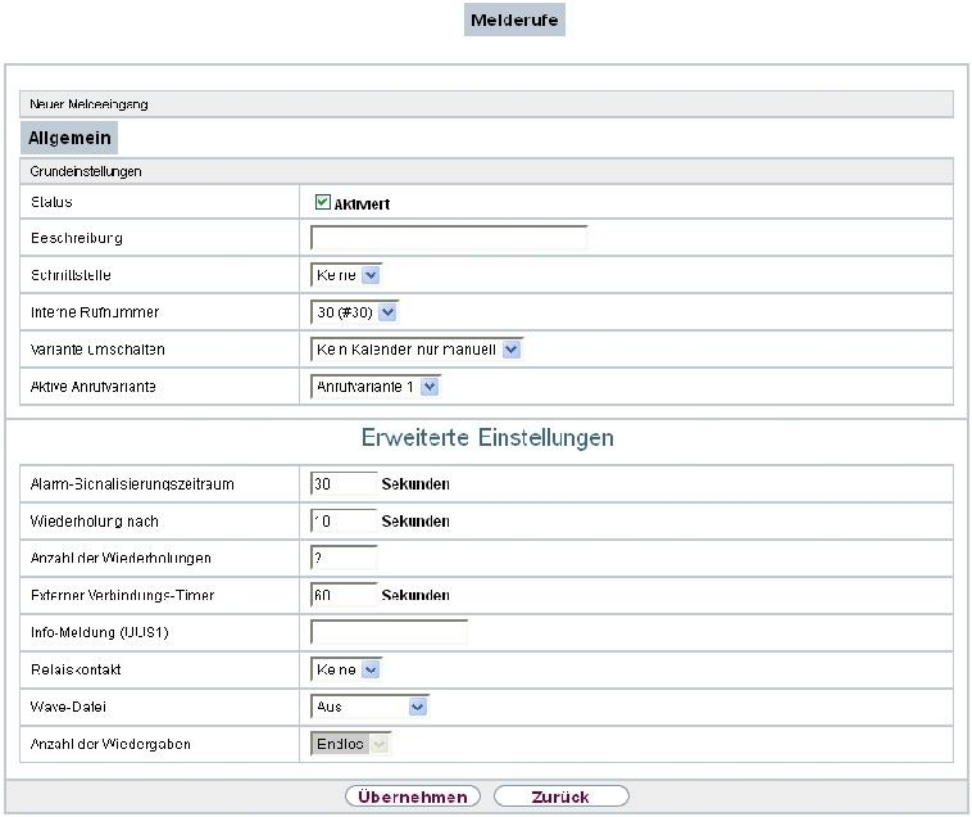


Abb. 145: **Anwendungen->Meldeeingang->Melderufe->Allgemein**

Das Menü **Anwendungen->Meldeeingang->Melderufe->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Status	Aktivieren oder deaktivieren Sie die Funktion. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den Melderuf ein.
Schnittstelle	Wählen Sie die Schnittstelle aus, welche für diesen Melderuf verwendet werden soll.
Interne Rufnummer	Wählen Sie eine interne Rufnummer aus, die für den Melderuf genutzt werden soll.

Feld	Beschreibung
Variante umschalten	Legen Sie fest, wie der eingerichtete Melderuf geschaltet werden soll. Mögliche Werte: • *Kein Kalender, nur manuell*: Die manuelle Umschaltung wird aktiv. • *<Kalendereintrag>*: Wählen Sie einen der für den Melderuf konfigurierten Kalendereinträge aus.
Aktive Anrufvariante	Wählen Sie die Anrufvariante aus, die aktiv sein soll. Sie können die Varianten konfigurieren, sobald Sie die Eingabe im Reiter **Allgemein** mit **OK** bestätigt haben.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Alarm-Signalisierungszeitraum	Geben Sie die Zeit in Sekunden ein, wie lange ein Melderuf signalisiert werden soll. Standardwert ist *30* Sekunden.
Wiederholung nach	Geben Sie die Zeit zwischen den Wiederholungen des Melderufs in Sekunden ein. Möglich ist ein Wert zwischen *1* und *600* Sekunden. Standardwert ist *10* Sekunden. Melderufwiederholungen über eine FXO-Schnittstelle sind nicht möglich.
Anzahl der Wiederholungen	Geben Sie die Anzahl der Wiederholungen ein, wenn der Melderuf nicht angenommen wird. Möglich ist ein Wert zwischen 1 und 10 Wiederholungen. Standardwert ist *2*. Melderufwiederholungen über eine FXO-Schnittstelle sind nicht möglich.
Externer Verbindungs-Timer	Geben Sie max. Dauer eines externen Melderuf (in Sekunden ein), nachdem dieser angenommen wurde.

Feld	Beschreibung
	Möglich ist ein Wert zwischen *1* und *600* Sekunden. Standardwert ist *60* Sekunden.
Info-Meldung (UUS1)	Optional kann eine Nachricht (max. 32 Zeichen) an ISDN-Endgeräte gesendet werden.
Relaiskontakt	Wenn ein Relais während des Melderufs geschaltet werden soll: Wählen Sie das zu verwendende Relais. Die Konfiguration des Relais erfolgt im Menü **Physikalische Schnittstellen**->**Relais**.
Wave-Datei	Wählen Sie aus, ob und welche gespeicherte Wave-Datei bei Annahme des Melderufs gespielt werden soll. Mögliche Werte: • *Aus* (Standardwert): Ein gehaltener Anrufer soll keine Wartemusik hören. • *<Wave-Datei>*: Der gerufene Teilnehmer soll die ausgewählte Wave-Datei hören.
Anzahl der Wiedergaben	Wählen Sie aus, wie oft die Ansage hintereinander abgespielt werden soll. Mögliche Werte: • *Endlos (Standardwert)* • *1* bis *10*

17.8.1.2 Variante 1 und 2

Sie können zwei Varianten des Melderufs konfigurieren. In der Regel wird eine Variante die Möglichkeit nutzen, interne Teilnehmer zu rufen, die andere die Möglichkeit, externe Teilnehmer zu rufen.

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Zuordnung	Sie können jedem Melderuf bis zu acht interne Rufnummern oder zwei externe Rufnummern zuordnen. Legen Sie fest, ob die Anrufe bei einem Melderuf bei den internen Teilnehmern oder bei dem externen Teilnehmer signalisiert werden sollen. Mögliche Werte:

Feld	Beschreibung
	• *Extern*: Die eingetragene externe Rufnummer wird gerufen. Bei einem Melderuf können zwei externe Nummern alternativ angerufen werden. • *Intern* (Standardwert): Die Teilnehmer, die den ausgewählten Rufnummern zugeordnet sind, werden entsprechend der eingestellten Signalisierung gerufen. Bei einem Melderuf können acht interne Teilnehmer gleichzeitig angerufen werden.
Erste Externe Rufnummer	Nur für **Zuordnung** = *Extern*Geben Sie die erste Rufnummer des externen Teilnehmers ein.
Zweite externe Rufnummer	Nur für **Zuordnung** = *Extern*Geben Sie die zweite Rufnummer des externen Teilnehmers ein.
Interne Zuordnung	Nur für **Zuordnung** = *Intern*Wählen Sie die internen Teilnehmer aus. Fügen Sie mit **Hinzufügen** weitere interne Rufnummern hinzu.

17.9 Voice Mail System

Das Voice Mail System ist ein intelligenter Anrufbeantworter für die Nutzer Ihrer Telefonanlage . Für jede Nebenstelle kann eine individuelle Voice Mail Box konfiguriert werden. Über einen persönlichen PIN-Code können alle Teilnehmer ihre Nachrichten von jedem Telefon aus abhören, speichern oder löschen.

Die Teilnehmer können sich per E-Mail über eingegangene Anrufe informieren lassen. Aufgezeichnete Nachrichten können automatisch an eine beliebige E-Mail-Adresse weitergeleitet werden.

Die allgemeinen Einstellungen des Voice Mail Systems werden auf Ihrer Telefonanlage vorgenommen. Die Bedienung der individuellen Voice Mail Box erfolgt über ein Telefon.

Jeder Teilnehmer kann seine individuelle Voice Mail Box nutzen, indem er sein Telefon auf seine Voice Mail Box umleitet.

Hinweis

Wenn Sie eine Voice Mail Box nutzen wollen, benötigen Sie eine installierte SD-Karte. Gegebenenfalls müssen Sie die benötigte Ordnerstruktur mit den Ansagetexten auf die SD-Karte laden. Wählen Sie dazu im Menü **Wartung**->**Software &Konfiguration** die Option *Voice Mail Wave-Dateien importieren*.

Achtung

Entfernen Sie die SD-Karte nicht während eines Lese- oder Schreibzugriffes, um Datenverlust oder einen Defekt der Karte zu vermeiden. Beobachten Sie die entsprechende LED an der Geräteoberseite: bei einem Lese- oder Schreibzugriff flackert diese.

17.9.1 Voice Mail Boxen

Im Menü **Anwendungen**->**Voice Mail System**->**Voice Mail Boxen** wird eine Liste mit den individuellen Voice Mail Boxes der einzelnen Teilnehmer angezeigt, sofern Voice Mail Boxes konfiguriert sind.

Abb. 146: **Anwendungen**->**Voice Mail System**->**Voice Mail Boxen**

Werte in der Liste Voice Mail Boxen

Feld	Beschreibung
Interne Rufnummer	Zeigt die Rufnummer des internen Teilnehmers an, für den die Voice Mail Box konfiguriert ist.
Benutzer	Zeigt den Namen des internen Teilnehmers an, für den die Voice Mail Box konfiguriert ist.
Sprache	Zeigt die Sprache der Ansagetexte auf der Voice Mail Box an. *Standard* bedeutet, dass die zentral eingestellte Sprache benutzt wird, die im Menü **Anwendungen**->**Voice Mail System**->**Allgemein** für das gesamte Voice Mail System festgelegt ist.
Benachrichtigung	Zeigt, ob der Teilnehmer über entgangene Anrufe informiert wird.

Feld	Beschreibung
Aktive Anrufvariante	Zeigt den aktuellen Zustand der Voice Mail Box (*Im Büro* oder *Außer Haus*.
Lizenz Zuordnung	Zeigt, ob einer Voice Mail Box aktuell eine Lizenz zugeordnet ist.

Hinweis

Die Anzahl der konfigurierten Voice Mail Boxes darf die Anzahl der vorhandenen Lizenzen übersteigen. Sie müssen jedoch darauf achten, dass die Anzahl der aktuell verwendeten Voice Mail Boxes durch die Anzahl der Lizenzen abgedeckt ist.

17.9.1.1 Bearbeiten oder Neu

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

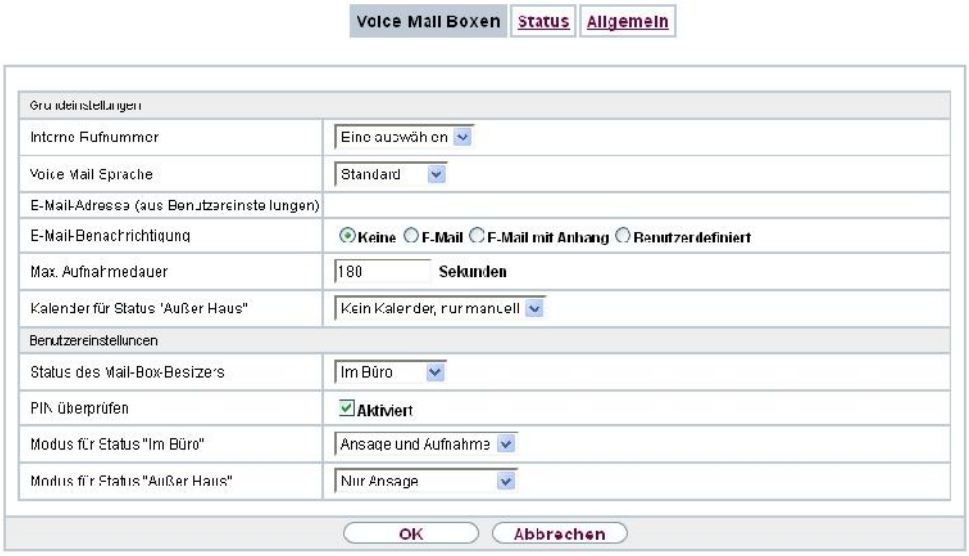


Abb. 147: **Anwendungen->Voice Mail System->Voice Mail Boxen->Neu**

Das Menü **Anwendungen->Voice Mail System->Voice Mail Boxen->Neu** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Interne Rufnummer	Wählen Sie die interne Rufnummer des Teilnehmers, für den Sie eine Voice Mail Box einrichten wollen. Sie können unter den internen Rufnummern wählen, die im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer** konfiguriert sind.
Voice Mail Sprache	Wählen Sie die gewünschte Sprache für die Ansagen der Voice Mail Box. Mögliche Werte: • *Deutsch*: Die Voice Mail Box verwendet deutsche Texte. • *Niederländisch*: Die Voice Mail Box verwendet niederländische Texte. • *Englisch*: Die Voice Mail Box verwendet englische Texte. • *Italienisch*: Die Voice Mail Box verwendet italienische Texte. • *Französisch*: Die Voice Mail Box verwendet französische Texte. • *Standard* (Standardwert): Die Voice Mail Box verwendet die Sprache, welche im Menü **Anwendungen**->**Voice Mail**->**Allgemein** zentral für das gesamte Voice Mail System festgelegt ist. **Hinweis** Eine Einstellung abweichend von *Standard* benötigen Sie nur dann, wenn Sie innerhalb Ihres Voice Mail Systems Voice Mail Boxes mit verschiedenen Sprachen betreiben wollen.
E-Mail-Adresse (aus Benutzereinstellungen)	Hier wird die E-Mail-Adresse des Benutzers angezeigt, an welche eine Benachrichtigung geschickt werden soll, wenn auf der Voice Mail Box eine Nachricht hinterlassen wurde. Die E-Mail-Adresse wird im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Grundeinstellungen** hinterlegt.
E-Mail-Benachrichtigung	Wenn eine Nachricht auf der Voice Mail Box hinterlassen wurde, kann der Teilnehmer benachrichtigt werden.

Feld	Beschreibung
	Mögliche Werte: • *Keine* (Standardwert): Der Teilnehmer wird nicht benachrichtigt. • *E-Mail*: Der Teilnehmer wird per E-Mail über eine hinterlassene Nachricht informiert. • *E-Mail mit Anhang*: Wenn ein Anrufer eine Nachricht hinterlassen hat, erhält der Teilnehmer eine E-Mail mit einer Aufzeichnung der Nachricht im Anhang. • *Benutzerdefiniert*: Wenn der Administrator die Funktion *Benutzerdefiniert* freischaltet, kann die Einstellung für die E-Mail-Benachrichtigung vom Benutzer im **Benutzerzugang** verändert werden.Setzt der Administrator einen anderen Wert, sind Veränderungen durch den Benutzer gesperrt.  **Hinweis** Nachdem ein Teilnehmer per E-Mail über eine neue Nachricht informiert wurde, ändert sich der **Status** der Mitteilung entsprechend den Einstellungen im **Benutzerzugang**. So können Sie im Menü **Benutzerzugang**->**Voice Mail System**->**Einstellungen** unter **Verhalten der E-Mail-Weiterleitung** das Status-Verhalten konfigurieren.
Max. Aufnahmedauer	Geben Sie die maximale Aufzeichnugszeit pro Nachricht ein. Mögliche Werte sind *5* bis *300* Sekunden, der Standardwert ist *180* Sekunden.
Kalender für Status "Außer Haus"	Wenn der Teilnehmer außer Haus ist, kann die Voice Mail Box über einen Kalender geschaltet werden. Wenn ein Kalender verwendet werden soll, muss dieser im Menü **Anwendungen**->**Kalender** mit der Einstellung **Anwendung** = *Voice Mail System* konfiguriert sein. Mögliche Werte: • *Kein Kalender, nur manuell* (Standardwert): Der Teilnehmer kann die Voice Mail Box manuell ein- oder ausschalten. • <Kalender>: Die Voice Mail Box kann mit Hilfe des gewählten

Feld	Beschreibung
	Kalenders zu den dort festgelegten Zeiten ein- oder ausgeschaltet werden.

Felder im Menü Benutzereinstellungen

Feld	Beschreibung
Status des Mail-Box-Besitzers	Bestimmen Sie, mit welchem Modus die Mail Box beim Start des Voice Mail Systems benutzt werden soll. Mögliche Werte: • *Im Büro* (Standardwert): Wählen Sie diese Einstellung, wenn sich der Teilnehmer im Büro befindet, wenn das Voice Mail System gestartet wird. • *Außer Haus*: Wählen Sie diese Einstellung, wenn sich der Teilnehmer außer Haus befindet, wenn das Voice Mail System gestartet wird.
PIN überprüfen	Wählen Sie, ob die aktuell konfigurierte Voice Mail Box durch eine PIN geschützt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Die PIN für die persönliche Voice Mail Box können Sie im Menü **Nummerierung**->**Benutzereinstellungen**->**Benutzer**->**Berechtigungen** unter **PIN für Zugang via Telefon** ändern.
Modus für Status "Im Büro"	Die Voice Mail Box kann während der Bürozeiten mit zwei verschiedenen Einstellungen betrieben werden. Mögliche Werte: • *Ansage und Aufnahme* (Standardwert): Ein Anrufer hört einen Ansagetext und kann eine Nachricht hinterlassen. • *Nur Ansage*: Ein Anrufer hört einen Ansagetext, kann aber selbst keine Nachricht hinterlassen.
Modus für Status "Außer Haus"	Die Voice Mail Box kann außerhalb der Bürozeiten mit zwei verschiedenen Einstellungen betrieben werden. Mögliche Werte: • *Nur Ansage* (Standardwert): Ein Anrufer hört einen Ansage-

Feld	Beschreibung
	text, kann aber selbst keine Nachricht hinterlassen. • *Ansage und Aufnahme* : Ein Anrufer hört einen Ansagetext und kann eine Nachricht hinterlassen.

17.9.2 Status

Im Menü **Anwendungen**->**Voice Mail**->**Status** wird der Status der individuellen Voice Mail Boxes der einzelnen Teilnehmer angezeigt. Sie können sehen, wie viele neue Anrufe auf welcher Voice Mail Box eingegangen sind und wie viele "alte" Anrufe bereits vorhanden waren.

Abb. 148: **Anwendungen**->**Voice Mail**->**Status**

Werte in der Liste Systemmeldungen

Feld	Beschreibung
Interne Rufnummer	Zeigt die Rufnummer des internen Teilnehmers an, für den die Voice Mail Box konfiguriert ist.
Benutzer	Zeigt den Namen des internen Teilnehmers an, für den die Voice Mail Box konfiguriert ist.
Neue Anrufe	Zeigt die Anrufe, die vom Teilnehmer noch nicht abgehört wurden.
Alte Anrufe	Zeigt die Anrufe, die vom Teilnehmer bereits abgehört oder gespeichert wurden.

17.9.3 Allgemein

In diesem Menü konfigurieren Sie die allgemeinen Einstellungen für Ihr Voice Mail System.

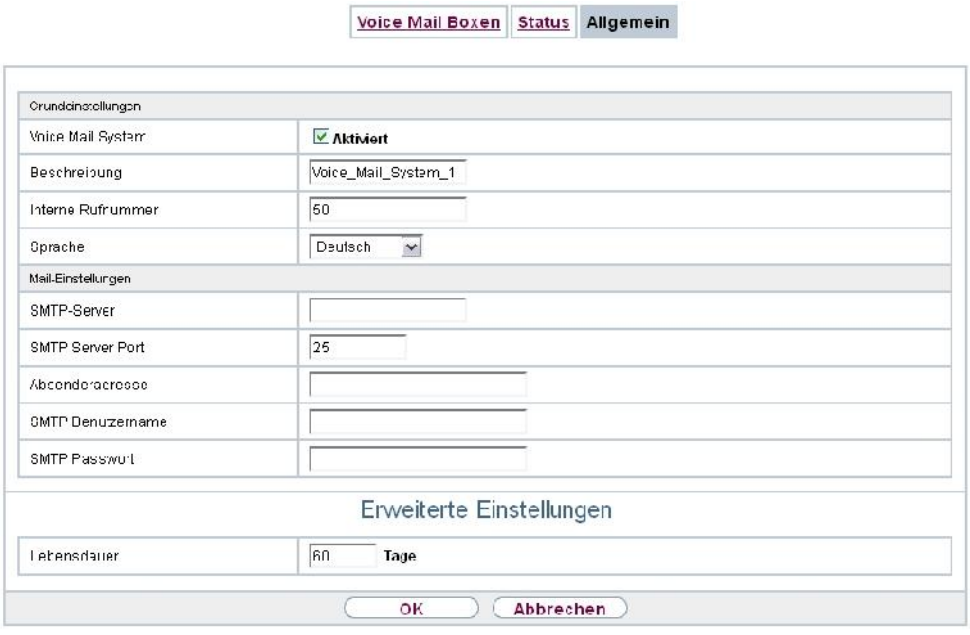


Abb. 149: **Anwendungen->Voice Mail->Allgemein**

Das Menü **Anwendungen->Voice Mail->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Voice Mail System	Wählen Sie, ob Ihre Voice Mail System aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Nur für **Voice Mail System** aktiviert. Geben Sie eine Beschreibung für Ihr Voice Mail System ein. Wenn ein Telefon beim Voice Mail System anruft, wird diese Beschreibung am Telefon angezeigt. Standardwert ist *Voice Mail*.
Interne Rufnummer	Nur für **Voice Mail System** aktiviert. Tragen Sie die interne Rufnummer ein, unter der Ihr Voice Mail Systems zu erreichen ist.

Feld	Beschreibung
	Standardwert ist *50*.
Sprache	Wählen Sie die Sprache für das gesamte Voice Mail System. Mögliche Werte: • *Deutsch* (Standardwert) • *Niederländisch* • *Englisch* • *Italienisch* • *Französisch* Abweichend von der hier eingestellten Sprache kann im Menü **Anwendungen**->**Voice Mail**->**Voice Mail Boxen**->**Neu** für jede Voice Mail Box individuell eine Sprache festgelegt werden.

Felder im Menü Mail-Einstellungen

Feld	Beschreibung
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des E-Mail-Servers ein, der für die Versendung von E-Mails genutzt werden soll.
SMTP Server Port	Geben Sie den Port ein, der für die Versendung von E-Mails benutzt werden soll. Standardwert ist *25*.
Absenderadresse	Geben Sie eine beliebige Adresse ein, die bei der Versendung von E-Mails als Absender genutzt werden soll. Die Adresse dient lediglich zur Kennzeichnung der E-Mails im Posteingang.
SMTP Benutzername	Geben Sie den Benutzernamen für den SMTP-Server ein.
SMTP Passwort	Geben Sie das Passwort für den Benutzer des SNMP-Servers ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Lebensdauer	Die Voice-Mail-Nachrichten werden nach einer einstellbaren Zeit automatisch gelöscht. Mögliche Werte sind *10* bis *60* Tage. Standardwert ist *60*.

Kapitel 18 LAN

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

18.1 IP-Konfiguration

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

18.1.1 Schnittstellen

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

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

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

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

Hinweis

Beachten Sie bitte:

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

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

Beispiel Teilnetze

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

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

18.1.1.1 Bearbeiten oder Neu

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

Abb. 150: **LAN->IP-Konfiguration->Schnittstellen->** **/Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird.

Feld	Beschreibung
	Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.
Adressmodus	Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird. Mögliche Werte: • *Statisch* (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in **IP-Adresse / Netzmaske** zugewiesen. • *DHCP*: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse / Netzmaske	Nur für **Adressmodus** = *Statisch* Fügen Sie mit **Hinzufügen** einen neuen Adresseintrag hinzu und geben Sie die **IP-Adresse** und die entsprechende **Netzmaske** der virtuellen Schnittstelle ein.
Schnittstellenmodus	Nur bei physikalischen Schnittstellen im Routing-Modus und bei virtuelle Schnittstellen. Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: • *Untagged* (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet. • *Tagged (VLAN)*: Diese Option gilt nur für Routing-Schnittstellen. Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu. Dies geschieht über die VLAN-ID, die in diesem Modus angezeigt wird und konfiguriert werden kann. Die Definition einer MAC-Adresse in **MAC-Adresse** ist in diesem Modus optional.
MAC-Adresse	Geben Sie die mit der Schnittstelle verbundene MAC-Adresse ein. Sie können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde, wenn Sie **Voreingestellte verwenden** aktivieren. Die VLAN IDs müssen sich jedoch unterscheiden. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt (sie können jedoch geändert werden).

Feld	Beschreibung
	Wenn **Voreingestellte verwenden** aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet. Standardmäßig ist **Voreingestellte verwenden** aktiv.
VLAN-ID	Nur für **Schnittstellenmodus** = *Tagged (VLAN)* Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben. Mögliche Werte sind *1* (Standardwert) bis *4094*.

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Proxy ARP	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für definierte Gegenstellen beantworten soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-MSS-Clamping	Wählen Sie aus, ob Ihr Gerät das Verfahren MSS Clamping anwenden soll. Um die Fragmentierung von IP-Paketen zu verhindern, wird hierbei vom Gerät automatisch die MSS (Maximum Segment Size) auf den hier einstellbaren Wert verringert. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Bei Aktivierung ist im Eingabefeld der Standardwert *1350* eingetragen.

18.2 VLAN

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

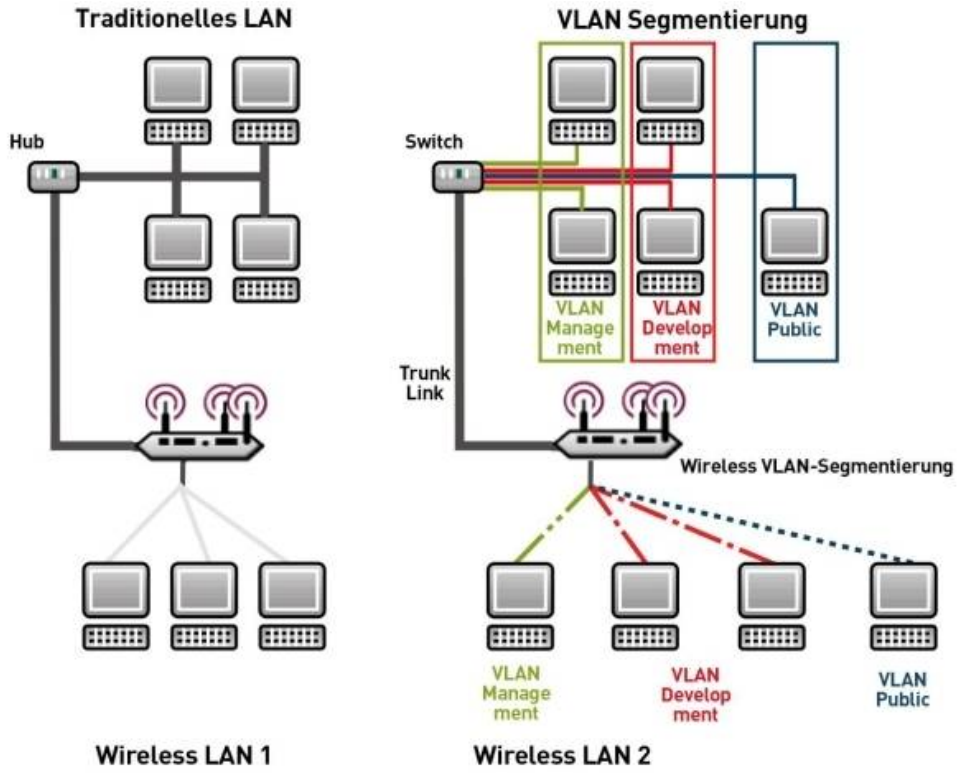


Abb. 151: VLAN-Segmentierung

VLAN für Bridging und VLAN für Routing

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

Achtung

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

18.2.1 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.

18.2.1.1 Bearbeiten oder Neu

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

Abb. 152: **LAN->VLAN->VLANs->Neu**

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

Felder im Menü VLAN konfigurieren

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

Feld	Beschreibung
	übertragen werden sollen.

18.2.2 Portkonfiguration

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

Abb. 153: **LAN->VLANs->Portkonfiguration**

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

Felder im Menü Portkonfiguration

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

18.2.3 Verwaltung

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

Abb. 154: **LAN->VLANs->Verwaltung**

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

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

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

Kapitel 19 Wireless LAN Controller

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

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

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

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

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

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

19.1 Wizard

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

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

Hinweis

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

19.1.1 Grundeinstellungen

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

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

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

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

Schnittstelle

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

DHCP-Server

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

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

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

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

IP-Adressbereich

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

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

19.1.2 Funkmodulprofil

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

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

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

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

Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Standardmäßig ist die Funktion nicht aktiv.

19.1.3 Drahtlosnetzwerk

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

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

Mithilfe von -Symbol können Sie Einträge löschen.

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

Hinweis

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

19.1.3.1 Drahtlosnetzwerke ändern oder hinzufügen

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

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

Folgende Parameter stehen zur Verfügung

Netzwerkname (SSID)

Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.

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

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

Sicherheitsmodus

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

Hinweis: *WPA-Enterprise* bedeutet 802.11x.

WPA-Modus

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

Preshared Key

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

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

Wichtig

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

RADIUS-Server

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

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

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

EAP-Vorabauthentifizierung

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

VLAN

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

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

Hinweis

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

19.1.4 Automatische Installation starten

Sie sehen eine Liste der gefundenen Access Points.

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

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

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

Standort

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

Zugewiesene Drahtlosnetzwerke (VSS)

Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

Folgende Parameter stehen im Menü Funkmodul 1 zur Verfügung:

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

Betriebsmodus

Wählen Sie den Betriebsmodus des Funkmoduls.

Mögliche Werte:

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

- *Aus*: Das Funkmodul ist nicht aktiv.

Aktives Funkmodulprofil

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

Kanal

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

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

Hinweis

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

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

Sendeleistung

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

Mit **OK** übernehmen Sie die Einstellungen.

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

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

Hinweis

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

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

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

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

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

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

19.2 Controller-Konfiguration

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

19.2.1 Allgemein

Abb. 155: **Wireless LAN Controller->Controller-Konfiguration->Allgemein**

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

Felder im Menü Grundeinstellungen

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

Feld	Beschreibung
	Hinweis: Stellen Sie bei Nutzung eines externen DHCP-Servers sicher, dass CAPWAP Option 138 aktiv ist. Wenn Sie z. B. ein bintec elmeg Gateway als DHCP-Server verwenden wollen, klicken Sie im **GUI** Menü dieses Geräts unter **Lokale Dienste**->**DHCP-Server**->**DHCP Pool**->**Neu**->**Erweiterte Einstellungen** im Feld **DHCP-Optionen** auf die Schaltfläche **Hinzufügen**. Wählen Sie als **Option** *CAPWAP Controller* und tragen Sie im Feld **Wert** die IP-Adresse des WLAN Controllers ein. Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü **Systemverwaltung**->**Globale Einstellungen**->**System** im Feld **Manuelle IP-Adresse des WLAN-Controller** eintragen. Mögliche Werte: • *Extern oder statisch* (Standardwert): Ein externer DHCP-Server mit aktiver CAPWAP Option 138 vergibt die IP-Adressen an die APs oder Sie vergeben statische IP-Adressen an die APs. • *Intern*: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.
IP-Adressbereich	Nur für **DHCP-Server** = *Intern* Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein. Diese IP-Adressen und Ihr Gerät müssen aus demselben Netz stammen.
Slave-AP-Standort	Wählen Sie aus, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden. Mögliche Werte: • *Lokal (LAN)* (Standardwert) • *Entfernt (WAN)* Die Einstellung *Entfernt (WAN)* ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die

Feld	Beschreibung
	APs über VPN angebunden sind, kann es vorkommen, dass eine Verbindung unterbrochen wird. In diesem Fall behält der entsprechende AP mit der Einstellung *Entfernt (WAN)* seine Konfiguration bis die Verbindung wieder hergestellt ist. Danach bootet er und anschließend synchronisieren sich Controller und AP erneut.
Slave-AP-LED-Modus	Wählen Sie das Leuchtverhalten der Slave-AP-LEDs. Mögliche Werte: • *Status* (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde. • *Blinkend*: Die LEDs zeigen ihr Standardverhalten. • *Aus*: Alle LEDs sind deaktiviert.

19.3 Slave-AP-Konfiguration

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

19.3.1 Slave Access Points

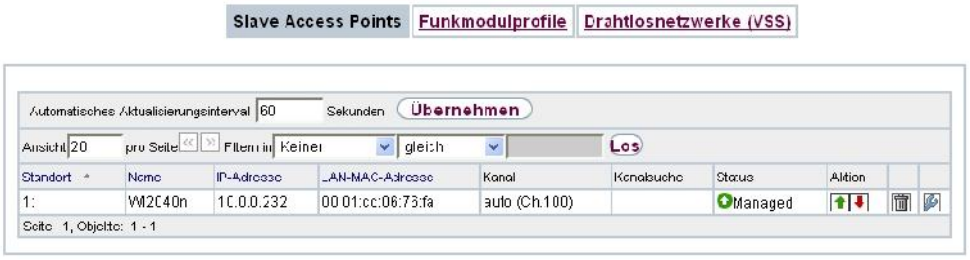


Abb. 156: **Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points**

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

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

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

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

Mögliche Werte für Status

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

19.3.1.1 Bearbeiten

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

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

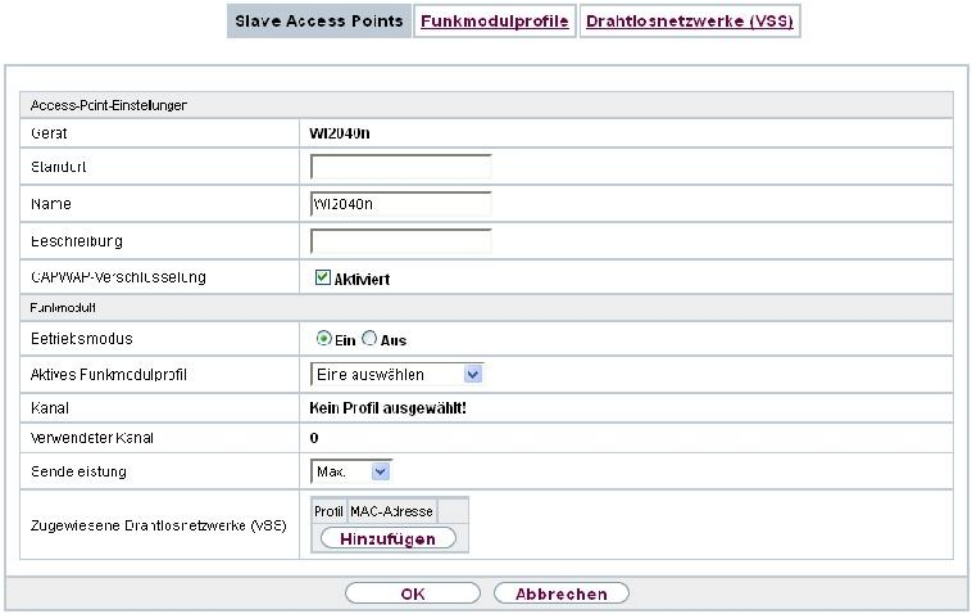


Abb. 157: **Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points->**

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Gerät	Zeigt den Gerätetyp des APs.
Standort	Zeigt den Standort des APs. Wenn kein Standort angegeben ist, werden die Standorte nummeriert. Sie können einen anderen Standort eingeben.
Name	Zeigt den Namen des APs. Sie können den Namen ändern.
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den AP ein.
CAPWAP-Verschlüsselung	Wählen Sie aus, ob die Kommunikation zwischen Master und Slaves verschlüsselt werden soll.

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

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

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

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

19.3.2 Funkmodulprofile

Abb. 158: **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile**

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

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

19.3.2.1 Bearbeiten oder Neu

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

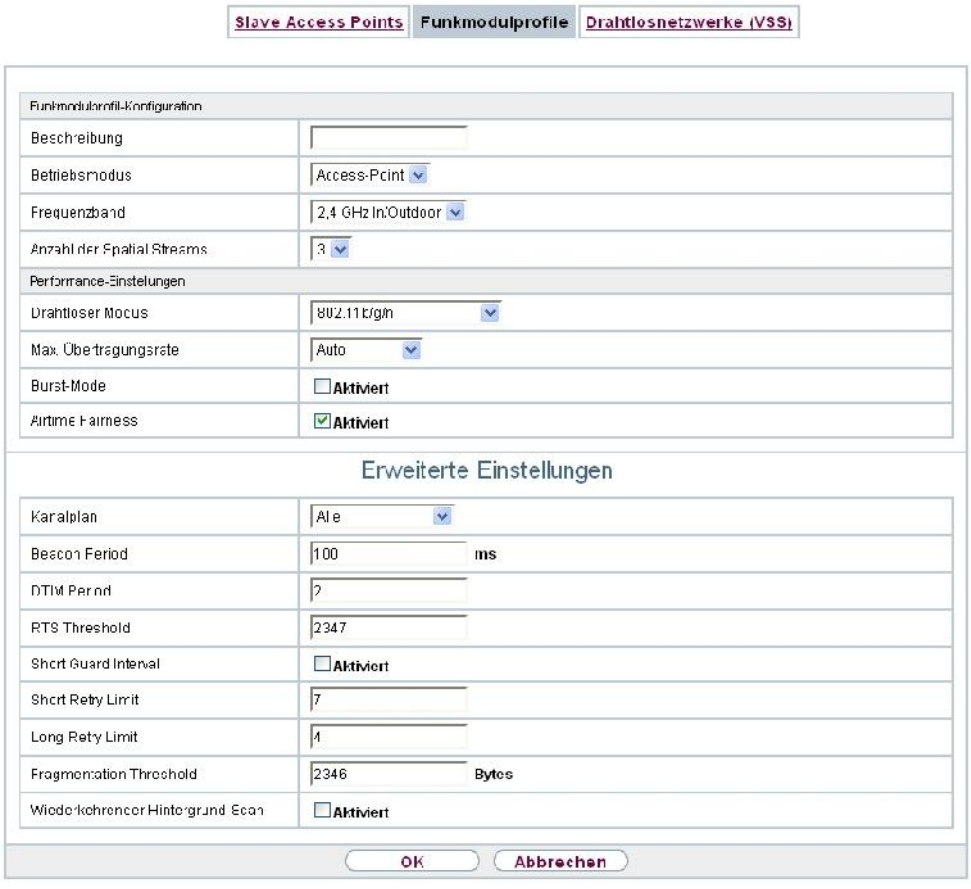


Abb. 159: **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile-> / Neu**

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

Felder im Menü Funkmodulprofil-Konfiguration

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

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

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

Felder im Menü Performance-Einstellungen

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

Feld	Beschreibung
	• *802.11a*: Ihr Gerät arbeitet ausschließlich nach 802.11a. • *802.11n*: Ihr Gerät arbeitet ausschließlich nach 802.11n. • *802.11a/n*: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n.
Max. Übertragungsrate	Wählen Sie die Übertragungsgeschwindigkeit aus. Mögliche Werte: • *Auto* (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt. • *<Wert>*: Je nach Einstellung für **Frequenzband**, **Bandbreite**, **Anzahl der Spatial Streams** und **Drahtloser Modus** stehen verschiedene feste Werte in MBit/s zur Auswahl.
Burst-Mode	Aktivieren Sie diese Funktion, um die Übertragungsgeschwindigkeit für 802.11g durch Frame Bursting zu erhöhen. Dabei werden mehrere Pakete nacheinander ohne Wartezeiten verschickt. Dies ist besonders effektiv im 11b/g Mischbetrieb. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion nicht aktiv sein.
Airtime Fairness	Diese Funktion ist nicht für alle Geräte verfügbar. Mit der **Airtime Fairness** -Funktion wird gewährleistet, dass Senderessourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	Das DTIM Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *2*.
RTS Threshold	Sie können hier den Schwellwert in Bytes (1..2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden.
Short Guard Interval	Aktivieren Sie diese Funktion, um den Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
Short Retry Limit	Geben Sie die maximale Anzahl von Sendeversuchen eines Frames ein, dessen Länge kürzer oder gleich dem in **RTS Threshold** definierten Wert ist. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *7*.
Long Retry Limit	Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, dessen Länge größer ist als der in **RTS Threshold** definierte Wert. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen. Mögliche Werte sind *1* bis *255*. Der Standardwert ist *4*.
Fragmentation Threshold	Geben Sie die maximale Größe in Byte an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert. Möglich Werte sind *256* bis *2346*.

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

19.3.3 Drahtlosnetzwerke (VSS)

Abb. 160: **Wireless LAN Controller->Slave-AP-Konfiguration->Drahtlosnetzwerke (VSS)**

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

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

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

19.3.3.1 Bearbeiten oder Neu

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

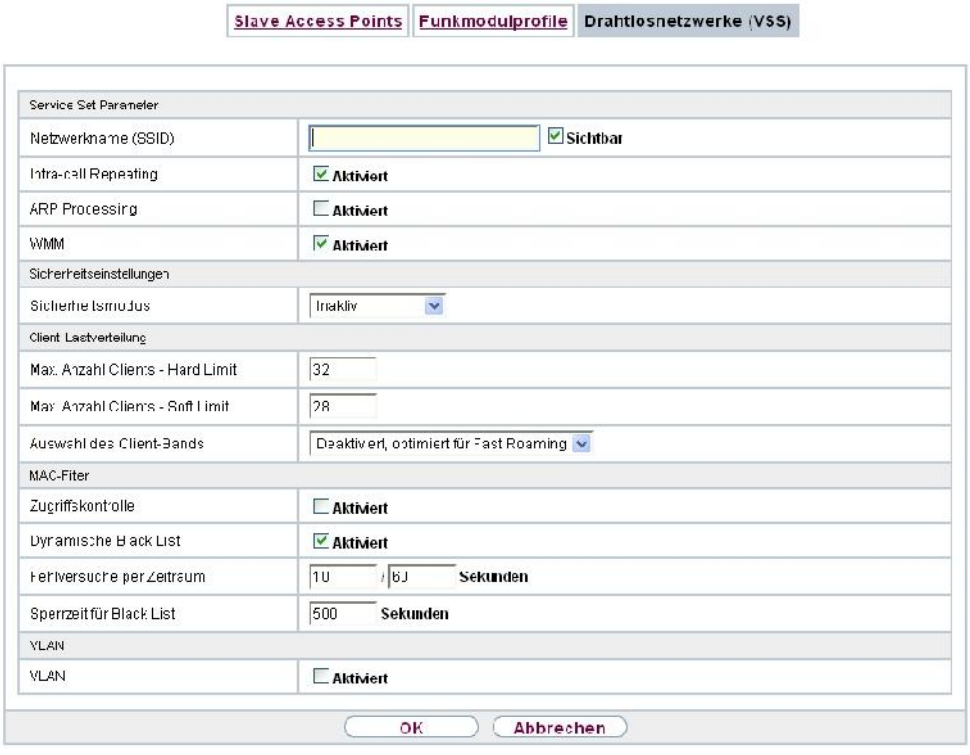


Abb. 161: **Wireless LAN Controller->Slave-AP-Konfiguration->Drahtlosnetzwerke (VSS)->Neu**

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

Felder im Menü Service Set Parameter

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

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

Felder im Menü Sicherheitseinstellungen

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

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

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

Feld	Beschreibung
	se über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü Client-Lastverteilung

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

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

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	Wählen Sie aus, ob für dieses Drahtlosnetzwerk nur bestimmte Clients zugelassen werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Erlaubte Adressen	Legen Sie Einträge mit **Hinzufügen** an und geben Sie die MAC-Adressen der Clients (**MAC-Adresse**) ein, die zugelassen werden sollen.
Dynamische Black List	Mithilfe der Funktion **Dynamische Black List** ist es möglich, Clients, die sich möglicherweise unbefugt Zugriff auf das Netzwerk verschaffen wollen, zu erkennen und für einen bestimmten Zeitraum zu sperren. Ein Client wird dann gesperrt, wenn die

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

Felder im Menü VLAN

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

19.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.

19.4.1 Aktive Clients

Abb. 162: **Wireless LAN Controller->Monitoring->Aktive Clients**

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

Für jeden Client sehen Sie einen Eintrag mit folgendem Parametersatz: **Standort**, **Name**, **VSS**, **Client MAC**, **Client-IP-Adresse**, **Signal : Noise (dBm)** , **Status**, **Uptime**.

Mögliche Werte für Status

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

19.4.2 Drahtlosnetzwerke (VSS)

Abb. 163: **Wireless LAN Controller->Monitoring->Drahtlosnetzwerke (VSS)**

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

19.4.3 Client-Verwaltung

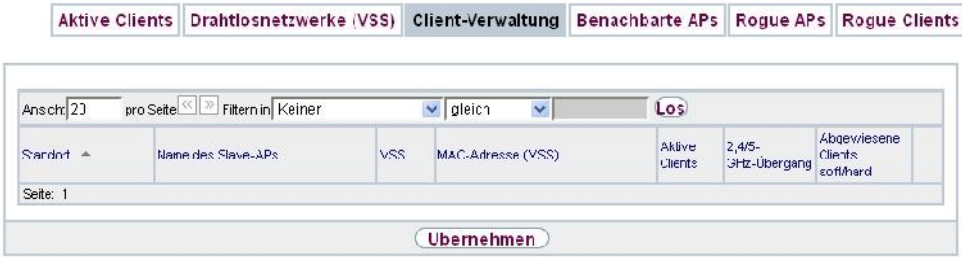


Abb. 164: **Wireless LAN Controller->Monitoring+Client-Verwaltung**

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

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

19.4.4 Benachbarte APs

Abb. 165: **Wireless LAN Controller->Monitoring->Benachbarte APs**

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

Hinweis

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

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

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

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

19.4.5 Rogue APs

Abb. 166: **Wireless LAN Controller->Monitoring->Rogue APs**

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

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

Hinweis

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

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

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

19.4.6 Rogue Clients

Abb. 167: **Wireless LAN Controller->Monitoring->Rogue Clients**

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

Mögliche Werte für Rogue Clients

Status	Bedeutung
MAC-Adresse des Rogue Clients	Zeigt die MAC-Adresse des Clients an, der sich auf der Blacklist befindet.
SSID	Zeigt die beteiligten SSID an.
Angegriffener Access Point	Zeigt den betroffenen AP an.
Signal dBm	Zeigt die Signalstärke des Clients während des Zugriffsversuchs an.
Art des Angriffs	Hier wird die Art des möglichen Angriffs angezeigt, z. B. eine fehlerhafte Authentifizierung.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Zugriffsversuchs an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Zugriffsversuchs an.
Statische Black List	Sie können einen Rogue Client als nicht vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte **Statische Black List** aktivieren. Die Sperrung des Clients endet dann nicht automatisch, sondern muss von Ihnen manuell wieder aufgehoben werden.
Löschen	Mithilfe des -Symbols können Sie Einträge löschen.

19.4.6.1 Neu

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

Abb. 168: **Wireless LAN Controller->Monitoring->Rogue Clients->Neu**

Das Menü besteht aus folgenden Feldern:

Felder im Menü Neuer Eintrag in die Blacklist.

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

19.5 Wartung

Dieses Menü dient zur Wartung Ihrer managed APs.

19.5.1 Firmware-Wartung

Abb. 169: **Wireless LAN Controller->Wartung->Firmware-Wartung**

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

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

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

Mögliche Werte für Status

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

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

Felder im Menü Firmware-Wartung

Feld	Beschreibung
Aktion	Wählen Sie die Aktion aus, die Sie ausführen wollen.

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

Kapitel 20 Netzwerk

20.1 Routen

Standard-Route (Default Route)

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

20.1.1 Konfiguration von IPv4-Routen

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

20.1.1.1 Bearbeiten oder Neu

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

Abb. 170: **Netzwerk**->**Routen**->**Konfiguration von IPv4-Routen**->**Neu** *mit* **Erweiterte Route** = *Standard.*

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

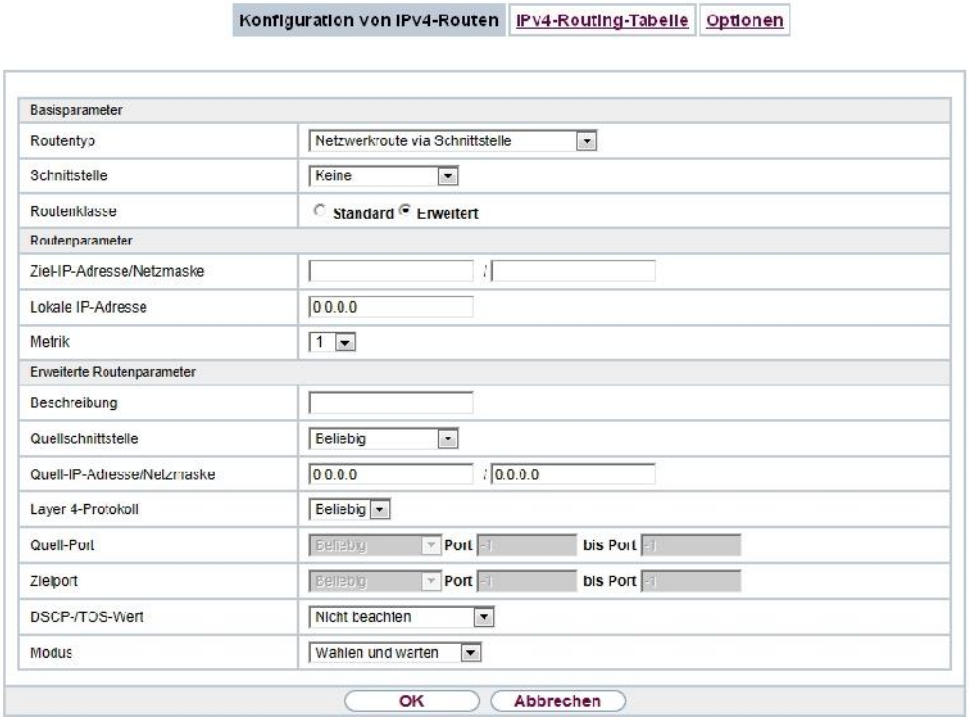


Abb. 171: **Netzwerk**->**Routen**->**Konfiguration von IPv4-Routen**->**Neu** *mit* **Erweitert** = `Aktiviert`

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

Feld im Menü Basisparameter

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

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

Felder im Menü Routenparameter

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

Feld	Beschreibung
	Geben Sie die IP-Adresse des Hosts ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Ziel-IP-Adresse/Netzmaske	Nur für **Routentyp** *Host-Route über Schnittstelle* oder *Netzwerkroute via Schnittstelle* Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein. Bei **Routentyp** = *Netzwerkroute via Schnittstelle* Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.
Gateway-IP-Adresse	Nur für **Routentyp** = *Standardroute über Gateway*, *Host-Route via Gateway* oder *Netzwerkroute via Gateway* Geben Sie die IP-Adresse des Gateways ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von *0* bis *15*. Standardwert ist *1*.

Felder im Menü Erweiterte Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IP-Route ein.
Quellschnittstelle	Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen. Standardwert ist *Keine*.
Quell-IP-Adresse/Netzmaske	Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.
Layer 4-Protokoll	Wählen Sie ein Protokoll aus. Mögliche Werte: *ICMP*, *IGMP*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *PIM*, *L2TP*, *Beliebig*.

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

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

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

20.1.2 IPv4-Routing-Tabelle

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

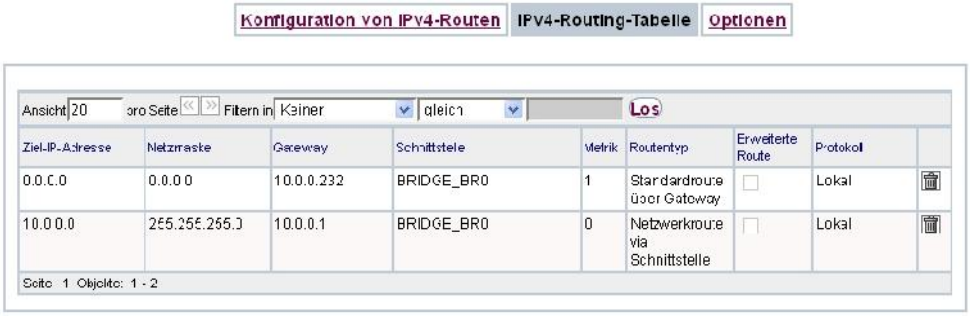


Abb. 172: **Netzwerk**->**Routen**->**IPv4-Routing-Tabelle**

Felder im Menü IPv4-Routing-Tabelle

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

20.1.3 Optionen

Überprüfung der Rückroute

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

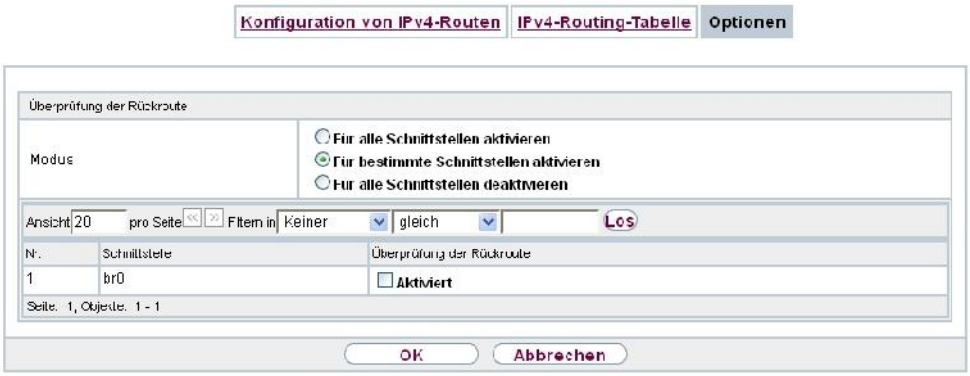


Abb. 173: **Netzwerk->Routen->Optionen**

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

Felder im Menü Überprüfung der Rückroute

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

Feld	Beschreibung
	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.

20.2 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in *NAT-Konfiguration* auf Seite 409).

20.2.1 NAT-Schnittstellen

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

Abb. 174: **Netzwerk**->**NAT**->**NAT-Schnittstellen**

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

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

Optionen im Menü NAT-Schnittstellen

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

20.2.2 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.

20.2.2.1 Neu

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

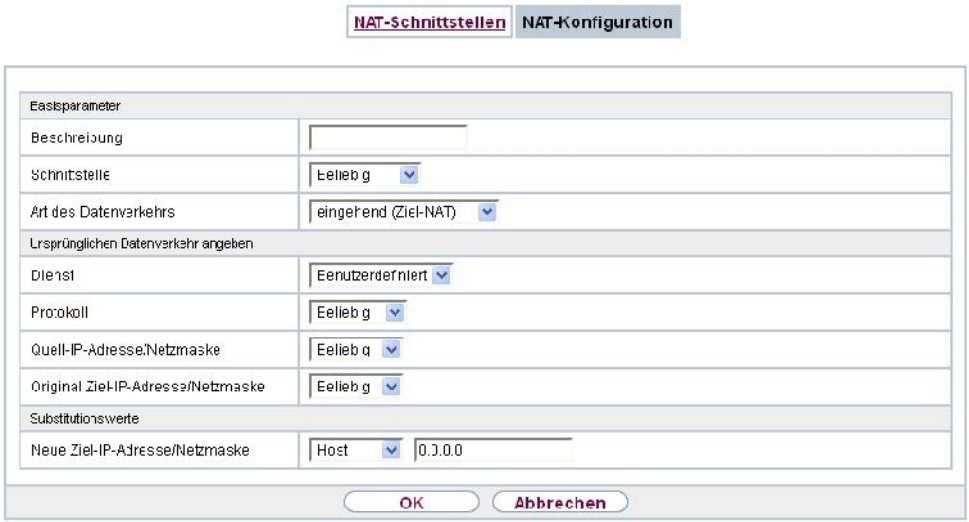


Abb. 175: **Netzwerk->NAT->NAT-Konfiguration ->Neu**

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

Feld im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
Schnittstelle	Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll. Mögliche Werte: • *Beliebig* (Standardwert): NAT wird für alle Schnittstellen konfiguriert. • *<Schnittstellenname>*: Wählen Sie eine der 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.

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

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

Felder im Menü Ursprünglichen Datenverkehr angeben

Feld	Beschreibung
Dienst	Nicht für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *full-cone*, *restricted-cone* oder *port-restricted-cone*. Wählen Sie einen der vorkonfigurierten Dienste aus.

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

Feld	Beschreibung
	• *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP* • *ISO-IP* • *Kryptolan* • *L2TP* • *OSPF* • *PUP* • *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP* • *VRRP* • *XNS-IDP*
Quell-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* oder *exklusiv (ohne NAT)* Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Ziel-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.
Original Ziel-Port/Bereich	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ur-

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

Feld	Beschreibung
	sprünglichen Datenpakete ein. Die Standardeinstellung *-Alle-* bedeutet, dass der Port nicht näher spezifiziert ist.

Im Menü **NAT-Konfiguration** ->**Substitutionswerte** können Sie, abhängig davon, ob es sich um eingehenden oder ausgehenden Datenverkehr handelt, neue Adressen und Ports definieren, auf welche bestimmte Adressen und Ports aus dem Menü **NAT-Konfiguration** ->**Ursprünglichen Datenverkehr angeben** umgesetzt werden.

Felder im Menü Substitutionswerte

Feld	Beschreibung
Neue Ziel-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)* Geben Sie diejenige Ziel-IP-Adresse und die zugehörige Netzmaske ein, auf welche die ursprüngliche Ziel-IP-Adresse umgesetzt werden soll.
Neuer Ziel-Port	Nur für **Art des Datenverkehrs** = *eingehend (Ziel-NAT)*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Belassen Sie den Ziel-Port oder geben Sie denjenigen Ziel-Port ein, auf den der ursprüngliche Ziel-Port umgesetzt werden soll. Mit Auswahl von *Original* belassen Sie den ursprünglichen Ziel-Port. Wenn Sie *Original* deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Ziel-Port eingeben. Standardmäßig ist *Original* aktiv.
Neue Quell-IP-Adresse/Netzmaske	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)* und **NAT-Methode** = *symmetrisch* Geben Sie diejenige Quell-IP-Adresse ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.
Neuer Quell-Port	Nur für **Art des Datenverkehrs** = *ausgehend (Quell-NAT)*, **NAT-Methode** = *symmetrisch*, **Dienst** = *Benutzerdefiniert* und **Protokoll** = *TCP*, *UDP*, *TCP/UDP* Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-Port ein, auf den der ursprüngliche Quell-Port umgesetzt werden soll.

Feld	Beschreibung
	Mit Auswahl von *Original* belassen Sie den ursprünglichen Quell-Port. Wenn Sie *Original* deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Quell-Port eingeben. Standardmäßig ist *Original* aktiv. Haben Sie für **Original Quell-Port/Bereich** *Portbereich angeben* gewählt, stehen folgende Auswahlmöglichkeiten zur Verfügung: • *Original Quell-Port/Bereich verwenden*: Der in **Original Quell-Port/Bereich** angegebene Bereich wird nicht verändert, die Portnummern bleiben erhalten. • *Verwende Port/Bereich beginnend bei*: Es erscheint ein Eingabefeld, in das Sie die Portnummer eingeben können, bei der der Portbereich beginnen soll, durch den der ursprüngliche Portbereich ersetzt wird. Die Anzahl der Ports bleibt dabei gleich.

20.3 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

20.3.1 QoS-Filter

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

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

20.3.1.1 Neu

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

Abb. 176: **Netzwerk->QoS->QoS-Filter->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Standardwert ist *Benutzerdefiniert*.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.

Feld	Beschreibung
Typ	Nur für **Protokoll** = *ICMP* Wählen Sie einen Typ aus. Mögliche Werte: *Beliebig*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Siehe RFC 792. Standardwert ist *Beliebig*.
Verbindungsstatus	Bei **Protokoll** = *TCP* können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt. Mögliche Werte: • *Hergestellt*: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • *Beliebig* (Standardwert): Das Filter passt auf alle TCP-Pakete.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Quell-Port-Nummer bzw. einen Bereich von

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

20.3.2 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.

20.3.2.1 Neu

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

Abb. 177: **Netzwerk**->**QoS**->**QoS-Klassifizierung**->**Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Klassenplan	Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen. Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an. • *<Name des Klassenplans>*: Zeigt einen bereits angeleg-

Feld	Beschreibung
	ten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	Nur für **Klassenplan** = *Neu* Geben Sie die Bezeichnung des Klassenplans ein.
Filter	Wählen Sie ein IP-Filter aus. Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll. Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü **Netzwerk**->**QoS**->**QoS-Filter** konfiguriert sein.
Richtung	Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen. Mögliche Werte: • *Eingehend*: Eingehende Datenpakete werden der im Folgenden zu definierenden Klasse (**Klassen-ID**) zugeordnet. • *Ausgehend* (Standardwert): Ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (**Klassen-ID**) zugeordnet. • *Beide*: Eingehende und ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (**Klassen-ID**) zugeordnet.
High-Priority-Klasse	Aktivieren oder deaktivieren Sie die High-Priority-Klasse. Wenn die High-Priority-Klasse aktiv ist, werden die Datenpakete der Klasse mit der höchsten Priorität zugeordnet, die Priorität 0 wird automatisch gesetzt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Klassen-ID	Nur für **High-Priority-Klasse** nicht aktiv. Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zu-

Feld	Beschreibung
	weist. **Hinweis** Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.) Mögliche Werte sind ganze Zahlen zwischen *1* und *254*.
Setze DSCP/TOS Wert (Layer 3)	Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (**Klassen-ID**) setzen bzw. ändern. Mögliche Werte: • *Erhalten* (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • *DSCP-Hexadezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalem Format). • *TOS-Binärwert*: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • *TOS-Dezimalwert*: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • *TOS-Hexadezimalwert*: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
Setze COS Wert (802.1p/Layer 2)	Hier können Sie die Serviceklasse (Layer-2-Priorität) im VLAN Ethernet Header der IP-Pakete in Abhängigkeit zur definierten Klasse (**Klassen-ID**) setzen/ändern. Mögliche Werte sind ganze Zahlen zwischen *0* und *7*. Standardwert ist *Erhalten*.

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

20.3.3 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.

20.3.3.1 Neu

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

Abb. 178: **Netzwerk**->**QoS**->**QoS-Schnittstellen/Richtlinien**->**Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, für die QoS konfiguriert werden soll.
Priorisierungsalgorithmus	Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausgewählten Schnittstelle. Mögliche Werte: • *Priority Queueing*: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. • *Weighted Round Robin*: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird gemäß der Gewichtung (weight) der Queues verteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig behandelt. • *Weighted Fair Queueing*: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird möglichst "fair" unter den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig bedient. • *Deaktiviert* (Standardwert): QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.

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

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

Feld	Beschreibung
	erkannt wurde. • *Inaktiv*: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • *Nur kontrollierte RTP-Streams*: Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gateway (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW. • *Immer*: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.
Queues/Richtlinien	Konfigurieren Sie die gewünschten QoS-Queues. Für jede angelegte Klasse aus dem Klassenplan, die mit der gewählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und hier angezeigt (nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr). Fügen Sie mit **Hinzufügen** neue Einträge hinzu. Das Menü **Queue/Richtlinie bearbeiten** öffnet sich. Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag DEFAULT mit der niedrigsten Priorität 255 erstellt.

Das Menü **Queue/Richtlinie bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Queue/Richtlinie bearbeiten

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung der Queue/Richtlinie an.
Ausgehende Schnittstelle	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
Priorisierungsqueue	Wählen Sie den Typ für die Priorisierung der Queue aus. Mögliche Werte: • *Klassenbasiert* (Standardwert): Queue für "normal"-klassifizierte Daten. • *Hohe Priorität*: Queue für "high-priority"- klassifizierte

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

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Dropping-Algorithmus	Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird. Mögliche Werte: • *Tail Drop* (Standardwert): Das neu hinzugekommene Paket wird verworfen. • *Head Drop*: Das älteste Paket in der Queue wird verworfen. • *Random Drop*: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Vermeidung von Datenstau (RED)	Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen. Pakete, deren Datengröße zwischen **Min. Queue-Größe** und **Max. Queue-Größe** liegt, werden vorbeugend verworfen, um einen Queue-Überlauf zu verhindern (RED=Random Early Detection). Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine insgesamt kleinere Queue, sodass selbst Traffic-Bursts meist ohne größere Paketverluste übertragen werden können. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Min. Queue-Größe	Geben Sie den unteren Schwellwert für das Verfahren **Vermeidung von Datenstau (RED)** in Byte ein. Mögliche Werte sind *0* bis *262143*. Der Standardwert ist *0*.
Max. Queue-Größe	Geben Sie den oberen Schwellwert für das Verfahren **Vermeidung von Datenstau (RED)** in Byte ein. Mögliche Werte sind *0* bis *262143*. Der Standardwert ist *16384*.

20.4 Zugriffsregeln

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

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

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

Möchten z. B. Standorte, deren LANs über ein bintec elmeg-Gateway miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access-Listen ein effektives Mittel.

Access-Filter auf dem Gateway basieren auf der Kombination von Filtern und Aktionen zu Filterregeln (= rules) und der Verknüpfung dieser Regeln zu sogenannten Regelketten. Sie wirken auf die eingehenden Datenpakete und können so bestimmten Daten den Zutritt zum Gateway erlauben oder verbieten.

Ein Filter beschreibt einen bestimmten Teil des IP-Datenverkehrs, basierend auf Quell- und/oder Ziel-IP-Adresse, Netzmaske, Protokoll, Quell- und/ oder Ziel-Port.

Mit den Regeln, die Sie in Access Lists organisieren, teilen Sie dem Gateway mit, wie es mit gefilterten Datenpaketen umgehen soll – ob es sie annehmen oder abweisen soll. Sie können auch mehrere Regeln definieren, die Sie in Form einer Kette organisieren und ihnen damit eine bestimmte Reihenfolge geben.

Für die Definition von Regeln bzw. Regelketten gibt es verschiedene Ansätze:

Nehme alle Pakete an, die nicht explizit verboten sind, d. h.:

- Weise alle Pakete ab, auf die Filter 1 zutrifft.
- Weise alle Pakete ab, auf die Filter 2 zutrifft.
- ...
- Lass den Rest durch.

oder

Nehme nur Pakete an, die explizit erlaubt sind, d. h.:

- Nehme alle Pakete an, auf die Filter 1 zutrifft.
- Nehme alle Pakete an, auf die Filter 2 zutrifft.
- ...
- Weise den Rest ab.

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

Es können mehrere getrennte Regelketten angelegt werden. Eine gemeinsame Nutzung von Filtern in verschiedenen Regelketten ist dabei möglich.

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.

Achtung

Achten Sie darauf, dass Sie sich beim Konfigurieren der Filter nicht selbst aussperren:

Greifen Sie zur Filter-Konfiguration möglichst über die serielle Konsolen-Schnittstelle oder mit ISDN-Login auf Ihr Gateway zu.

20.4.1 Zugriffsfilter

In diesem Menü werden die Access-Filter konfiguriert. Jedes Filter beschreibt einen bestimmten Teil des IP-Traffic und definiert z. B. die IP-Adressen, das Protokoll, den Quell- oder Ziel-Port.

Im Menü **Netzwerk**->**Zugriffsregeln**->**Zugriffsfilter** wird eine Liste aller Access Filter angezeigt.

Abb. 179: **Netzwerk**->**Zugriffsregeln**->**Zugriffsfilter**

20.4.1.1 Bearbeiten oder Neu

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

Abb. 180: **Netzwerk->Zugriffsregeln->Zugriffsfilter->Neu**

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

Felder im Menü Basisparameter

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

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

Feld	Beschreibung
	• *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk*: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Nur bei **Protokoll** = *TCP*, *UDP* Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein, auf den das Filter passt. Mögliche Werte: • *-Alle-* (Standardwert): Das Filter gilt für alle Port-Nummern • *Port angeben*: Ermöglicht Eingabe einer Port-Nummer. • *Portbereich angeben*: Ermöglicht Eingabe eines Bereiches von Port-Nummern.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse und die Netzmaske der Datenpakete ein.
Quell-Port/Bereich	Nur bei **Protokoll** = *TCP*, *UDP* Geben Sie die Quell-Port-Nummer bzw. den Bereich von Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Das Filter gilt für alle Port-Nummern • *Port angeben*: Ermöglicht Eingabe einer Port-Nummer. • *Portbereich angeben*: Ermöglicht Eingabe eines Bereiches von Port-Nummern.
DSCP/TOS-Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • *DSCP-Dezimalwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).

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

20.4.2 Regelketten

Im Menü **Regelketten** werden Regeln für IP-Filter konfiguriert. Diese können separat angelegt oder in Regelketten eingebunden werden.

Im Menü **Netzwerk**->**Zugriffsregeln**->**Regelketten** werden alle angelegten Filterregeln aufgelistet.

Abb. 181: **Netzwerk**->**Zugriffsregeln**->**Regelketten**

20.4.2.1 Bearbeiten oder Neu

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

Abb. 182: **Netzwerk->Zugriffsregeln->Regelketten->Neu**

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	men, wenn das Filter nicht passt. • *Verweigern, wenn Filter passt*: Paket abweisen, wenn das Filter passt. • *Verweigern, wenn Filter nicht zutrifft*: Paket abweisen, wenn das Filter nicht passt. • *Nicht beachten*: Nächste Regel anwenden.

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

20.4.3 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. 183: **Netzwerk**->**Zugriffsregeln**->**Schnittstellenzuweisung**

20.4.3.1 Bearbeiten oder Neu

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

Abb. 184: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.
Verwerfen ohne Rückmeldung	Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll. • *Aktiviert* (Standardwert) : Der Absender wird nicht informiert. • *Deaktiviert*: Der Absender erhält eine ICMP-Nachricht.
Berichtsmethode	Legen Sie fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll. Mögliche Werte: • *Kein Bericht*: Keine Syslog-Meldung. • *Info* (Standardwert): Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IPAdresse und Quell-Port-Nummer wird generiert. • *Dump*: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

20.5 Drop-In

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

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

20.5.1 Drop-In-Gruppen

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

20.5.1.1 Neu

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

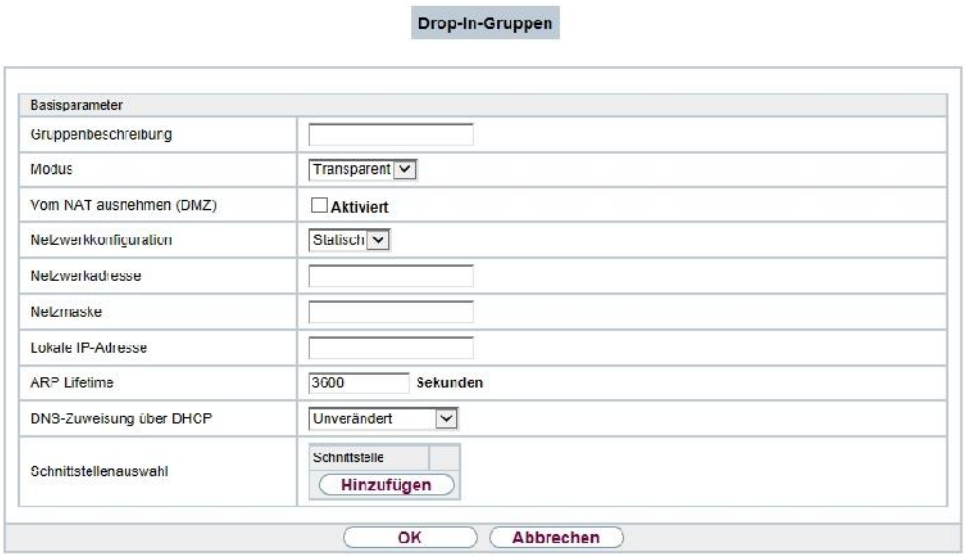


Abb. 185: **Netzwerk**->**Drop-In**->**Drop-In-Gruppen**->**Neu**

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

Felder im Menü Basisparameter

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

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

Kapitel 21 Multicast

Was ist Multicasting?

Viele jüngere Kommunikations-Technologien basieren auf der Kommunikation von einem Sender zu mehreren Empfängern. Daher liegt auf der Reduzierung des Datenverkehrs ein Hauptaugenmerk von modernen Telekommunikationssystemen wie Voice-over-IP oder Video- und Audio-Streaming (z. B. IPTV oder Webradio), z. B. im Rahmen von TriplePlay (Voice, Video, Daten). Multicast bietet eine kostengünstige Lösung zur effektiven Bandbreitennutzung, dadurch dass der Sender das Datenpaket, welches mehrere Empfänger empfangen können, nur einmal senden muss. Dabei wird an eine virtuelle Adresse gesendet, die als Multicast-Gruppe bezeichnet wird. Interessierte Empfänger melden sich bei diesen Gruppen an.

Weitere Anwendungsbereiche

Ein klassischer Einsatzbereich von Multicast sind Konferenzen (Audio/Video) mit mehreren Empfängern. Allen voran dürften die bekanntesten MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) und das Whiteboard (WB) sein. Mit Hilfe von VAT können Audiokonferenzen durchgeführt werden. Hierzu werden alle Gesprächspartner in einem Fenster sichtbar gemacht und der/die Sprecher mit einem schwarzen Kasten gekennzeichnet. Andere Anwendungsgebiete sind vor allem für Firmen interessant. Hier bietet Multicasting die Möglichkeit, die Datenbanken mehrerer Server gleichzeitig zu synchronisieren, was für multinationale oder auch für Firmen mit nur wenigen Standorten lohnenswert ist.

Adressbereich für Multicast

Für IPv4 sind im Klasse-D-Netzwerk die IP-Adressen 224.0.0.0 bis 239.255.255.255 (224.0.0.0/4) für Multicast reserviert. Eine IP-Adresse aus diesem Bereich repräsentiert eine Multicast-Gruppe, für die sich mehrere Empfänger anmelden können. Der Multicast-Router leitet dann gewünschte Pakete in alle Subnetze mit angemeldeten Empfängern weiter.

Multicast Grundlagen

Multicast ist verbindungslos, d. h. eine etwaige Fehlerkorrektur oder Flusskontrolle muss auf Applikationsebene gewährleistet werden.

Auf der Transportebene kommt fast ausschließlich UDP zum Einsatz, da es im Gegensatz

zu TCP nicht an eine Punkt-zu-Punkt-Verbindung angelehnt ist.

Der wesentliche Unterschied besteht somit auf IP-Ebene darin, dass die Zieladresse keinen dedizierten Host adressiert, sondern an eine Gruppe gerichtet ist, d. h. beim Routing von Multicast-Paketen ist allein entscheidend, ob sich in einem angeschlossenen Subnetz ein Empfänger befindet.

Im lokalen Netzwerk sind alle Hosts angehalten, alle Multicast-Pakete zu akzeptieren. Das basiert bei Ethernet oder FDD auf einem sogenannten MAC-Mapping, bei dem die jeweilige Gruppen-Adresse in die Ziel-MAC-Adresse kodiert wird. Für das Routing zwischen mehreren Netzen müssen sich bei den jeweiligen Routern vorerst alle potentiellen Empfänger im Subnetz bekannt machen. Dies geschieht durch sog. Membership-Management-Protokolle wie IGMP bei IPv4 und MLP bei IPv6.

Membership-Management-Protokoll

IGMP (Internet Group Management Protocol) ist in IPv4 ein Protokoll, mit dem Hosts dem Router Multicast-Mitgliedsinformationen mitteilen können. Hierbei werden für die Adressierung IP-Adressen des Klasse-D-Adressraums verwendet. Eine IP-Adresse dieser Klasse repräsentiert eine Gruppe. Ein Sender (z. B. Internetradio) sendet an diese Gruppe. Die Adressen (IP) der verschiedenen Sender innerhalb einer Gruppe werden als Quell(-Adressen) bezeichnet. Es können somit mehrere Sender (mit unterschiedlichen IP-Adressen) an dieselbe Multicast-Gruppe senden. So kommt eine 1-zu-n-Beziehung zwischen Gruppen- und Quelladressen zustande. Diese Informationen werden an den Router über Reports weitergegeben. Ein Router kann bei eingehenden Multicast-Datenverkehr anhand dieser Informationen entscheiden, ob ein Host in seinem Subnetz diesen empfangen will oder nicht. Ihr Gerät unterstützt die aktuelle Version IGMP V3, welche abwärtskompatibel ist, d. h. es können sowohl V3- als auch V1- und V2-Hosts verwaltet werden.

Ihr Gerät unterstützt folgende Multicast-Mechanismen:

- Forwarding (Weiterleiten): Dabei handelt es sich um statisches Forwarding, d.h. eingehender Datenverkehr für eine Gruppe wird auf jeden Fall weitergeleitet. Dies bietet sich an, wenn Multicast-Datenverkehr permanent weitergeleitet werden soll.
- IGMP: Mittels IGMP werden Informationen über die potentiellen Empfänger in einem Subnetz gesammelt. Bei einem Hop kann dadurch eingehender Multicast-Datenverkehr ausgesondert werden.

Tipp

Bei Multicast liegt das Hauptaugenmerk auf dem Ausschluss von Datenverkehr ungewünschter Multicast-Gruppen. Beachten Sie daher, dass bei einer etwaigen Kombination von Forwarding mit IGMP die Pakete an die im Forwarding angegebenen Gruppen auf jeden Fall weitergeleitet werden können.

21.1 Allgemein

21.1.1 Allgemein

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

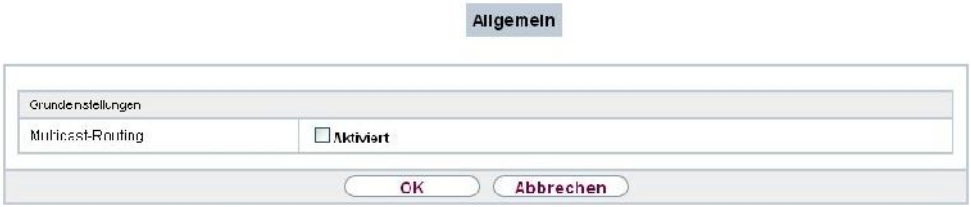


Abb. 186: **Multicast**->**Allgemein**->**Allgemein**

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

Felder im Menü Grundeinstellungen

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

21.2 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.

21.2.1 IGMP

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

21.2.1.1 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. 187: **Multicast->IGMP->IGMP->Neu**

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

Felder im Menü IGMP-Einstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der IGMP aktiviert werden soll, d.h. Queries werden versendet und Antworten akzeptiert.
Abfrage Intervall	Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen. Möglich Werte sind *0* bis *600*.

Feld	Beschreibung
	Der Standardwert ist *125*.
Maximale Antwortzeit	Geben Sie für das Senden von Queries an, in welchem Zeitintervall in Sekunden Hosts auf jeden Fall antworten müssen. Die Hosts wählen aus diesem Intervall zufällig eine Verzögerung, bis die Antwort gesendet wird. Damit können Sie bei Netzen mit vielen Hosts eine Streuung und somit eine Entlastung erreichen. Möglich Werte sind *0,0* bis *25,0*. Der Standardwert ist *10,0*.
Robustheit	Wählen Sie den Multiplikator zur Steuerung interner Timer-Werte aus. Mit einem höheren Wert kann z. B. in einem verlustreichen Netzwerk ein Paketverlust kompensiert werden. Durch einen zu hohen Wert kann sich aber auch die Zeit zwischen dem Abmelden und dem Stopp des eingehenden Datenverkehrs erhöhen (Leave Latency). Möglich Werte sind *2* bis *8*. Der Standardwert ist *2*.
Antwortintervall (Letztes Mitglied)	Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet. Wenn Sie den Wert verkleinern, wird schneller erkannt, ob das letzte Mitglied eine Gruppe verlassen hat und somit keine Pakete mehr für diese Gruppe an diese Schnittstelle weitergeleitet werden müssen. Möglich Werte sind *0,0* bis *25,0*. Der Standardwert ist *1,0*.
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:

Feld	Beschreibung
	• `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.

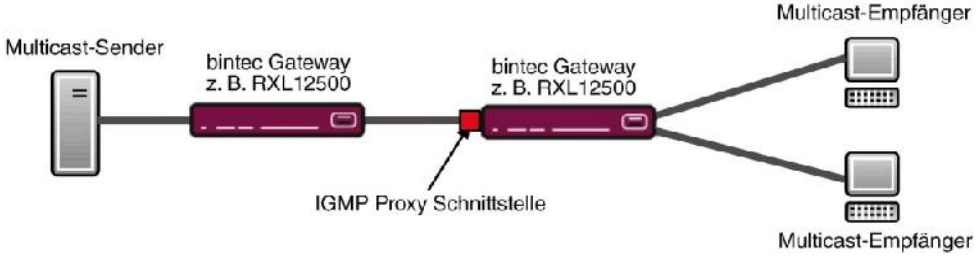


Abb. 188: IGMP Proxy

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.

21.2.2 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. 189: **Multicast->IGMP->Optionen**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
IGMP-Status	Wählen Sie den IGMP-Status aus. Mögliche Werte: • *Auto* (Standardwert): Multicast wird für Hosts automatisch eingeschaltet, wenn diese Anwendungen öffnen, die Multicast verwenden. • *Aktiv*: Multicast ist immer aktiv. • *Inaktiv*: Multicast ist immer inaktiv.
Modus	Nur für **IGMP-Status** = *Aktiv* oder *Auto* Wählen Sie den Multicast-Modus aus. Mögliche Werte: • *Kompatibilitätsmodus* (Standardwert): Der Router verwendet IGMP Version 3. Bemerkt er eine niedrigere Version im Netz, verwendet er die niedrigste Version, die er erkennen konnte. • *Nur Version 3*: Nur IGMP Version 3 wird verwendet.
Maximale Gruppen	Geben Sie ein, wie viele Gruppen sowohl intern als auch in Reports maximal möglich sein sollen.
Maximale Quellen	Geben Sie die maximale Anzahl der Quellen ein, die in den Re-

Feld	Beschreibung
	ports 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.

21.3 Weiterleiten

21.3.1 Weiterleiten

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

21.3.1.1 Neu

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

Abb. 190: **Multicast->Weiterleiten->Weiterleiten->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Alle Multicast-Gruppen	Wählen Sie aus, ob alle Multicast-Gruppen, d. h. der komplette Multicast-Adressraum 224.0.0.0/4, von der definierten **Quell-**

Feld	Beschreibung
	schnittstelle 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 22 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.

22.1 Internet + Einwählen

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

Darüber hinaus können Sie Adress-Pools für die dynamische Vergabe von IP-Adressen anlegen.

Um mit Ihrem Gerät Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner auf Ihrem Gerät einrichten. Dies gilt sowohl für ausgehende Verbindungen (z. B. Ihr Gerät wählt sich bei einem entfernten Partner ein), als auch für eingehende Verbindungen (z. B. ein entfernter Partner wählt sich bei Ihrem Gerät ein).

Wenn Sie einen Internetzugang herstellen wollen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider (ISP) einrichten. Für Breitband-Internetzugänge stellt Ihr Gerät die Protokolle PPP-over-Ethernet (PPPoE), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung. Ein Internetzugang mittels ISDN ist ebenfalls konfigurierbar.

Hinweis

Beachten Sie die Vorgaben Ihres Providers!

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

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

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

Mögliche Werte für Status

Feld	Beschreibung
	verbunden
	nicht verbunden (Wählverbindung); Verbindungsaufbau möglich

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

Standard-Route (Default Route)

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

NAT aktivieren

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

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

Timeout bei Inaktivität festlegen

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

Blockieren nach Verbindungsfehler

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

Authentifizierung

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

ren, bevor der Ruf angenommen wird.

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

Callback

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

Kanalbündelung

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

Dynamisch

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

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

Statisch

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

22.1.1 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.

22.1.1.1 Neu

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

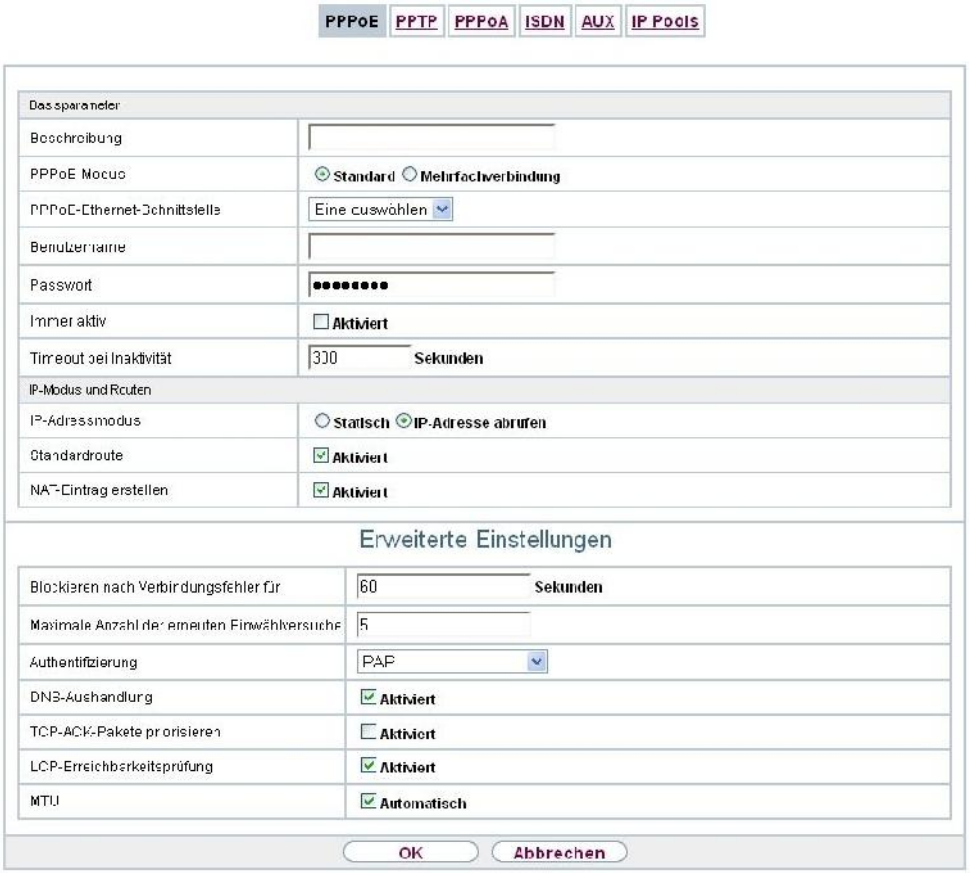


Abb. 191: **WAN**->**Internet + Einwählen**->**PPPoE**->**Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE (*Standard*) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll (*Mehrfachverbindung*). Wählen Sie *Mehrfachverbindung*, so können Sie mehrere DSL-Verbindungen eines Providers über PPP als statische Bündel koppeln, um mehr Bandbreite zu erhalten. Jede dieser DSL-Verbindungen sollte dafür eine separate Ethernet-Verbindung nutzen. Aktuell ist bei vielen Providern die Funktion PPPoE Multilink erst in Vorbereitung. Wir empfehlen Ihnen, für PPPoE Multilink den Ethernet Switch Ihres Geräts im Split-Port-Modus zu betreiben und für jede PPPoE-Verbindung eine eigene Ethernet-Schnittstelle zu benutzen, z. B. *en1-1*, *en1-2*. Wenn Sie für PPPoE Multilink zusätzlich ein externes Modem benutzen wollen, müssen Sie den Ethernet-Switch Ihres Geräts im Split-Port-Modus betreiben.
PPPoE-Ethernet-Schnittstelle	Nur für **PPPoE-Modus** = *Standard* Wählen Sie die Ethernet-Schnittstelle aus, die für eine Standard-PPPoE-Verbindung vorgegeben wird. Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist. Bei Verwendung des internen DSL-Modems, wählen Sie hier die in **WAN**->**ATM**->**Profile**->**Neu** für diese Verbindung konfigurierte EthoA-Schnittstelle aus.
PPPoE-Schnittstelle für Mehrfachlink	Nur für **PPPoE-Modus**= *Mehrfachverbindung* Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die **Hinzufügen**-

Feld	Beschreibung
	Schaltfläche, um weitere Einträge anzulegen.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
VLAN	Einige Internet Service Provider erfordern eine VLAN-ID. Aktivieren Sie diese Funktion, um unter **VLAN-ID** einen Wert eingeben zu können.
VLAN-ID	Nur wenn **VLAN** aktiviert ist. Geben Sie die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Shorthold. Standardwert ist *300*. Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.

Feld	Beschreibung
	Mögliche Werte: • *IP-Adresse abrufen* (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • *Statisch*: Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Lokale IP-Adresse	Nur bei **IP-Adressmodus** = *Statisch* Geben Sie die statische IP-Adresse des Verbindungspartners ein.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). 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 sind *0* bis *100*. Der Standardwert ist *5*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Feld	Beschreibung
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
MTU	Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die Verbindung verwendet werden darf. Mit dem Standardwert *Automatisch* wird der Wert beim Verbindungsaufbau durch das Link Control Protocol vorgegeben. Wenn Sie *Automatisch* deaktivieren, können Sie einen Wert eingeben. Mögliche Werte sind *1* bis *8192*. Standardwert ist *0*.

22.1.2 PPTP

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

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

22.1.2.1 Neu

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

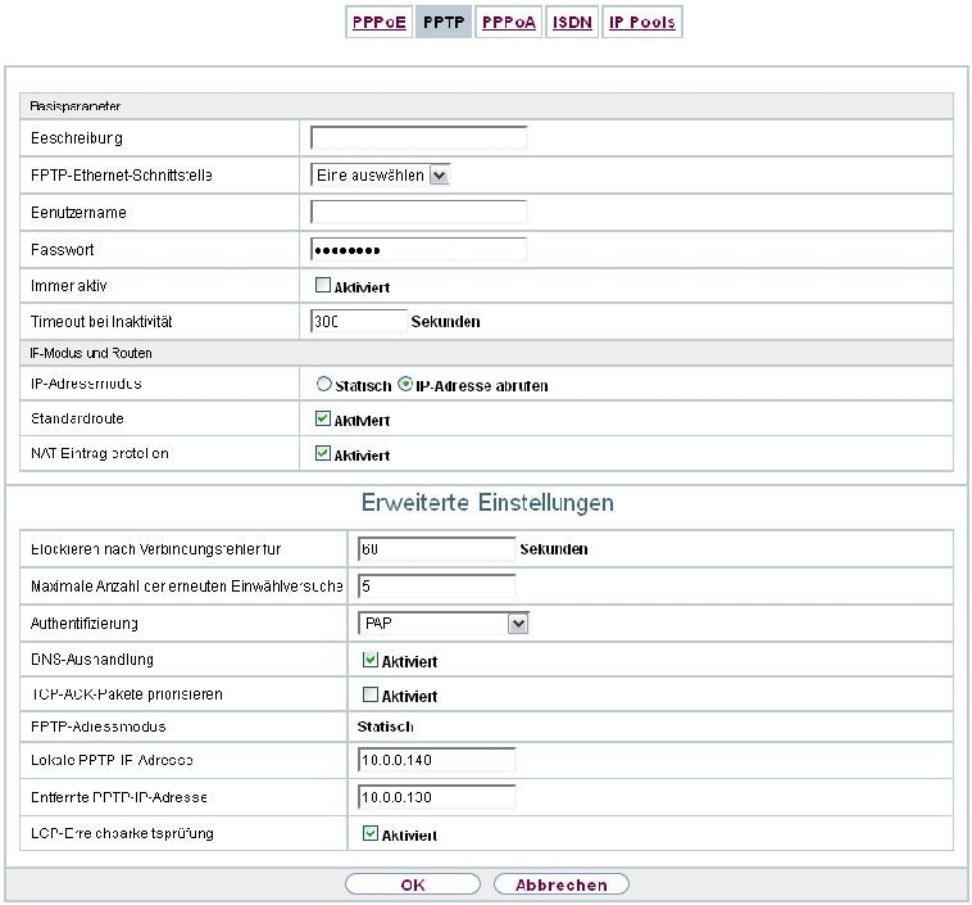


Abb. 192: **WAN->Internet + Einwählen->PPTP->Neu**

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist. Bei Verwendung des internen DSL-Modems, wählen Sie hier die in **Physikalische Schnittstellen**->**ATM**->**Profile**->**Neu** für diese Verbindung konfigurierte EthoA-Schnittstelle z. B. *ethoa50-0*, aus.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte sind *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. Der Standardwert ist *300*. Bsp. *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *IP-Adresse abrufen* (Standardwert): Ihr Gerät erhält dynamisch eine temporär gültige IP-Adresse vom Provider.

Feld	Beschreibung
	• *Statisch*: Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Lokale IP-Adresse	Nur für **IP-Adressmodus** = *Statisch* Weisen Sie der PPTP-Schnittstelle eine IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen PPTP-Partner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Standardwert ist *1*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät un-

Feld	Beschreibung
	ternommen werden soll. Standardwert ist *60*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind *0* bis *100*. Der Standardwert ist *5*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für

Feld	Beschreibung
	asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
PPTP-Adressmodus	Zeigt den Adressmodus an. Der Wert kann nicht verändert werden. Mögliche Werte: • *Statisch*: Die **Lokale PPTP-IP-Adresse** wird dem ausgewählten Ethernet-Port zugewiesen.
Lokale PPTP-IP-Adresse	Weisen Sie der PPTP-Schnittstelle eine IP-Adresse zu, die als Quelladresse verwendet wird. 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 aktiv.

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

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

werden.

22.1.3.1 Neu

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

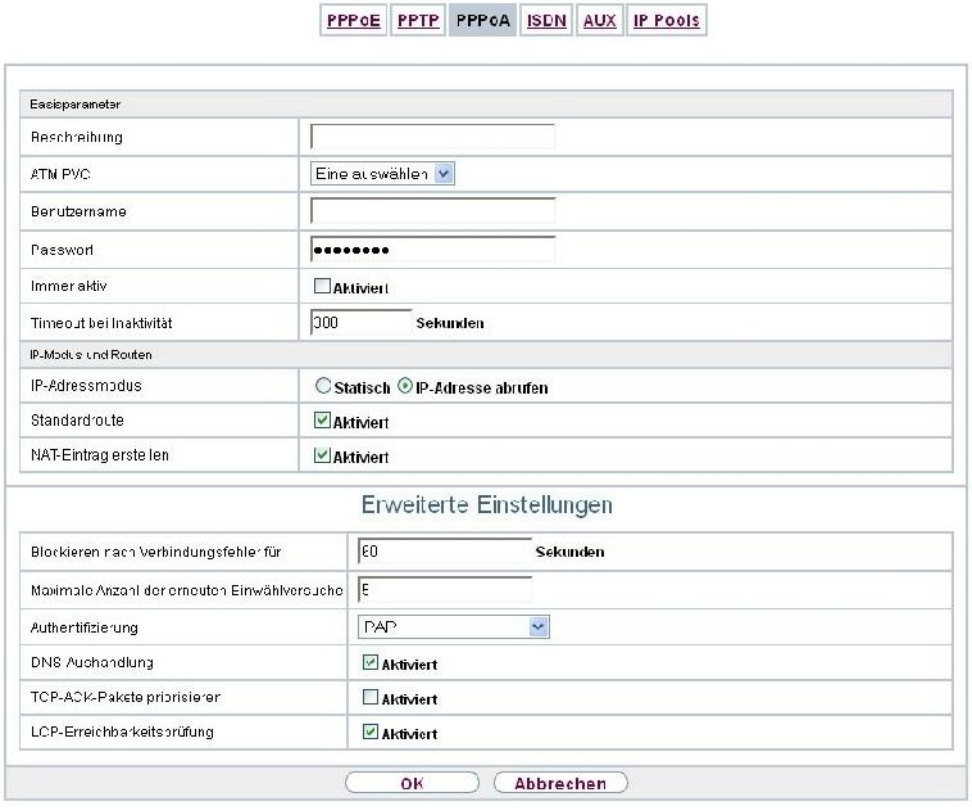


Abb. 193: **WAN->Internet + Einwählen->PPPoA->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
ATM PVC	Wählen Sie ein im Menü **ATM->Profile** angelegtes ATM-Profil, dargestellt durch die vom Provider vorgegebenen globalen ID

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

Felder im Menü IP-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. • *Statisch*: Sie geben eine statische IP-Adresse ein.
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.

Feld	Beschreibung
	Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion 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*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind *0* bis *100*.

Feld	Beschreibung
	Standardwert ist *5*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch

Feld	Beschreibung
Erreichbarkeitsprüfung	Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Diese ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

22.1.4 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) Dial-in
- Nutzung der Funktion ISDN Callback

22.1.4.1 Neu

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

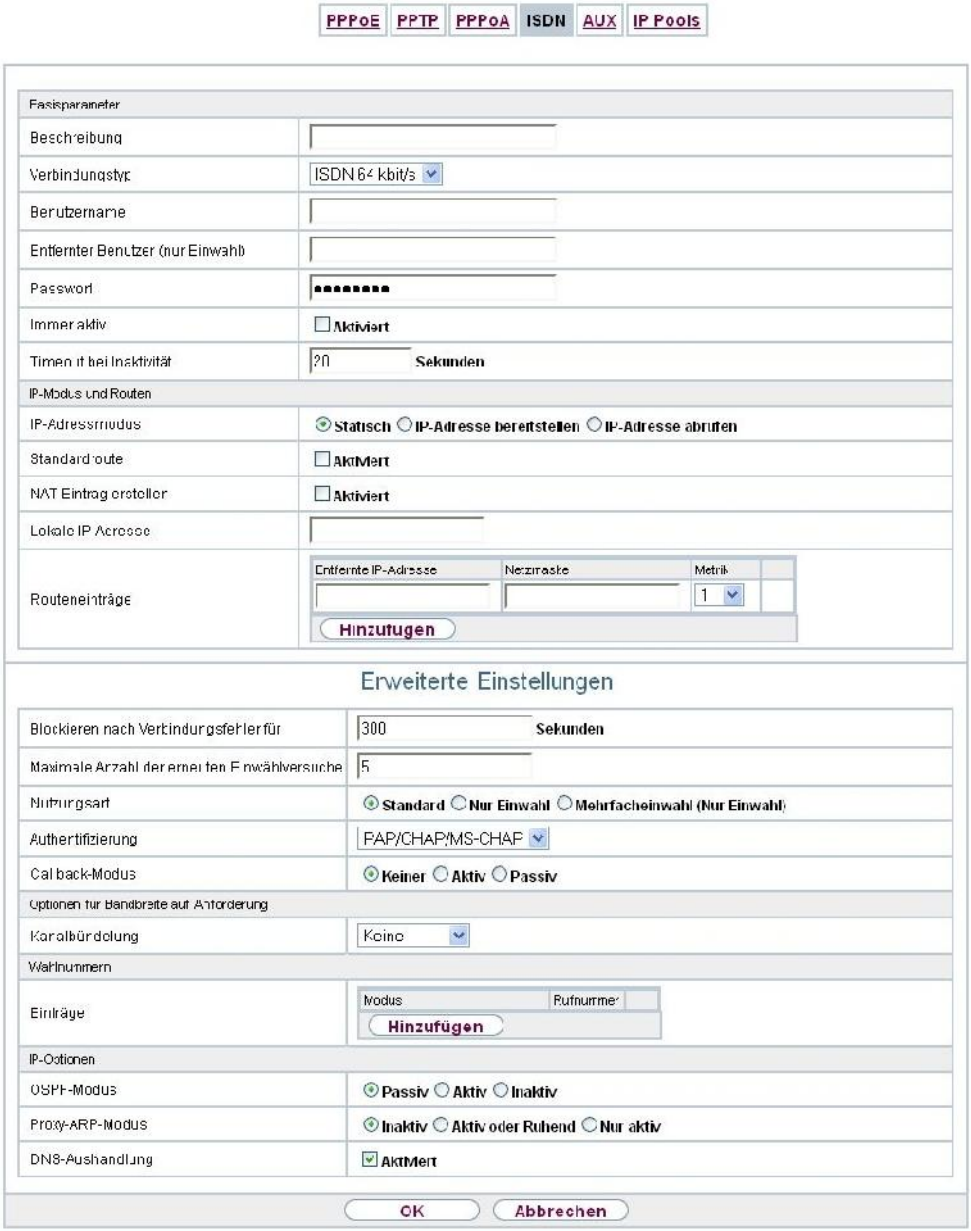


Abb. 194: **WAN->Internet + Einwählen->ISDN->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
Verbindungstyp	Wählen Sie aus, welches Layer-1-Protokoll Ihr Gerät nutzen soll. Diese Einstellung gilt für ausgehende Verbindungen zum Verbindungspartner und nur für eingehende Verbindungen vom Verbindungspartner, wenn sie anhand der Calling Party Number identifiziert werden konnten. Mögliche Werte: • *ISDN 64 kbit/s*: Für ISDN-Datenverbindungen mit 64 kbit/s • *ISDN 56 kbit/s*: Für ISDN-Datenverbindungen mit 56 kbit/s
Benutzername	Geben Sie die Kennung Ihres Geräts (lokaler PPP-Benutzername) ein.
Entfernter Benutzer (nur Einwahl)	Geben Sie die Kennung der Gegenstelle (entfernter PPP-Benutzername) ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.

Feld	Beschreibung
	Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. Standardwert ist *20*.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll. Mögliche Werte: • *Statisch* (Standardwert): Sie geben eine statische IP-Adresse ein. • *IP-Adresse bereitstellen*: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	Nur bei **IP-Adressmodus** = *Statisch* und *IP-Adresse abrufen* Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. 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

Feld	Beschreibung
	LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur bei **IP-Adressmodus** = *Statisch* Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Der Standardwert ist *1*.
IP-Zuordnungspool	Nur bei **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *300*.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind *0* bis *100*. Der Standardwert ist *5*.
Nutzungsart	Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle. Mögliche Werte:

Feld	Beschreibung
	• *Standard* (Standardwert): Kein spezieller Typ ist ausgewählt. • *Nur Einwahl*: Die Schnittstelle wird für eingehende Wählverbindungen und für von außen initiierten Callback verwendet. • *Mehrfacheinwahl (Nur Einwahl)*: Die Schnittstelle wird als Multi-User-Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen PPTP Partner aus. Mögliche Werte: • *PAP* (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *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.

Feld	Beschreibung
	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.

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 ein DFÜ-Netzwerk ist dies derzeit nicht vermeidbar.
	  • *Verzögert, nur CLID*: Ihr Gerät ruft nach ca. vier Sekunden zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert worden ist. Nur sinnvoll bei CLID.
	  • *Windows-Servermodus, Rückruf optional*: Wie

Feld	Beschreibung
	Windows-Servermodus mit Abbruchoption. Diese Einstellung ist aus Sicherheitsgründen zu vermeiden. Der Microsoft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu Ihrem Gerät ohne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer für den Verbindungspartner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit **Abbrechen** geschlossen wird.

Felder im Menü Optionen für Bandbreite auf Anforderung

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

Feld im Menü Wahlnummern

Feld	Beschreibung
Einträge	Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.

Felder im Menü Konfiguration der Wahlnummern (erscheint nur für Einträge = Hinzufügen)

Feld	Beschreibung
Modus	Nur wenn **Einträge** = *Hinzufügen* Die Calling Party Number des Rufes wird mit der unter **Rufnummer** eingetragenen Nummer verglichen. Wählen Sie aus, ob **Rufnummer** für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte: • *Beide* (Standardwert): Für eingehende und ausgehende Rufe. • *Eingehend*: Für eingehende Rufe, wenn der Verbindungspartner sich bei Ihrem Gerät einwählen soll. • *Ausgehend*: Für ausgehende Rufe, wenn Sie sich beim Verbindungspartner einwählen wollen. Die Nummer des Anrufers eines eingehenden Rufs (Calling Party Number) wird mit der unter **Rufnummer** eingetragenen Nummer verglichen.
Rufnummer	Geben Sie die Rufnummern des Verbindungspartners ein.
Anzahl Verwendeter Ports	Wählen Sie aus, welcher Port zu verwenden ist.

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellen Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert. • *Aktiv*: OSPF ist für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob und wie ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner

Feld	Beschreibung
	beantwortet werden. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner *aktiv* oder *Ruhend* ist. Bei *Ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner *aktiv* ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** und **WINS-Server Primär** und **Sekundär** vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

22.1.5 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 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 Stun-

de wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

22.1.5.1 Bearbeiten oder Neu

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

Abb. 195: **WAN->Internet + Einwählen->IP Pools->Neu**

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

22.2 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.

22.2.1 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*).

22.2.1.1 Neu

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

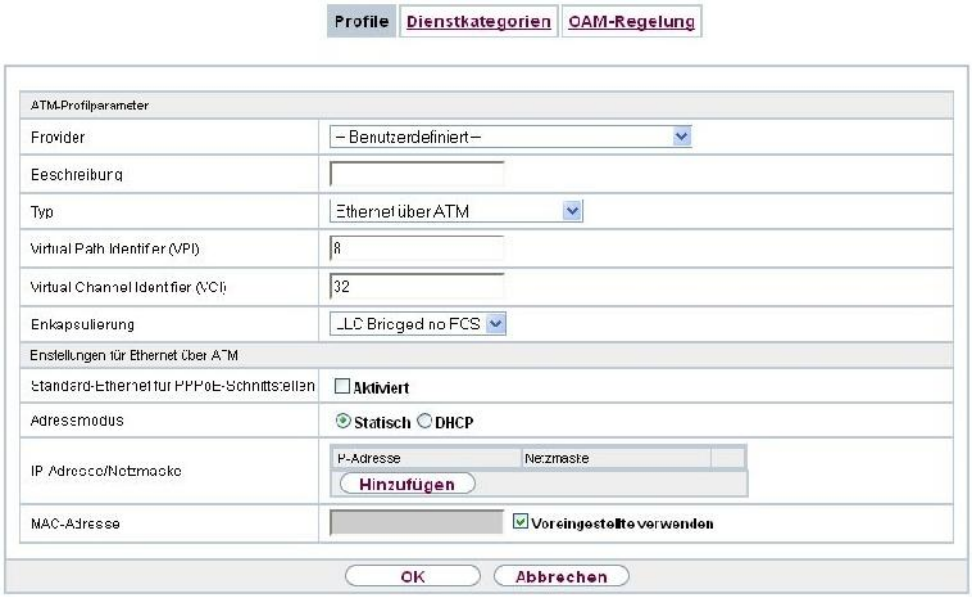


Abb. 196: **WAN->ATM->Profile->Neu**

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

Felder im Menü ATM-Profilparameter

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

Feld	Beschreibung
ATM-Schnittstelle	Nur, wenn mehrere ATM-Schnittstellen verfügbar sind, z. B. wenn bei Geräten mit SHDSL mehrere Schnittstellen separat konfiguriert sind. Wählen Sie die ATM-Schnittstelle, die Sie für die Verbindung verwenden wollen.
Typ	Nur für **Provider** = *-- Benutzerdefiniert --* Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte: • *Ethernet über ATM* (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet. • *Geroutete Protokolle über ATM*: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) werden geroutete Protokolle über ATM (RPoA) verwendet. • *PPP über ATM*: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.
Virtual Path Identifier (VPI)	Nur für **Provider** = *-- Benutzerdefiniert --* Geben Sie den VPI-Wert der ATM-Verbindung ein. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind *0* bis *255*. Der Standardwert ist *8*.
Virtual Channel Identifier (VCI)	Nur für **Provider** = *-- Benutzerdefiniert --* Geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind *32* bis *65535*. Der Standardwert ist 32.

Feld	Beschreibung
Enkapsulierung	Nur für **Provider** = *-- Benutzerdefiniert --* Wählen Sie die zu verwendende Enkapsulierung aus. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte (nach RFC 2684): • *LLC Bridged no FCS* (Standardwert für Ethernet über ATM): Wird nur für **Typ** = *Ethernet über ATM* angezeigt. Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen). • *LLC Bridged FCS*: Wird nur für **Typ** = *Ethernet über ATM* angezeigt. Bridged Ethernet mit LLC/SNAP-Enkapsulierung mit Frame Check Sequence (Prüfsummen). • *Nicht ISO* (Standardwert für Geroutete Protokolle über ATM): Wird nur für **Typ** = *Geroutete Protokolle über ATM* angezeigt. Enkapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing. • *LLC*: Wird nur für **Typ** = *PPP über ATM* angezeigt. Enkapsulierung mit LLC-Header. • *VC-Multiplexing* (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Enkapsulierung (Null Einkapselung) mit Frame Check Sequence (Prüfsummen).

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

Feld	Beschreibung
Standard-Ethernet für PPPoE-Schnittstellen	Nur für **Typ** = *Ethernet über ATM* Wählen Sie aus, ob diese Ethernet-over-ATM-Schnittstelle für alle PPPoE-Verbindungen verwendet werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Adressmodus	Nur für **Typ** = *Ethernet über ATM*

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

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

Feld	Beschreibung
IP-Adresse/Netzmaske	Geben Sie die IP-Adressen (**IP-Adresse**) und die entsprechenden Netzmasken (**Netzmaske**) der ATM-Schnittstelle ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

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

Feld	Beschreibung
Client-Typ	Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll. Mögliche Werte: • *Auf Anforderung* (Standardwert): Die PPPoA wird nur bei Bedarf aufgebaut, z. B. für den Internetzugang. Zusätzliche Informationen zu PPP über ATM finden Sie unter *PPPoA* auf Seite 465.

22.2.2 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 elmeg-Geräte. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.

22.2.2.1 Neu

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

Abb. 197: **WAN->ATM->Dienstkategorien->Neu**

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

Felder im Menü Basisparameter

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

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

Feld	Beschreibung
(MBS)	*(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*.

22.2.3 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 elmeg-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.

22.2.3.1 Neu

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

Abb. 198: **WAN->ATM->OAM-Regelung->Neu**

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

Felder im Menü OAM-Flusskonfiguration

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

Felder im Menü Loopback

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

Feld	Beschreibung
	Geben Sie ein, wie viele direkt aufeinanderfolgende Loopback-Zellen ausbleiben dürfen, bevor die Verbindung als unterbrochen ("inaktiv") angesehen wird. Mögliche Werte sind *1* bis *99*. Der Standardwert ist *5*.

Felder im Menü CC-Aktivierung

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

Feld	Beschreibung
	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.

22.3 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.

22.3.1 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.

22.3.1.1 Neu

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

Abb. 199: **WAN->Real Time Jitter Control->Regulierte Schnittstellen->Neu**

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

Felder im Menü Grundeinstellungen

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

Kapitel 23 VPN

Als VPN (Virtual Private Network) wird eine Verbindung bezeichnet, die das Internet als "Transportmedium" nutzt, aber nicht öffentlich zugänglich ist. Nur berechtigte Benutzer haben Zugang zu einem solchen VPN, das anschaulich auch als VPN-Tunnel bezeichnet wird. Üblicherweise werden die über ein VPN transportierten Daten verschlüsselt.

Über ein VPN kann z. B. ein Außendienstmitarbeiter oder ein Mitarbeiter im Home Office auf die Daten im Firmennetz zugreifen. Filialen können ebenfalls über VPN an die Zentrale angebunden werden.

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

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

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

23.1 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 129) integriert werden. Die IPSec-Implementierung erreicht dieses Ziel zum einen durch die Benutzung des Authentication-Header-(AH)-Protokolls und des Encapsulated-Security-Payload-(ESP)-Protokolls. Zum anderen werden kryptografische Schlüsselverwaltungsmechanismen wie das Internet-Key-Exchange-(IKE)-Protokoll verwendet.

Zusätzlicher Filter des Datenverkehrs

bintec elmeg Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IP-Sec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des Datenverkehrs**, so wird es verworfen.

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

Hinweis

Der Parameter **Zusätzlicher Filter des Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.

Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

23.1.1 IPSec-Peers

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

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

zeigt.

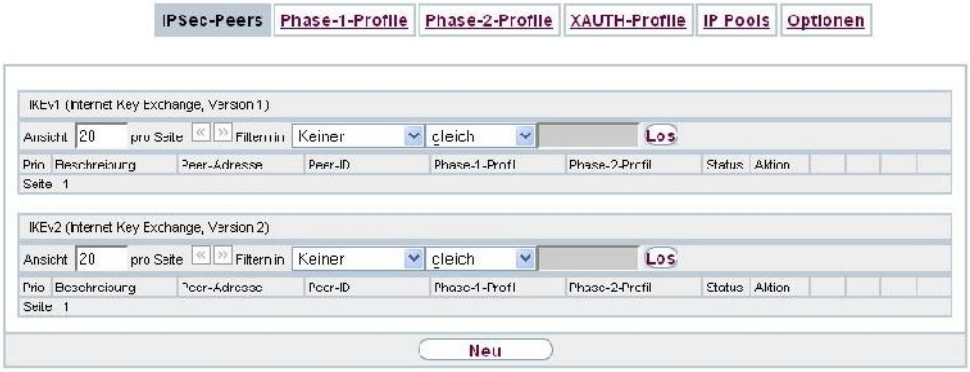


Abb. 200: **VPN**->**IPSec**->**IPSec-Peers**

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 680.

23.1.1.1 Neu

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

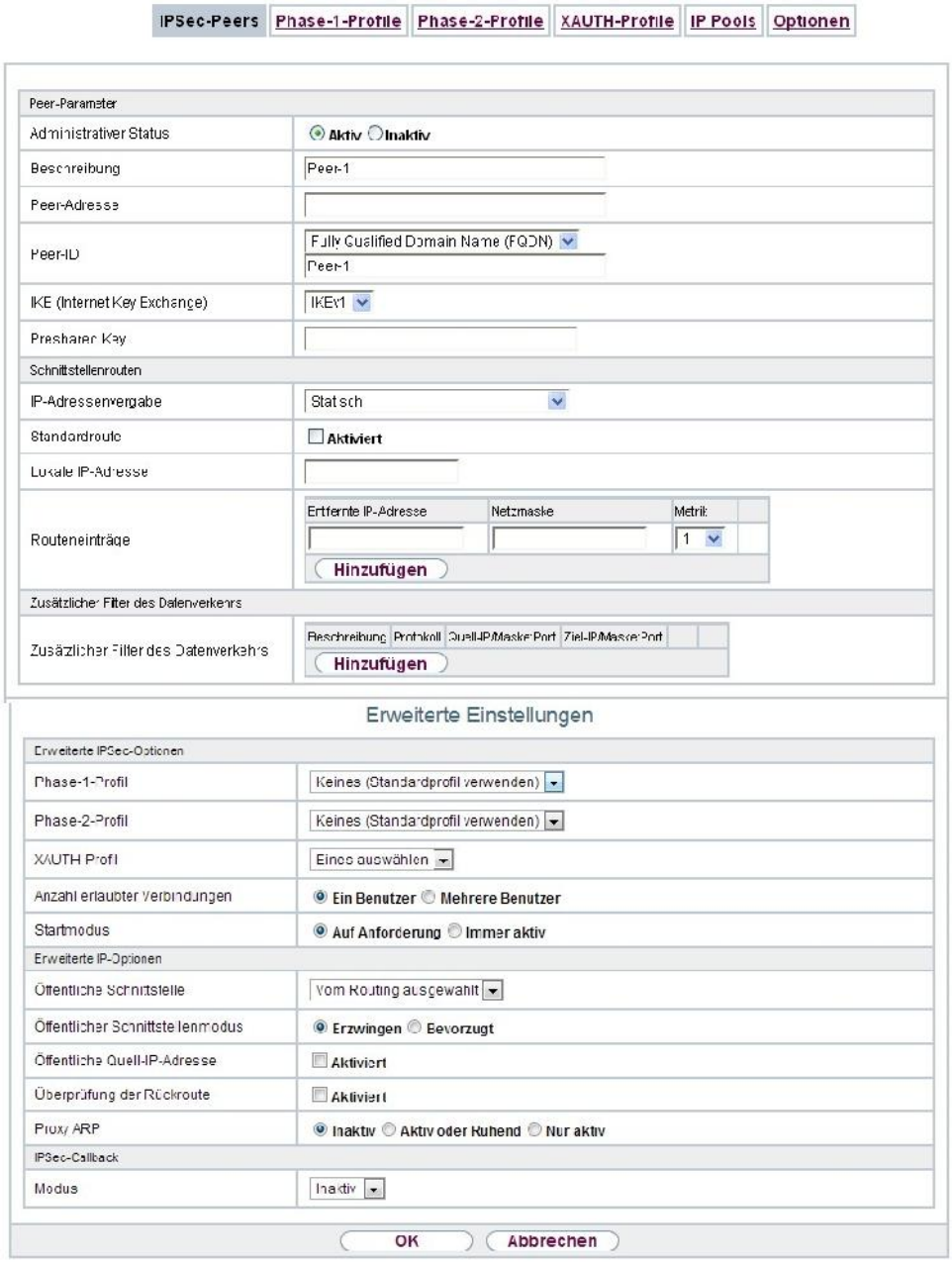


Abb. 201: **VPN**->**IPSec**->**IPSec-Peers**->**Neu**

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

Felder im Menü Peer-Parameter

Feld	Beschreibung
Administrativer Status	Wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Peer-Konfiguration versetzen wollen. Mögliche Werte: • *Aktiv* (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. • *Inaktiv*: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.
Beschreibung	Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Peer-Adresse	Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein. Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.
Peer-ID	Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein. Die Eingabe kann in bestimmten Konfigurationen entfallen. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen. Mögliche ID-Typen: • *Fully Qualified Domain Name (FQDN)*: Beliebige Zeichenkette • *E-Mail-Adresse* • *IPV4-Adresse* • *ASN.1-DN (Distinguished Name)* • *Schlüssel-ID*: Beliebige Zeichenkette Auf dem Peer-Gerät entspricht diese ID dem Parameter **Lokaler ID-Wert**.
IKE (Internet Key Exchange)	Für Geräte der **WIxxxxn**-Serie nicht verfügbar. Diese Geräte unterstützen nur IKEv1.

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

Feld	Beschreibung
	aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet. Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe *Zertifikate* auf Seite 129), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.
Preshared Key	Geben Sie das mit dem Peer vereinbarte Passwort ein. Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer `0x` am Anfang des Eintrags.

Felder im Menü Schnittstellenrouten

Feld	Beschreibung
IP-Adressenvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: • `Statisch` (Standardwert): Geben Sie eine statische IP-Adresse ein. • `Client im IKE-Konfigurationsmodus`: Nur für IKEv1 auswählbar. Wählen Sie diese Option, wenn Ihr Gateway als IPSec-Client vom Server eine IP-Adresse erhalten soll. • `Server im IKE-Konfigurationsmodus`: Wählen Sie diese Option, wenn Ihr Gateway als Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten **IP-Zuordnungspool** entnommen.
Konfigurationsmodus	Nur bei **IP-Adressenvergabe** = `Server im IKE-Konfigurationsmodus` oder `Client im IKE-Konfigurationsmodus` Mögliche Werte: • `Pull` (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage. • `Push`: Das Gateway schlägt dem Client eine IP-Adresse vor und der Client muss diese akzeptieren oder zurückweisen.

Feld	Beschreibung
	Dieser Wert muss für beide Seiten des Tunnels identisch sein.
IP-Zuordnungspool	Nur bei **IP-Adressenvergabe** = *Server im IKE-Konfigurationsmodus* Wählen Sie einen im Menü **VPN**->**IPSec**->**IP Pools** konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung *Noch nicht definiert*.
Standardroute	Nur für **IP-Adressenvergabe** = *Statisch* oder *Client im IKE-Konfigurationsmodus* Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur für **IP-Adressenvergabe** = *Statisch* oder *Server im IKE-Konfigurationsmodus* Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.
Metrik	Nur für **IP-Adressenvergabe** = *Statisch* oder *Client im IKE-Konfigurationsmodus* und **Standardroute** = *Aktiviert* Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von *0* bis *15*. Standardwert ist *1*.
Routeneinträge	Nur für **IP-Adressenvergabe** = *Statisch* oder *Client im IKE-Konfigurationsmodus* Definieren Sie Routing-Einträge für diesen Verbindungspartner. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -LANs.

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

Felder im Menü Zusätzlicher Filter des Datenverkehrs

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

Zusätzlicher Filter des Datenverkehrs

bintec elmeg Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IPSec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des Datenverkehrs**, so wird es verworfen.

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

Hinweis

Der Parameter **Zusätzlicher Filter des Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.

Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

Fügen Sie weitere Filter mit **Hinzufügen** hinzu.

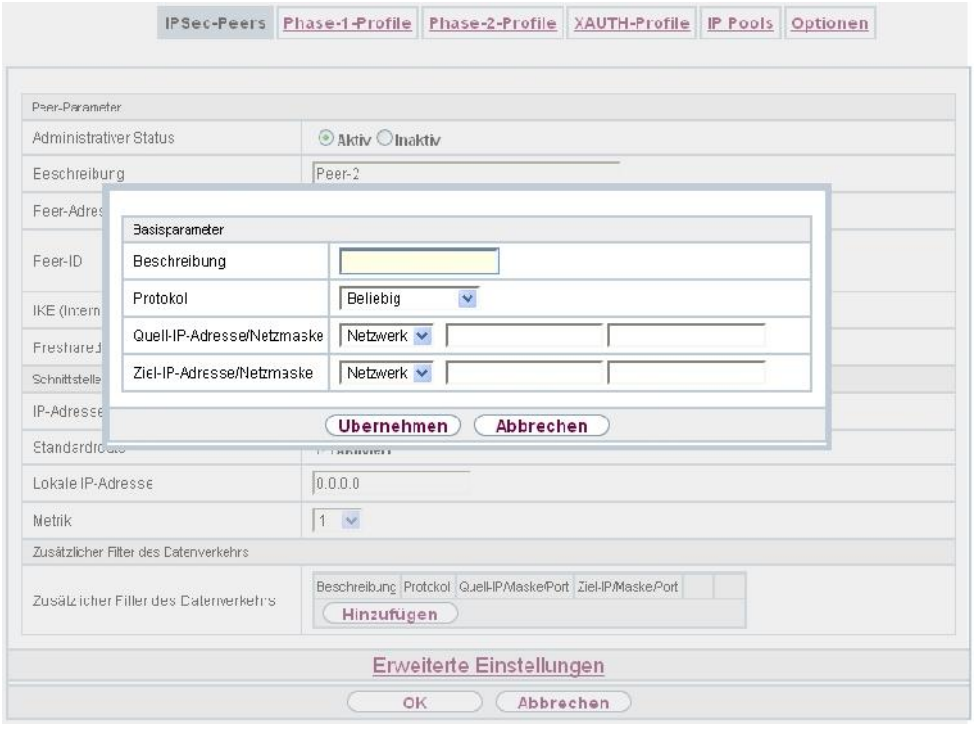


Abb. 202: **VPN->IPSec->IPSec-Peers->Neu->Hinzufügen**

Felder im Menü Basisparameter

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

Feld	Beschreibung
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: • *Beliebig* • *Host*: Geben Sie die IP-Adresse des Hosts ein. • *Netzwerk* (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie den Quell-Port der Datenpakete ein. Die Standardeinstellung *-Alle-* (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und die zugehörige Netzmaske der Datenpakete ein.
Ziel-Port	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie den Ziel-Port der Datenpakete ein. Die Standardeinstellung *-Alle-* (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.

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

Felder im Menü Erweiterte IPSec-Optionen

Feld	Beschreibung
Phase-1-Profil	Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: • *Keines (Standardprofil verwenden)*: Verwendet das Profil, das in **VPN**->**IPSec**->**Phase-1-Profile** als Standard markiert ist • *Multi-Proposal*: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/

Feld	Beschreibung
	MD5 enthält ungeachtet der Proposalauswahl im Menü **VPN**->**IPSec**->**Phase-1-Profile**. • *<Profilname>*: Verwendet ein Profil, das im Menü **VPN**->**IPSec**->**Phase-1-Profile** für Phase 1 konfiguriert wurde.
Phase-2-Profil	Wählen Sie ein Profil für die Phase 2 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: • *Keines (Standardprofil verwenden)*: Verwendet das Profil, das in **VPN**->**IPSec**->**Phase-2-Profile** als Standard markiert ist • **Multi-Proposal*: Verwendet ein spezielles Profil, das für Phase 2 die Proposals 3DES/MD5, AES-128/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü **VPN**->**IPSec**->**Phase-2-Profile**. • *<Profilname>*: Verwendet ein Profil, das im Menü **VPN**->**IPSec**->**Phase-2-Profile** für Phase 2 konfiguriert wurde.
XAUTH-Profil	Wählen Sie ein in **VPN**->**IPSec**->**XAUTH-Profile** angelegtes Profil aus, wenn Sie zur Authentifizierung dieses IPSec-Peers XAuth verwenden möchten. Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.
Anzahl erlaubter Verbindungen	Wählen Sie aus, wieviele Benutzer sich mit diesem Peer-Profil verbinden dürfen. Mögliche Werte: • *Ein Benutzer* (Standardwert): Es kann sich nur ein Peer mit den in diesem Profil definierten Daten verbinden. • *Mehrere Benutzer*: Es können sich mehrere Peers mit den in diesem Profil definierten Daten verbinden. Bei jeder Verbindungsanfrage mit den in diesem Profil definierten Daten, wird der Peer-Eintrag dupliziert. Die Konfiguration des dynamischen Peers darf keine Peer ID und keine Peer-IP-Adresse enthalten. Die CLients, die sich mit dem Gateway verbinden, müssen jedoch über eine Peer

Feld	Beschreibung
	ID verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen. Der resultierende Peer auf dem Gateway würde nun auf alle eingehenden Tunnel-Requests zutreffen. Daher ist es notwendig, ihn an das Ende der IPSec-Peer-Liste zu stellen. Andernfalls wären alle in der Listen folgenden Peers inaktiv.
Startmodus	Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt werden soll. Mögliche Werte: • *Auf Anforderung* (Standardwert): Der Peer wird durch einen Trigger in den aktiven Zustand versetzt. • *Immer aktiv*: Der Peer ist immer aktiv.

Felder im Menü Erweiterte IP-Optionen

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

Feld	Beschreibung
	aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll. Standardmäßig ist die Funktion nicht aktiv.
Überprüfung der Rückroute	Wählen Sie aus, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
MobIKE	Nur für Peers mit IKEv2. **MobIKE** ermöglicht es, bei wechselnden öffentlichen IP-Adressen lediglich diese Adressen in den SAs zu aktualisieren, ohne die SAs selbst neu aushandeln zu müssen. Standardmäßig ist die Funktion aktiv. Beachten Sie, dass MobIKE einen aktuellen IPSec Client voraussetzt, z. B. den aktuellen Windows-7- oder Windows-8-Client oder die neuste Version des bintec elmeg IPSec Clients.
Proxy ARP	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll. Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer *aktiv* (aktiv) oder *Ruhend* (ruhend) ist. Bei *Ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer

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

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen bintec elmeg-Geräte den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit IPSec-Callback geschaffen: Mithilfe eines direkten ISDN-Rufs bei einem Peer kann diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf von Ihrem Gerät nicht angenommen werden muss. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muss zunächst auf der passiven Seite im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration**->**Neu** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld **Dienst** der Wert *IPSec* zur Verfügung. Dieser Eintrag sorgt dafür, dass auf dieser Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Bei aktivem Callback wird, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlasst, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer (**MSN** im Menü **Physikalische Schnittstellen**->**ISDN-Ports**->**MSN-Konfiguration**->**Neu** für **Dienst** *IPSec*) eingeht. Auf diese Weise wird sichergestellt, dass beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt, wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.

Hinweis

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec-Daemon zunächst die Schnittstelle aktiviert, über die der Tunnel realisiert werden soll. Sofern auf dem lokalen Gerät IPSec mit DynDNS konfiguriert ist, wird die eigene IP-Adresse propagiert und erst dann der ISDN-Ruf an das entfernte Gerät abgesetzt. Auf diese Art ist sichergestellt, dass das entfernte Gerät das lokale auch tatsächlich erreichen kann, wenn es den Tunnelaufbau initiiert.

Übermittlung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Geräts über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs. Einschränkungen, die bei der IPSec-Konfiguration mit dynamischen IP-Adressen auftreten, können so umgangen werden.

Hinweis

Um die Funktion IP-Adressübermittlung über ISDN nutzen zu können, müssen Sie eine kostenfreie Zusatzlizenz erwerben.

Die Lizenzdaten der Zusatzlizenzen erhalten Sie über die Online-Lizenzierungs-Seiten im Support-Bereich auf *www.bintec-elmeg.com* . Bitte folgen Sie den Anweisungen der Online-Lizenzierung.

Vor Systemsoftware Release 7.1.4 unterstützte der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Auslösers auf indirektem Wege (z. B. über DynDNS) ermittelt werden konnte. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse über ISDN umgangen. Darüber hinaus ermöglicht es diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus (Haupt Modus) für den Tunnelaufbau zu verwenden.

Funktionsweise: Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht. Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in *Felder im Menü IPSec-Callback* auf Seite 512 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der

automatischen Auswahl durch das Gerät sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.

Hinweis

Damit Ihr Gerät die Informationen des gerufenen Peers über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Geräten analog vorgenommen werden.

Folgende Rollenverteilungen sind möglich:

- Eine Seite übernimmt die aktive, die andere die passive Rolle.
- Beide Seiten können beide Rollen (Beide) übernehmen.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

(1) Peer A (der Auslöser des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.

(2) Ihr Gerät erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden MIB-Eintrag.

(3) Ihr Gerät setzt den initialen ISDN-Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.

(4) Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten Calling Party Number (der ISDN-Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.

(5) Der IPSec-Daemon auf Ihrem Gerät von Peer B kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil des Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.

(6) Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.

Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Die folgenden Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü IPSec-Callback

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

Feld	Beschreibung
	das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.
Eigene IP-Adresse per ISDN/GSM übertragen	Wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Geräts über ISDN übertragen werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Übertragungsmodus	Nur für **Eigene IP-Adresse per ISDN/GSM übertragen** = aktiviert Wählen Sie aus, in welchem Modus Ihr Gerät versuchen soll, seine IP-Adresse an den Peer zu übertragen. Mögliche Werte: • *Automatische Erkennung des besten Modus*: Ihr Gerät bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird. (Die Verwendung des B-Kanals verursacht Kosten.) • *Nur D-Kanalmodi automatisch erkennen*: Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. • *Spezifischen D-Kanalmodus verwenden*: Ihr Gerät versucht, die IP-Adresse in dem im Feld **Modus** eingestellten Modus zu übertragen. • *Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen*: Ihr Gerät versucht, die IP-Adresse in dem im Feld **Modus** eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übetragen. (Dies verursacht Kosten.) • *Nur B-Kanalmodus verwenden*: Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.
Modus des D-Kanals	Nur für **Übertragungsmodus** = *Spezifischen D-Kanalmodus verwenden* oder *Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen* Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen.

Feld	Beschreibung
	Mögliche Werte: • *LLC* (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen. • *SUBADDR*: Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen. • *LLC und SUBADDR*: Die IP-Adresse wird sowohl in den "LLC-" als auch in den "Subaddress Information Elements" übertragen.

23.1.2 Phase-1-Profile

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

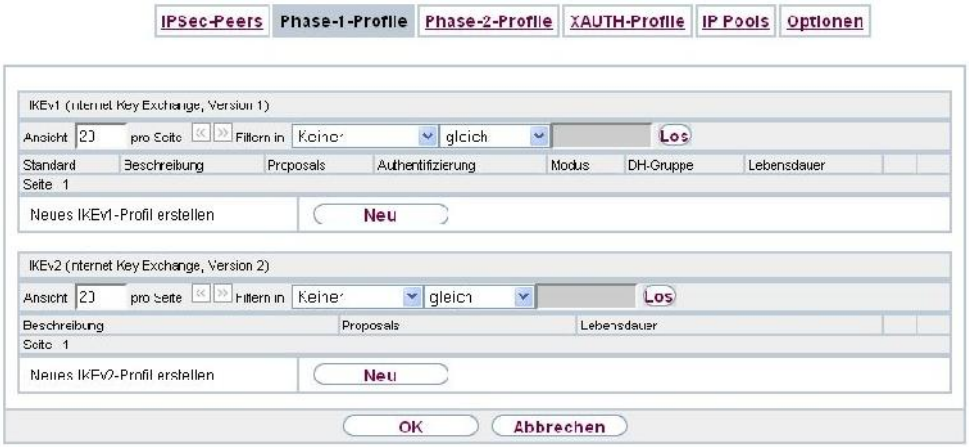


Abb. 203: **VPN**->**IPSec**->**Phase-1-Profile**

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

23.1.2.1 Neu

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

Abb. 204: **VPN**->**IPSec**->**Phase-1-Profile**->**Neu**

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

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

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

Feld	Beschreibung
	was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • *Twofish*: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • *Blowfish*: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • *CAST*: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • *DES*: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. • *AES*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter *AES* gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • *AES-128*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • *AES-192*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • *AES-256*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. Hash-Algorithmen (**Authentifizierung**): • *MD5* (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.

Feld	Beschreibung
	• *SHA1*: SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. • *RipeMD 160*: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt. • *Tiger192*: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus. Beachten Sie, dass die Beschreibung der Verschlüsselung und Authentifizierung oder der Hash-Algorithmen auf dem Kenntnisstand und der Meinung des Autors zum Zeitpunkt der Erstellung dieses Handbuchs basiert. Die Qualität der Algorithmen im besonderen unterliegt relativen Gesichtpunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.
DH-Gruppe	Nur für **Phase-1-Parameter (IKE)** Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec elmeg-Geräten unterstützt wird, steht für "modular exponentiation". Mögliche Werte: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *5 (1536 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	Legen Sie die Lebensdauer für Phase-1-Schlüssel fest. Folgende Optionen stehen für die Definition der **Lebensdauer**

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

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

Feld	Beschreibung
	Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet. Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe *Zertifikate* auf Seite 129), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.

Erreichbarkeitsprüfung

In der Kommunikation zweier IPSec-Peers kann es dazu kommen, dass einer der beiden z. B. aufgrund von Routing-Problemen oder aufgrund eines Neustarts nicht erreichbar ist. Dies ist aber erst dann feststellbar, wenn das Ende der Lebensdauer der Sicherheitsverbindung erreicht ist. Bis zu diesem Zeitpunkt gehen die Datenpakete verloren. Um dies zu verhindern, gibt es verschiedene Mechanismen einer Erreichbarkeitsprüfung. Im Feld **Erreichbarkeitsprüfung** wählen Sie aus, ob ein Mechanismus angewendet werden soll, um die Erreichbarkeit eines Peers zu überprüfen.

Hierbei stehen zwei Mechanismen zur Verfügung: Heartbeats und Dead Peer Detection.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Erreichbarkeitsprüfung	Nur für **Phase-1-Parameter (IKE)** Wählen Sie die Methode aus, mit der die Funktionalität der IPSec-Verbindung überprüft werden soll. Neben dem Standardverfahren Dead Peer Detection (DPD) ist auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird Mögliche Werte: • *Automatische Erkennung* (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • *Inaktiv*: Ihr Gerät sendet und erwartet keinen Heartbeat.

Feld	Beschreibung
	Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • *Heartbeats (Nur erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • *Heartbeats (Nur senden)*: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • *Heartbeats (Senden &Erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • *Dead Peer Detection*: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Erreichbarkeit des Peers nur überprüft, wenn tatsächlich Daten an ihn gesendet werden sollen. • *Dead Peer Detection (Idle)*: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vorgenommen. Nur für **Phase-1-Parameter (IKEv2)** Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung. Standardmäßig ist die Funktion aktiv.
Blockzeit	Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche. Zur Verfügung stehen Werte von *-1* bis *86400* (Sekunden), der Wert *-1* bedeutet die Übernahme des Wertes im Standardprofil, der Wert *0*, dass der Peer in keinem Fall blockiert wird. Standardwert ist *30*.
NAT-Traversal	NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.

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

23.1.3 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.

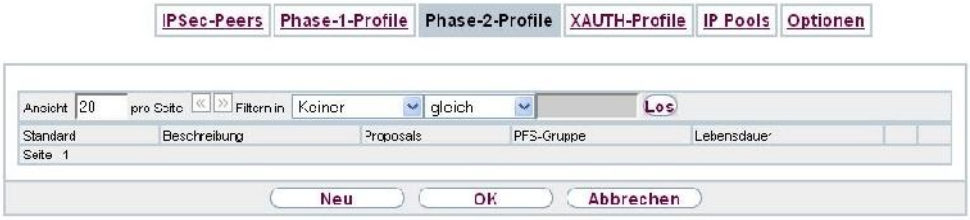


Abb. 205: **VPN**->**IPSec**->**Phase-2-Profile**

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

23.1.3.1 Neu

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

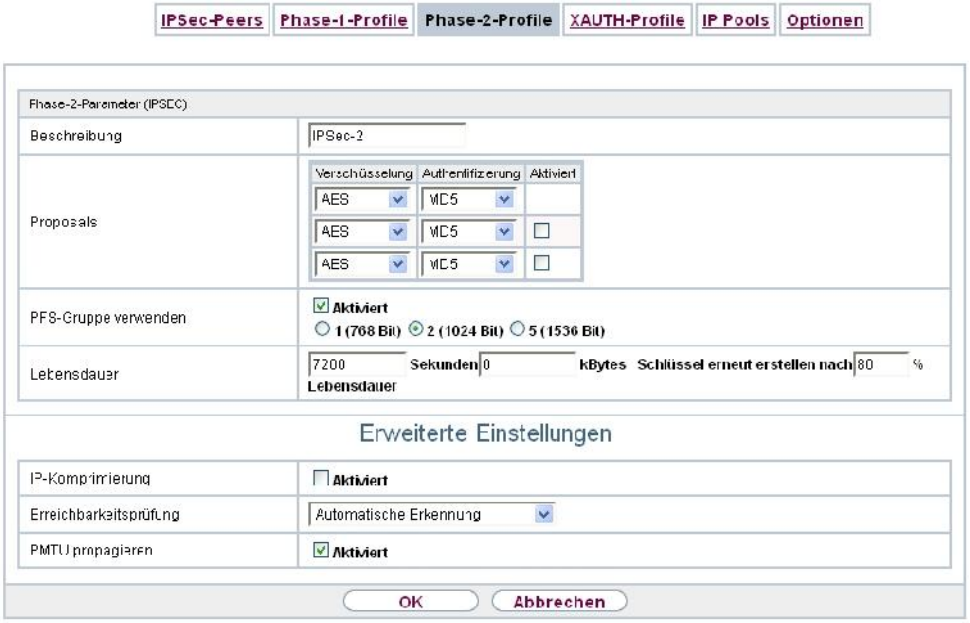


Abb. 206: **VPN**->**IPSec**->**Phase-2-Profile**->**Neu**

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

Felder im Menü Phase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.

Feld	Beschreibung
	Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Proposals	In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld. Verschlüsselungsalgorithmen (**Verschlüsselung**): • *3DES* (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • *-- ALLE --*: Alle Optionen können verwendet werden. • *AES*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter *AES* gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • *AES-128*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • *AES-192*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • *AES-256*: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. • *Twofish*: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • *Blowfish*: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish an-

Feld	Beschreibung
	gesehen werden. • *CAST*: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • *DES*: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. Hash-Algorithmen (**Authentifizierung**): • *MD5* (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • *-- ALLE --*: Alle Optionen können verwendet werden. • *SHA1*: SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.
PFS-Gruppe verwenden	Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (*Aktiviert*), sind die Optionen die gleichen, wie bei der Konfiguration von **DH-Gruppe** im Menü **VPN**->**IPSec**->**Phase-1-Profile** . PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind. Das Feld hat folgende Optionen: • *1 (768 Bit)*: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • *2 (1024 Bit)* (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.

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

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	nicht komprimierbaren Daten wird von der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Erreichbarkeitsprüfung	Wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden. Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, ist ein bintec elmeg IPSec-Heartbeat implementiert worden. Dieser sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen werden sollen. Mögliche Werte: • *Automatische Erkennung* (Standardwert): Automatische Erkennung, ob die Gegenstelle ein bintec elmeg-Gerät ist. Wenn ja, wird *Heartbeats (Senden &Erwarten)* (bei Gegenstelle mit bintec elmeg) oder *Inaktiv* (bei Gegenstelle ohne bintec elmeg) gesetzt. • *Inaktiv*: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • *Heartbeats (Nur erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • *Heartbeats (Nur senden)*: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • *Heartbeats (Senden &Erwarten)*: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.
PMTU propagieren	Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

23.1.4 XAUTH-Profile

Im Menü **XAUTH-Profile** wird eine Liste aller XAuth-Profile angezeigt.

Extended Authentication für IPSec (XAuth) ist eine zusätzliche Authentifizierungsmethode für Benutzer eines IPSec-Tunnels.

Das Gateway kann bei Nutzung von XAuth zwei verschiedene Rollen übernehmen, es kann als Server oder als Client dienen:

- Das Gateway fordert als Server einen Berechtigungsnachweis an.
- Das Gateway weist als Client seine Berechtigung nach.

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Die Berechtigung wird entweder anhand einer Liste oder über einen RADIUS Server geprüft. Bei Verwendung eines Einmalpassworts (One Time Password, OTP) kann die Passwortüberprüfung von einem Token-Server übernommen werden (z. B. beim Produkt SecOVID von Kobil), der hinter dem RADIUS-Server installiert ist. Wenn über IPSec eine Firmenzentrale mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden. Je nach Zuordnung verschiedener Profile kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechselnd in verschiedenen Filialen arbeitet, jeder Peer eine Filiale repräsentiert und der Angestellte jeweils vor Ort Zugriff auf den Tunnel haben will.

Nachdem IPSec IKE (Phase 1) erfolgreich beendet ist und bevor IKE (Phase 2) beginnt, wird XAuth realisiert.

Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.

23.1.4.1 Neu

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

Abb. 207: **VPN**->**IPSec**->**XAUTH-Profile**->**Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für dieses XAuth-Profil ein.
Rolle	Wählen Sie die Rolle des Gateways bei der XAuth-Authentifizierung aus. Mögliche Werte: • *Server* (Standardwert): Das Gateway fordert einen Berechtigungsnachweis an. • *Client*: Das Gateway weist seine Berechtigung nach.
Modus	Nur für **Rolle** = *Server* Wählen Sie aus, wie die Authentifizierung durchgeführt wird. Mögliche Werte: • *RADIUS* (Standardwert): Die Authentifizierung wird über einen RADIUS-Server durchgeführt. Dieser wird im Menü **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS** konfiguriert und im Feld **RADIUS-Server Gruppen-ID** ausgewählt. • *Lokal*: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.
Name	Nur für **Rolle** = *Client* Geben Sie den Authentifizierungsnamen des Clients ein.

Feld	Beschreibung
Passwort	Nur für **Rolle** = *Client* Geben Sie das Authentifizierungspasswort ein.
RADIUS-Server Gruppen-ID	Nur für **Rolle** = *Server* Wählen Sie die gewünschte in **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS** konfigurierte RADIUS-Gruppe aus.
Benutzer	Nur für **Rolle** = *Server* und **Modus** = *Lokal* Ist Ihr Gateway als XAuth-Server konfiguriert, können die Clients über eine lokal konfigurierte Benutzerliste authentifiziert werden. Definieren Sie hier die Mitglieder der Benutzergruppe dieses XAUTH-Profils, indem Sie den Authentifizierungsnamen des Clients (**Name**) und das Authentifizierungspasswort (**Passwort**) eingeben. Fügen Sie weitere Mitglieder mit **Hinzufügen** hinzu.

23.1.5 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.

23.1.5.1 Bearbeiten oder Neu

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

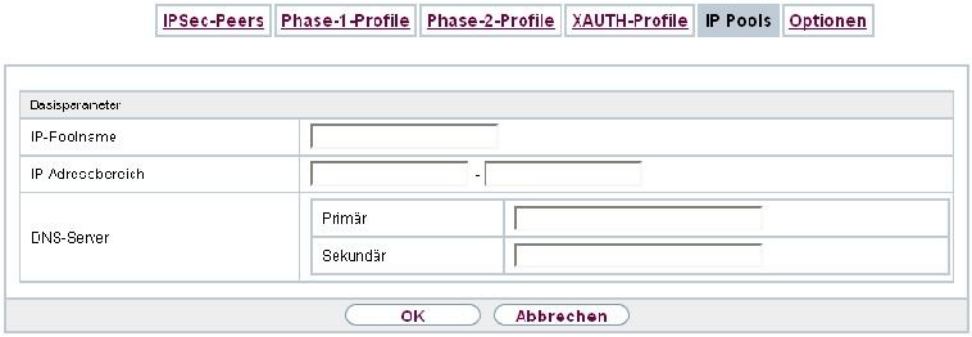


Abb. 208: **VPN->IPSec->IP Pools->Neu**

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

23.1.6 Optionen

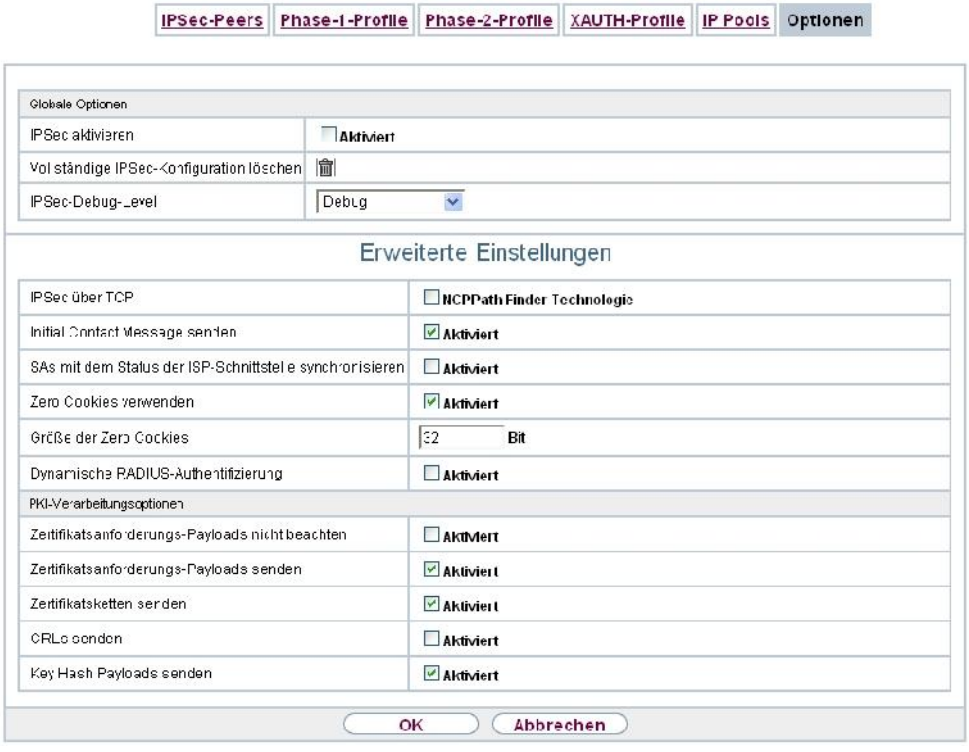


Abb. 209: **VPN->IPSec->Optionen**

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

Felder im Menü Globale Optionen

Feld	Beschreibung
IPSec aktivieren	Wählen Sie, ob Sie IPSec aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.
Vollständige IPSec-Konfiguration löschen	Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts. Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die

Feld	Beschreibung
	Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen. Das Löschen der Konfiguration ist nur möglich mit **IPSec aktivieren** = nicht aktiviert.
IPSec-Debug-Level	Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems. Mögliche Werte: • *Notfall* (höchste Priorität) • *Alarm* • *Kritisch* • *Fehler* • *Warnung* • *Benachrichtigung* • *Informationen* • *Debug* (Standardwert, niedrigste Priorität) Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level "Debug" sämtliche erzeugten Meldungen aufgezeichnet werden.

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen bintec elmeg-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	Wählen Sie aus, ob IPSec über TCP verwendet werden soll. IPSec über TCP basiert auf der NCP-Path-Finder-Technologie. Diese Technologie sorgt dafür, dass der Datenverkehr (IKE,

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

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	Wählen Sie aus, ob Zertifikatanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungs-Payloads senden	Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatanforderungen gesendet werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Zertifikatsketten senden	Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.
CRLs senden	Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Key Hash Payloads senden	Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen. Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung. Aktivieren Sie diese Funktion mit *Aktiviert*, um dieses Verhalten

Feld	Beschreibung
	zu unterdrücken.

23.2 L2TP

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

Ihr bintec elmeg-Gerät unterstützt die folgenden zwei Modi:

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

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

23.2.1 Tunnelprofile

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

23.2.1.1 Neu

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

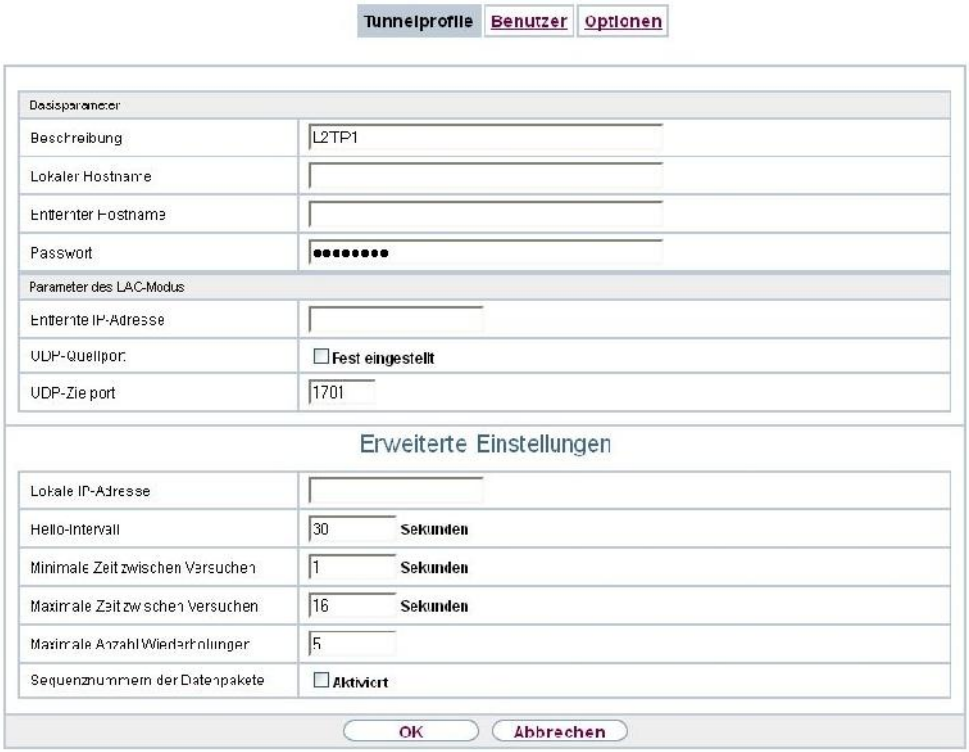


Abb. 210: **VPN->L2TP->Tunnelprofile->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für das aktuelle Profil ein. Ihr Gerät benennt die Profile automatisch mit *L2TP* und nummeriert diese, der Wert kann jedoch geändert werden.
Lokaler Hostname	Geben Sie den Hostnamen für LNS bzw. LAC ein. • *LAC*: Der lokale Hostname wird in abgehenden Tunnelaufbaumeldungen zur Identifizierung dieses Geräts aufgenommen und wird dem entfernten Hostnamen eines der am LNS konfigurierten Tunnelprofile zugeordnet. Bei diesen Tunnelaufbaumeldungen handelt es sich um die vom LAC ausgesandten SCCRQs (Start Control Connection Request) und die vom LNS ausgesandten SCCRPs (Start Control Connection Reply).

Feld	Beschreibung
	• *LNS*: Entspricht dem Wert für **Entfernter Hostname** der eingehenden Tunnelaufbaumeldung vom LAC.
Entfernter Hostname	Geben Sie den Hostnamen des LNS bzw. LAC ein: • *LAC*: Definiert den Wert für **Lokaler Hostname** des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). Ein im LAC konfigurierter **Lokaler Hostname** muss zu **Entfernter Hostname**n passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. • *LNS*: Definiert den **Lokaler Hostname**n des LAC. Falls das Feld **Entfernter Hostname** auf dem LNS leer bleibt, wird das dazugehörige Profil als Standardeintrag qualifiziert, der für alle ankommenden Rufe benutzt wird, für die kein Profil mit passendem entfernten Hostnamen gefunden werden kann.
Passwort	Geben Sie das Passwort ein, welches für die Tunnel-Authentifizierung benutzt wird. Die Authentifizierung zwischen LAC und LNS erfolgt in beiden Richtungen, d. h. der LNS prüft den **Lokaler Hostname**n und das **Passwort**, die in der SCCRQ des LAC enthalten sind und vergleicht sie mit denen, die im relevanten Profil angegeben sind. Der LAC macht das Gleiche mit den jeweiligen Feldern der SCCRP des LNS. Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.

Felder im Menü Parameter des LAC-Modus

Feld	Beschreibung
Entfernte IP-Adresse	Geben Sie die feste IP-Adresse des LNS ein, die als Zieladresse für Verbindungen genutzt wird, die auf diesem Profil aufbauen. Das Ziel muss ein Gerät sein, welches sich wie ein LNS verhalten kann.
UDP-Quellport	Geben Sie an, wie die Portnummer ermittelt werden soll, die als Quellport für alle abgehenden L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen. Standardmäßig ist die Option **Fest eingestellt** deaktiviert, was

Feld	Beschreibung
	bedeutet, dass den Verbindungen, die dieses Profil nutzen, Ports dynamisch zugeordnet werden. Wenn Sie einen fixen Port eingeben möchten, aktivieren Sie die Option *Fest eingestellt*. Wenn Sie Probleme mit der Firewall bzw. NAT feststellen, wählen Sie diese Option. Verfügbare Werte sind dann *0* bis *65535*.
UDP-Zielport	Geben Sie die Zielportnummer ein, die für alle Rufe genutzt wird, die auf diesem Profil aufbauen. Der entfernte LNS, der den Ruf empfängt, muss diesen Port auf L2TP-Verbindungen überwachen. Mögliche Werte sind *0* bis *65535*. Der Standardwert ist *1701* (RFC 2661).

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	1 bis *255*, der Standardwert ist *1*.
Maximale Zeit zwischen Versuchen	Geben Sie die maximale Zeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *16*.
Maximale Anzahl Wiederholungen	Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden. Verfügbare Werte sind *8* bis *255*, der Standardwert ist *5*.
Sequenznummern der Datenpakete	Wählen Sie aus, ob Ihr Gerät für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folgenummern benutzen soll oder nicht. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

23.2.2 Benutzer

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

23.2.2.1 Neu

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

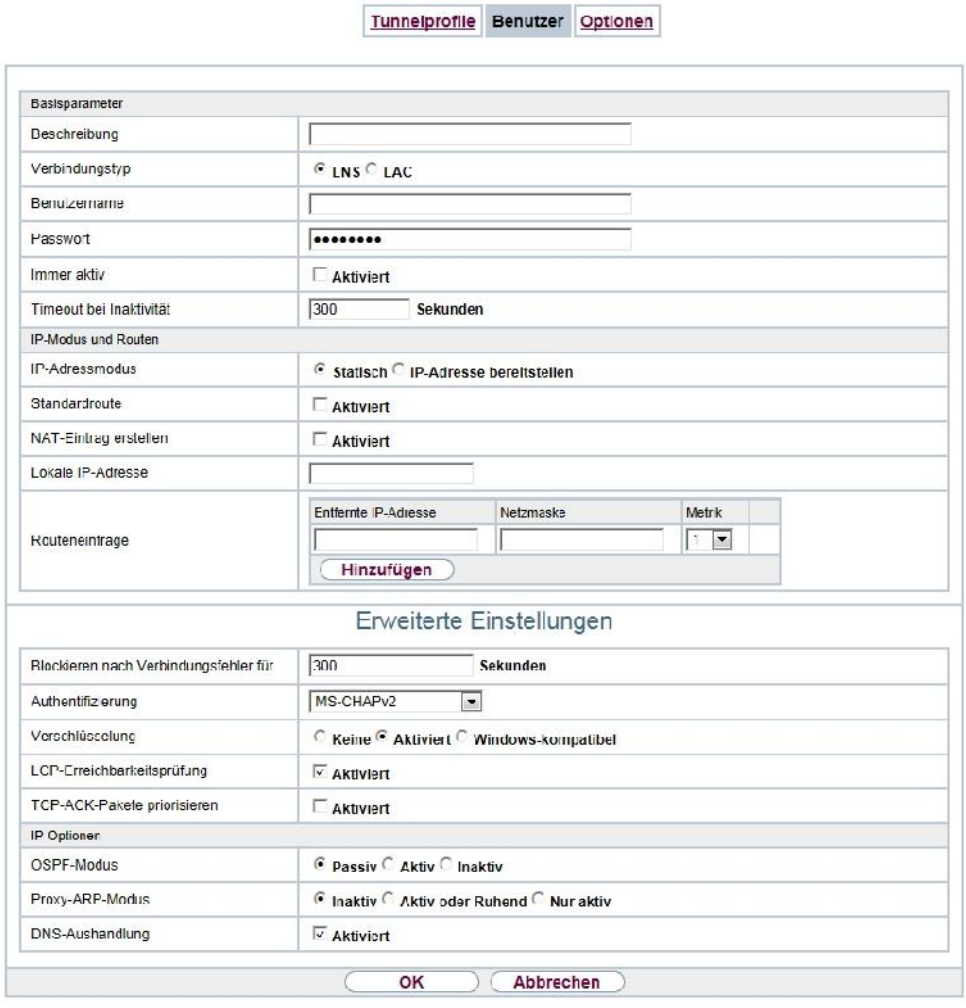


Abb. 211: **VPN->L2TP->Benutzer->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den L2TP-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden. Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.

Feld	Beschreibung
Verbindungstyp	Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerkservers (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll. Mögliche Werte: • *LNS* (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • *LAC*: Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.
Tunnelprofil	Nur für **Verbindungstyp** = *LAC* Wählen Sie ein im Menü **Tunnelprofil** erstelltes Profil für die Verbindung zu diesem L2TP-Partner aus.
Benutzername	Geben Sie die Kennung Ihres Geräts ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Zur Verfügung stehen Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Short Hold. Der Standardwert ist *300*.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.

Feld	Beschreibung
	Mögliche Werte: • *Statisch* (Standardwert): Sie geben eine statische IP-Adresse ein. • *IP-Adresse bereitstellen*: Nur für **Verbindungstyp** = *LNS*. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • *IP-Adresse abrufen*: Nur für **Verbindungstyp** = *LAC*. Ihr Gerät erhält dynamisch eine IP-Adresse.
IP-Zuordnungspool (IPCP)	Nur für **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie einen im Menü **WAN**->**Internet + Einwählen**->**IP Pools** konfigurierten IP Pool aus.
Standardroute	Nur für **IP-Adressmodus** = *IP-Adresse abrufen* und *Statisch* Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv .
NAT-Eintrag erstellen	Nur für **IP-Adressmodus** = *IP-Adresse abrufen* und *Statisch* Wählen Sie aus, ob Network Address Translation (NAT) für diese Verbindung aktiviert werden soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Nur für **IP-Adressmodus** = *Statisch* Geben Sie die WAN-IP-Adresse Ihres Geräts ein.
Routeneinträge	Nur für **IP-Adressmodus** = *Statisch* Geben Sie **Entfernte IP-Adresse** und **Netzmaske** des LANs des L2TP-Partners und die dazugehörige **Metrik** ein. Fügen Sie weitere Einträge mit **Hinzufügen** hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *300*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus. Mögliche Werte: • *PAP/CHAP/MS-CHAP* (Standardwert): Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *PAP*: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *MS-CHAPv2*: Nur MS-CHAP Version 2 ausführen. • *Keine*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Wenn **Verschlüsselung** gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: • *Keine*: Es wird keine MPP-Verschlüsselung angewendet. • *Aktiviert* (Standardwert): Die MPP-Verschlüsselung V2

Feld	Beschreibung
	mit 128 Bit wird nach RFC 3078 angewendet. • *Windows-kompatibel*: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen. Mögliche Werte: • *Passiv* (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing-Informationen berücksichtigt und über aktive Schnittstellen propagiert. • *Aktiv*: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • *Inaktiv*: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll.

Feld	Beschreibung
	Mögliche Werte: • *Inaktiv* (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner. • *Aktiv oder Ruhend*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner *aktiv* (aktiv) oder *ruhend* (ruhend) ist. Bei *ruhend* beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • *Nur aktiv*: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner *aktiv* (aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner besteht.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für **Primärer DNS-Server** und **Sekundärer DNS-Server** und **WINS-Server Primär** und **Sekundär** vom L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

23.2.3 Optionen

Abb. 212: **VPN->L2TP->Optionen**

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

Felder im Menü Globale Optionen

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

23.3 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.

23.3.1 PPTP-Tunnel

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

23.3.1.1 Neu

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

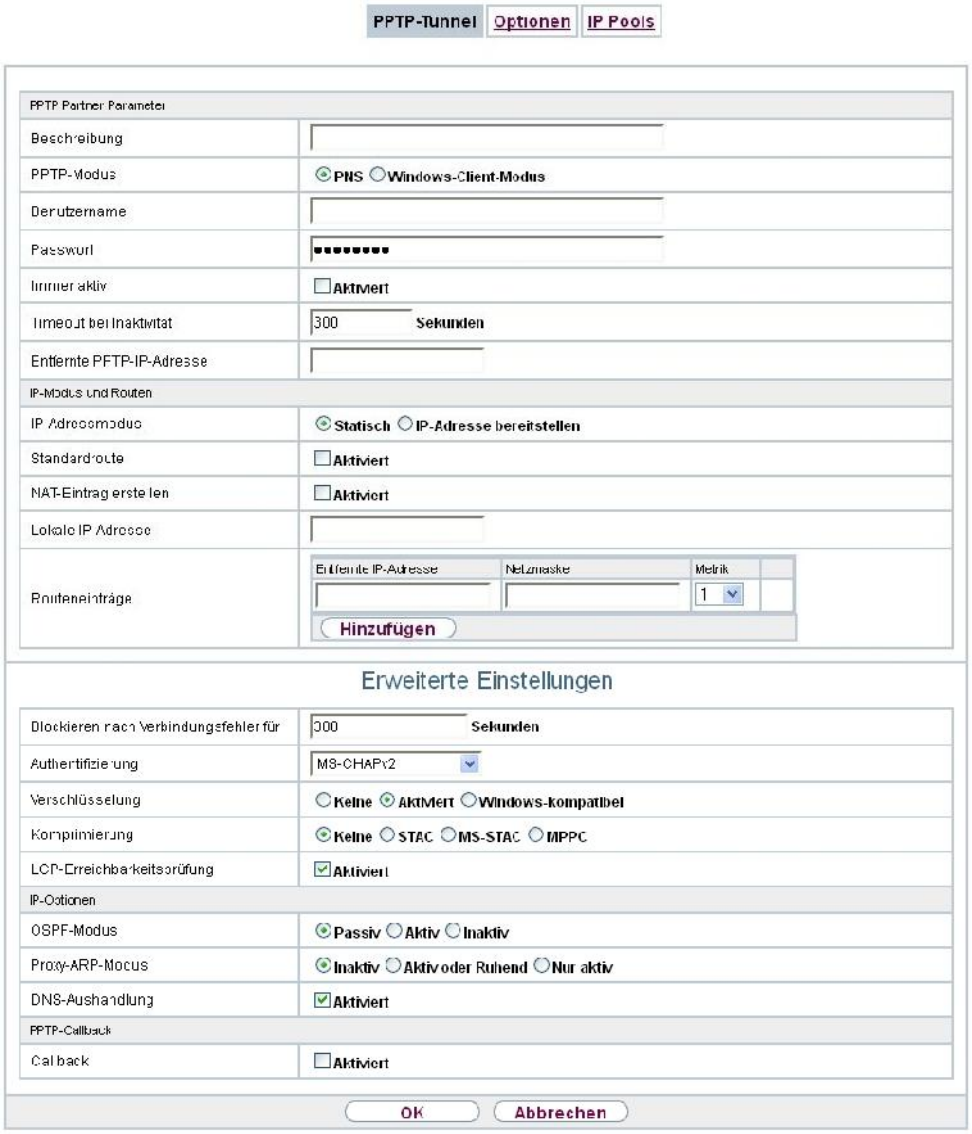


Abb. 213: **VPN**->**PPTP**->**PPTP-Tunnel**->**Neu**

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

Felder im Menü PPTP Partner Parameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Namen ein, um den Tunnel eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPTP-Modus	Geben Sie die Rollenverteilung der PPTP-Schnittstelle an. Mögliche Werte: • *PNS* (Standardwert): Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Servers zu. • *Windows-Client-Modus*: Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Clients zu.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Timeout bei Inaktivität	Nur wenn **Immer aktiv** deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von *0* bis *3600* (Sekunden). *0* deaktiviert den Timeout. Der Standardwert ist *300*. Beispiel: *10* für FTP-Übertragungen, *20* für LAN-zu-LAN-Übertragungen, *90* für Internetverbindungen.
Entfernte PPTP-IP-Adresse	Nur für **PPTP-Modus** = *PNS* Geben Sie die IP-Adresse des PPTP-Partners ein.
Entfernte PPTP-IP-Adresse / **Hostname**	Nur für **PPTP-Modus** = *Windows-Client-Modus* Geben Sie die IP-Adresse des PPTP-Partners ein.

Felder im Menü IP-Modus und Routen

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

Feld	Beschreibung
	• *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0 - 15*). Der Standardwert ist *1*.
IP-Zuordnungspool (IPCP)	Nur bei **PPTP-Modus** = *PNS*, **IP-Adressmodus** = *IP-Adresse bereitstellen* Wählen Sie hier einen im Menü **VPN**->**PPTP**->**IP Pools** konfigurierten IP-Pool aus.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist *300*.
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen PPTP-Partner aus. Mögliche Werte: • *PAP*: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • *CHAP*: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • *PAP/CHAP*: Vorrangig CHAP, sonst PAP ausführen. • *MS-CHAPv1*: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • *PAP/CHAP/MS-CHAP*: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP-Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • *MS-CHAPv2* (Standardwert): Nur MS-CHAP Version 2 ausführen. • *Keiner*: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.

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

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.

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

Felder im Menü PPTP-Callback

Feld	Beschreibung
Callback	Ermöglicht den Aufbau eines PPTP-Tunnels über das Internet mit einem PPTP-Partner, selbst wenn dieser momentan nicht online ist. In der Regel wird mittels ISDN-Ruf der PPTP-Partner aufgefordert, online zu gehen und eine PPTP-Verbindung aufzubauen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Beachten Sie, dass Sie die entsprechende Option auf den Gateways beider Partner aktivieren müssen. Für diese Funktion wird in der Regel ein ISDN-Anschluss benötigt. Ohne ISDN ist Callback nur in Spezialanwendungen zu aktivieren.
Eingehende ISDN-Nummer	Nur wenn **Callback** aktiviert ist. Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number).
Ausgehende ISDN-Nummer	Nur wenn **Callback** aktiviert ist. Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number).

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

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

23.3.2 Optionen

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

Abb. 214: **VPN->PPTP->Optionen**

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

Felder im Menü Globale Optionen

Feld	Beschreibung
GRE-Window-Anpassung	Wählen Sie, ob Sie GRE Window Adaption aktivieren wollen. Diese Anpassung ist erst notwendig, wenn Sie unter Microsoft Windows XP das Service Pack 1 installiert haben. Da Microsoft mit dem SP1 den Bestätigungalgorithmus innerhalb des GRE-Protokolls geändert hat, muss bei bintec elmeg-Geräten die automatische Window-Anpassung für GRE abgeschaltet werden. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
GRE-Window-Größe	Geben Sie die maximale Anzahl an GRE-Paketen ein, die ohne Bestätigung geschickt werden kann. Windows verwendet seit der Version XP ein höheres initiales Empfangs-Window im GRE, weshalb die maximale Sende-Window-Größe über den Wert **GRE-Window-Größe** angepasst werden sollte. Mögliche Werte sind *0* bis *256*. Standardwert ist *0*.
Max. eingehende Kontrollverbindungen über	Geben Sie die maximale Anzahl der Kontrollverbindungen ein.

Feld	Beschreibung
entfernte IP-Adresse	

23.3.3 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.

23.3.3.1 Bearbeiten oder Neu

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

Abb. 215: **VPN->PPTP->IP Pools->Neu**

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

23.4 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.

23.4.1 GRE-Tunnel

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

23.4.1.1 Neu

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

Abb. 216: **VPN->GRE->GRE-Tunnel->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein. Wird keine IP-Adresse (dies entspricht der IP-Adresse 0.0.0.0) angegeben, wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse der GRE-Pakete zum GRE-Partner ein.
Standardroute	Wenn Sie die **Standardroute** aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
Lokale IP-Adresse	Geben Sie hier die (LAN-seitige) IP-Adresse ein, die als Quelladresse Ihre Gerätes für eigene Pakete durch den GRE-Tunnel verwendet werden soll.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit **Hinzufügen** neue Einträge hinzu. • *Entfernte IP-Adresse*: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • *Netzmaske*: Netzmaske zu **Entfernte IP-Adresse**. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standard-Netzmaske. • *Metrik*: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich *0*... *15*). Der Standardwert ist *1*.
MTU	Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf. Mögliche Werte sind *1* bis *8192*. Der Standardwert ist *1500*.
Schlüssel verwenden	Aktivieren Sie die Eingabe einer Kennung für die GRE-Verbindung, welche die Unterscheidung mehrerer parallel laufender GRE-Verbindungen zwischen zwei GRE-Partnern ermöglicht (siehe RFC 1701). Mit *Aktiviert* wird die Kennung aktiviert. Standardmäßig ist die Funktion nicht aktiv.
Schlüsselwert	Nur wenn **Schlüssel verwenden** aktiviert ist. Geben Sie die GRE-Verbindungskennung ein. Mögliche Werte sind *0* bis *2147483647*. Der Standardwert ist *0*.

Kapitel 24 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen bintec elmeg Gateways über eine leistungsfähige Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann nicht nur aufgrund von Quell- und Zieladressen oder Ports, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung zu einem Partner gefällt werden.

Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören. Die Aushandlung einer FTP-Verbindung findet zum Beispiel über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

SIF und andere Sicherheitsfunktionen

Die Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der bintec elmeg-Geräte ein. Systemen wie Network Address Translation (NAT) und IP-Zugriffs-Listen (IPAL) gegenüber ist der Konfigurationsaufwand der SIF vergleichbar einfach.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muss man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, dass die Regeln der SIF generell global angewendet werden, d. h. nicht auf eine Schnittstelle beschränkt sind.

Grundsätzlich werden aber dieselben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske)
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)
- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der ein-

zelnen Sicherheitsinstanzen und ihrer Funktionsweise.

NAT

Eine der Grundfunktionen von NAT ist die Umsetzung lokaler IP-Adressen Ihres LANs in die globalen IP-Adressen, die Ihnen von Ihrem ISP zugewiesen werden, und umgekehrt. Dabei werden zunächst alle von außen initiierten Verbindungen abgeblockt, d. h. jedes Paket, welches Ihr Gerät nicht einer bereits bestehenden Verbindung zuordnen kann, wird abgewiesen. Auf diese Art kann eine Verbindung lediglich von innen nach außen aufgebaut werden. Ohne explizite Genehmigungen wehrt NAT jeden Zugriff aus dem WAN auf das LAN ab.

IP Access Listen

Hier werden Pakete ausschließlich aufgrund der oben aufgeführten Kriterien zugelassen oder abgewiesen, d. h. der Zustand der Verbindung wird nicht berücksichtigt (außer bei **Dienste** = *TCP*).

SIF

Die SIF sondert alle Pakete aus, die nicht explizit oder implizit zugelassen werden. Dabei gibt es sowohl ein "Verweigern", bei dem keine Fehlermeldung an den Sender des zurückgewiesenen Pakets ausgegeben wird, als auch ein "Ablehnen", bei dem der Sender über die Ablehnung des Pakets informiert wird.

Die eingehenden Pakete werden folgendermaßen bearbeitet:

- Zunächst überprüft die SIF, ob ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann. Ist dies der Fall, wird es weitergeleitet. Kann das Paket keiner bestehenden Verbindung zugeordnet werden, wird überprüft, ob eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden). Ist dies der Fall, wird das Paket ebenfalls akzeptiert.
- Wenn das Paket keiner bestehenden und auch keiner zu erwartenden Verbindung zugeordnet werden kann, werden die SIF-Filterregeln angewendet: Trifft auf das Paket eine Deny-Regel zu, wird es abgewiesen, ohne dass eine Fehlermeldung an den Sender des Pakets geschickt wird; trifft eine Reject-Regel zu, wird das Paket abgewiesen und eine ICMPHost-Unreachable-Meldung an den Sender des Paktes ausgegeben. Nur wenn auf das Paket eine Accept-Regel zutrifft, wird es weitergeleitet.
- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen (= Standardverhalten).

24.1 Richtlinien

24.1.1 Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

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

Abb. 217: **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.

24.1.1.1 Neu

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

Abb. 218: **Firewall**->**Richtlinien**->**Filterregeln**->**Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus. In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall**->**Schnittstellen**->**Gruppen**), Adressen (siehe **Firewall**->**Adressen**->**Adressliste**) und Adressgruppen (siehe **Firewall**->**Adressen**->**Gruppen**) zur Auswahl. Der Wert *Beliebig* bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.
Ziel	Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus. In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe **Firewall**->**Schnittstellen**->**Gruppen**), Adressen (siehe **Firewall**->**Adressen**->**Adressliste**) und Adressgruppen (siehe **Firewall**->**Adressen**->**Gruppen**) zur Auswahl. Der Wert *Beliebig* bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfi-

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

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

24.1.2 QoS

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

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

24.1.2.1 Neu

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

Abb. 219: **Firewall**->**Richtlinien**->**QoS**->**Neu**

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

Felder im Menü QoS-Schnittstelle konfigurieren

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

24.1.3 Optionen

In diesem Menü können Sie die Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wie vielen Sekunden Inaktivität eine Sitzung beendet werden soll.

Abb. 220: **Firewall->Richtlinien->Optionen**

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

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Firewall Status	Aktivieren oder deaktivieren Sie die Firewall-Funktion. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion aktiv.
Protokollierte Aktionen	Wählen Sie den Firewall-Syslog-Level aus. Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme. Mögliche Werte: • *Alle* (Standardwert): Alle Firewall-Aktivitäten werden angezeigt. • *Verweigern*: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion".

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

Felder im Menü Sitzungstimer

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

24.2 Schnittstellen

24.2.1 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.

24.2.1.1 Neu

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

Abb. 221: **Firewall**->**Schnittstellen**->**Gruppen**->**Neu**

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

Felder im Menü Basisparameter

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

24.3 Adressen

24.3.1 Adressliste

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

24.3.1.1 Neu

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

Abb. 222: **Firewall**->**Adressen**->**Adressliste**->**Neu**

Das Menü **Firewall**->**Adressen**->**Adressliste**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adresse ein.
Adresstyp	Wählen Sie aus, welche Art von Adresse Sie angeben wollen. Mögliche Werte: • *Adresse/Subnetz* (Standardwert): Sie geben eine IP-Adresse mit Subnetzmaske ein. • *Adressbereich*: Sie geben einen IP-Adressbereich mit Anfangs- und Endadresse ein.
Adresse/Subnetz	Nur für **Adresstyp** = *Adresse/Subnetz* Geben Sie die IP-Adresse des Hosts oder eine Netzwerk-Adresse und die zugehörige Netzmaske ein. Standardwert ist jeweils *0.0.0.0*.

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

24.3.2 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.

24.3.2.1 Neu

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

Abb. 223: **Firewall**->**Adressen**->**Gruppen**->**Neu**

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

Felder im Menü Basisparameter

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

24.4 Dienste

24.4.1 Diensteliste

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

24.4.1.1 Neu

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

Abb. 224: **Firewall**->**Dienste**->**Diensteliste**->**Neu**

Das Menü **Firewall**->**Dienste**->**Diensteliste**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protokoll	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
Zielportbereich	Nur für **Protokoll** = *TCP*, *UDP/TCP* oder *UDP* Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll. Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen. Mögliche Werte sind *1* bis *65535*.

Feld	Beschreibung
Quellportbereich	Nur für **Protokoll** = *TCP*, *UDP/TCP* oder *UDP* Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port an. Soll ein Portnummernbereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Portbereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen. Mögliche Werte sind *1* bis *65535*.
Typ	Nur für **Protokoll** = *ICMP* Das Feld **Typ** gibt die Klasse der ICMP-Nachrichten an, das Feld **Code** spezifiziert die Art der Nachricht genauer. Mögliche Werte: • *Beliebig* (Standardwert) • *Echo Reply* • *Destination Unreachable* • *Source Quench* • *Redirect* • *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	Nur für **Typ** = *Destination Unreachable* stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung. Mögliche Werte:

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

24.4.2 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.

24.4.2.1 Neu

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

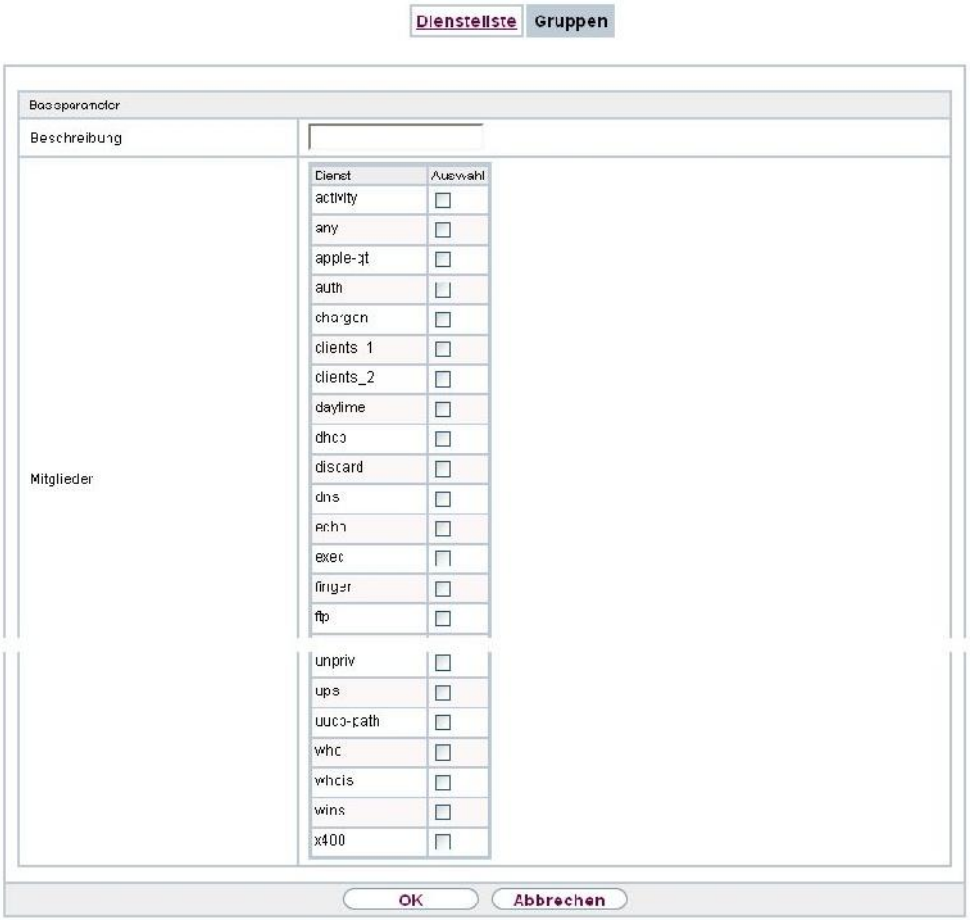


Abb. 225: **Firewall**->**Dienste**->**Gruppen**->**Neu**

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

Felder im Menü Basisparameter

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

Kapitel 25 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)
- Bereitstellung öffentlicher Internetzugänge (Hotspot)
- Wake on LAN, um Netzwerkgeräte zu aktivieren, die aktuell ausgeschaltet sind.

25.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste**->**DNS**->**Globale Einstellungen**->**Basisparameter** werden die IP-

Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der globalen Name-Server kann Ihr Gerät auch dynamisch via PPP oder DHCP erhalten bzw. diese ggf. übermitteln.

Strategie zur Namensauflösung auf Ihrem Gerät

Eine DNS-Anfrage wird von Ihrem Gerät folgendermaßen behandelt:

(1) Falls möglich, wird die Anfrage aus dem statischen oder dynamischen Cache direkt mit IP-Adresse oder negativer Antwort beantwortet.

(2) Ansonsten wird, falls ein passender Forwarding-Eintrag vorhanden ist, der entsprechende DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

(3) Ansonsten werden, falls Name-Server eingetragen sind, unter Berücksichtigung der konfigurierten Priorität und wenn der entsprechende Schnittstellenstatus "up" ist, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

(4) Ansonsten werden, falls eine Internet- oder Einwählverbindung als Standard-Schnittstelle ausgewählt ist, die dazugehörigen DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.

(5) Ansonsten wird, falls im Menü **WAN**->**Internet + Einwählen** ein Eintrag angelegt wurde und das Überschreiben der Adressen der globalen Name-Server zulässig ist (**Schnittstellenmodus** = *Dynamisch*), eine Verbindung zur ersten Internet- bzw. Einwählverbindung ggf. kostenpflichtig aufgebaut, die so konfiguriert ist, dass DNS-Server-Adressen von DNS-Servern angefordert werden können (**DNS-Aushandlung** = *Aktiviert*) - soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung stehen diese Name-Server somit für weitere Anfragen zur Verfügung.

(6) Ansonsten wird die initiale Anfrage mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit `non-existent domain` antwortet, wird die initiale Anfrage sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache Ihres Geräts aufgenommen.

25.1.1 Globale Einstellungen

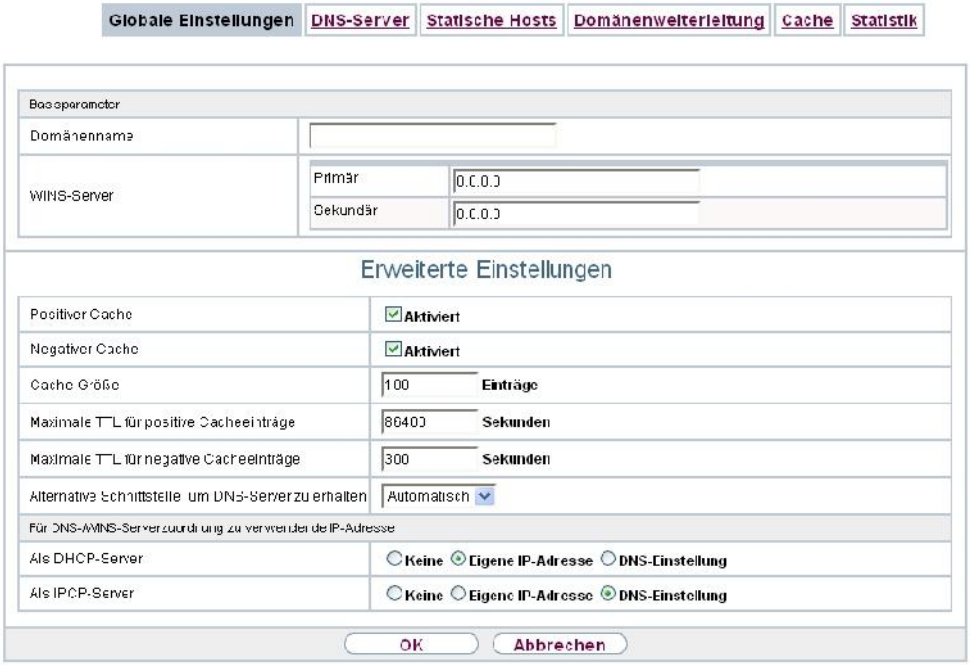


Abb. 226: **Lokale Dienste->DNS->Globale Einstellungen**

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
WINS-Server **Primär** **Sekundär**	Geben Sie die IP-Adresse des ersten und, falls erforderlich, des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	Wählen Sie aus, ob der positive dynamische Cache aktiviert

Feld	Beschreibung
	werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Negativer Cache	Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Cache-Größe	Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein. Wird dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird **Cache-Größe** vom Benutzer heruntergesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. **Cache-Größe** kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden. Mögliche Werte: *0*.. *1000*. 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 Schnittstel-	Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur

Feld	Beschreibung
le, um DNS-Server zu erhalten	Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren. Standardwert ist *Automatisch*, d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.

Felder im Menü Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse

Feld	Beschreibung
Als DHCP-Server	Wählen Sie aus, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn Ihr Gerät als DHCP-Server genutzt wird. Mögliche Werte: • *Keine*: Es wird keine Name-Server-Adresse übermittelt. • *Eigene IP-Adresse* (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • *DNS-Einstellung*: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	Wählen Sie aus, welche Name-Server-Adressen von Ihrem Gerät bei einer dynamischen Name-Server-Aushandlung übermittelt werden, wenn Ihr Gerät als IPCP-Server für PPP-Verbindungen genutzt wird. Mögliche Werte: • *Keine*: Es wird keine Name-Server-Adresse übermittelt. • *Eigene IP-Adresse*: Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • *DNS-Einstellung* (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

25.1.2 DNS-Server

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

25.1.2.1 Bearbeiten oder Neu

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

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern über unterschiedliche Schnittstellen eingerichtet sind und Lastverteilung verwendet wird.

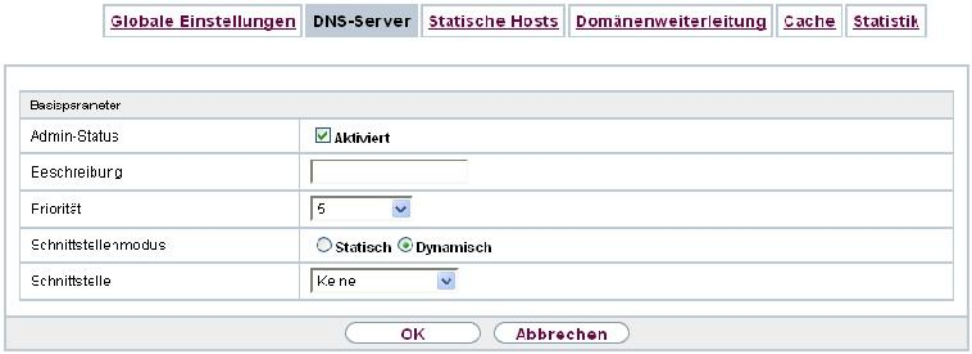


Abb. 227: **Lokale Dienste->DNS->DNS-Server->Neu**

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob der DNS-Server aktiv sein soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.
Priorität	Weisen Sie dem DNS-Server eine Priorität zu. Sie können einer Schnittstelle (d.h. zum Beispiel einem Ethernet-Port oder einem PPPoE-WAN-Partner) mehrere Paare von DNS-Servern (**Primärer DNS-Server** und **Sekundärer DNS-Server**) zuweisen. Verwendet wird das Paar mit der höchsten

Feld	Beschreibung
	Priorität, wenn die Schnittstelle im Zustand "up" ist. Mögliche Werte von *0* (höchste Priorität) bis *9* (niedrigste Priorität). Standardwert ist *5*.
Schnittstellenmodus	Wählen Sie aus, ob die IP-Adressen von Name-Servern für die Namensauflösung von Internet-Adressen automatisch bezogen oder ob abhängig von der Priorität bis zu zwei feste DNS-Server-Adressen eingetragen werden sollen. Mögliche Werte: • *Statisch* • *Dynamisch* (Standardwert)
Schnittstelle	Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll. Bei **Schnittstellenmodus** = *Dynamisch* Mit der Einstellung *Keine* wird ein globaler DNS-Server angelegt. Bei **Schnittstellenmodus** = *Statisch* Mit der Einstellung *Beliebig* wird ein DNS-Server für alle Schnittstellen konfiguriert.
Primärer DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie die IP-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.
Sekundärer DNS-Server	Nur bei **Schnittstellenmodus** = *Statisch* Geben Sie optional die IP-Adresse eines alternativen Name-Servers ein.

25.1.3 Statische Hosts

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

25.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

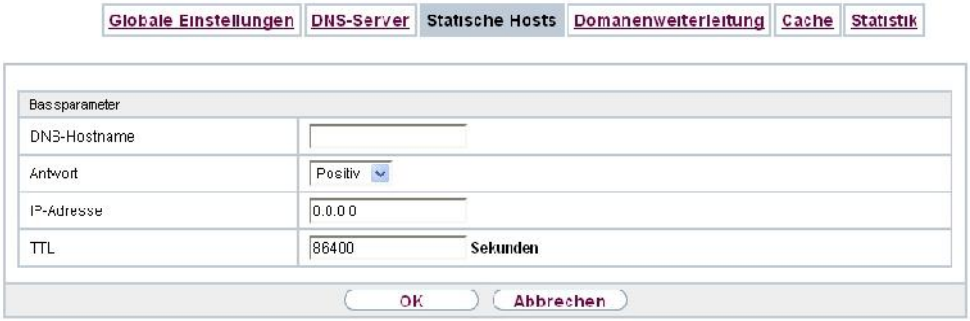


Abb. 228: **Lokale Dienste->DNS->Statische Hosts->Neu**

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DNS-Hostname	Geben Sie den Host-Namen ein, dem die in diesem Menü definierte **IP-Adresse** zugeordnet werden soll, wenn eine DNS-Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage negativ beantwortet wird, wird keine Adresse mitgeteilt. Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.bintec-elmeg.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit **OK** "<**Name**.> " ergänzt. Einträge mit Leerzeichen sind nicht erlaubt.
Antwort	Wählen Sie die Art der Antwort auf DNS-Anfragen zu diesem Eintrag aus. Mögliche Werte: • *Negativ*: Eine DNS-Anfrage nach **DNS-Hostname** wird negativ beantwortet. • *Positiv* (Standardwert): Eine DNS-Anfrage nach **DNS-Hostname** wird mit der dazugehörigen **IP-Adresse** beantwortet.

Feld	Beschreibung
	• *Keine*: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IP-Adresse	Nur bei **Antwort** = *Positiv* Geben Sie die IP-Adresse ein, die nach **DNS-Hostname** zugeordnet wird.
TTL	Geben Sie die Gültigkeitsdauer der Zuordnung von **DNS-Hostname** zu **IP-Adresse** in Sekunden ein (nur relevant bei **Antwort** = *Positiv*), die anfragenden Hosts übermittelt wird. Standardwert ist *86400* (= 24 h).

25.1.4 Domänenweiterleitung

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

25.1.4.1 Neu

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

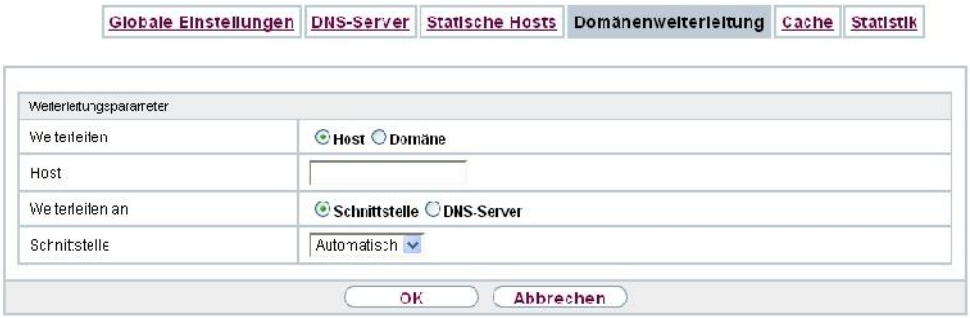


Abb. 229: **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu**

Das Menü **Lokale Dienste**->**DNS**->**Domänenweiterleitung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	Wählen Sie aus, ob ein Host oder eine Domäne weitergeleitet

Feld	Beschreibung
	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. *.binte-elmeg.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. *.bintec-elmeg.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-

Feld	Beschreibung
	Servers ein.

25.1.5 Cache

Im Menü **Lokale Dienste**->**DNS**->**Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

Abb. 230: **Lokale Dienste**->**DNS**->**Cache**

Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** markieren.

Durch Markieren eines Eintrags und Bestätigen mit **Als statisch festlegen** wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet aus dieser Liste und wird in der Liste im Menü **Statische Hosts** angezeigt. Die TTL wird übernommen.

25.1.6 Statistik

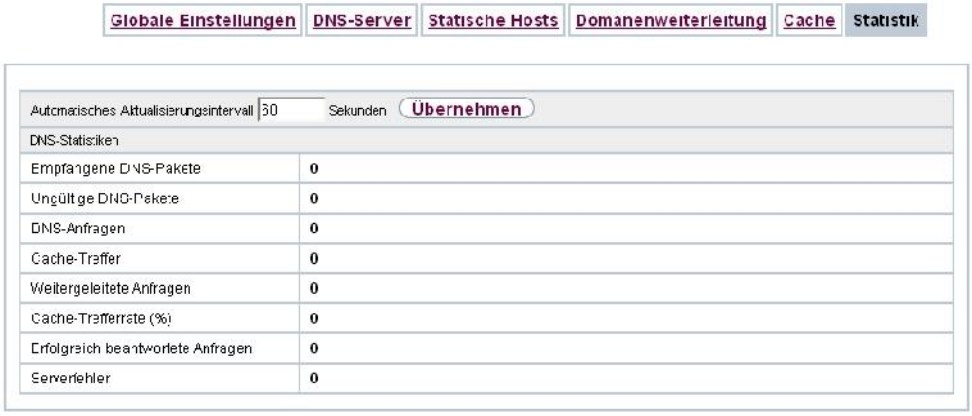


Abb. 231: **Lokale Dienste->DNS->Statistik**

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der **Cache-Treffer** pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

25.2 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.

25.2.1 HTTPS-Server

Im Menü **Lokale Dienste**->**HTTPS**->**HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Abb. 232: **Lokale Dienste**->**HTTPS**->**HTTPS-Server**

Das Menü **Lokale Dienste**->**HTTPS**->**HTTPS-Server** besteht aus folgenden Feldern:

Felder im Menü HTTPS-Parameter

Feld	Beschreibung
HTTPS-TCP-Port	Geben Sie den Port ein, über den die HTTPS-Verbindung aufgebaut werden soll. Möglich sind Werte von *0* bis *65535*. Standardwert ist *443*.
Lokales Zertifikat	Wählen Sie ein Zertifikat aus, das für die HTTPS-Verbindung verwendet werden soll. Mögliche Werte: • *Intern* (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möch-

Feld	Beschreibung
	ten. • *<Zertifikatsname>*: Wählen Sie ein unter **Systemverwaltung**->**Zertifikate**->**Zertifikatsliste** eingetragenes Zertifikat aus.

25.3 DynDNS-Client

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Hostnamens bei einem DynDNS-Provider
- Konfiguration Ihres Geräts

Registrierung

Bei der Registrierung des Hostnamens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Hostname für Ihr Gerät ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt für Sie die Aufgabe, alle DNS-Anfragen bezüglich des Hosts *dyn_client.provider.com* mit der dynamischen IP-Adresse Ihres Geräts zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Geräts informiert ist, kontaktiert Ihr Gerät beim Aufbau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse.

25.3.1 DynDNS-Aktualisierung

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

25.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

Abb. 233: **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu**

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internet Service Providers).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind. Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden. Weitere DynDNS-Provider können im Menü **Lokale**

Feld	Beschreibung
	DynDNS-Client->**DynDNS-Provider** konfiguriert werden. 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.

25.3.2 DynDNS-Provider

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

25.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

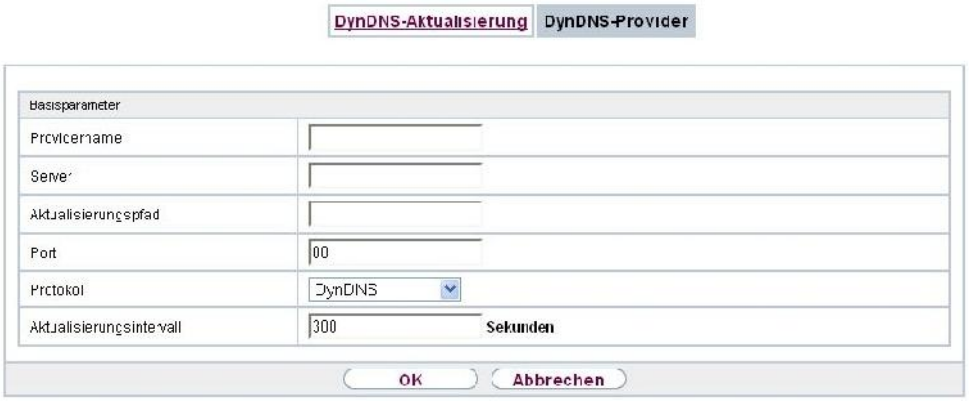


Abb. 234: **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu**

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider. Standardwert ist *80*.
Protokoll	Wählen Sie eines der implementierten Protokolle aus. Mögliche Werte: • *DynDNS* (Standardwert) • *Static DynDNS*

Feld	Beschreibung
	• *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Aktualisierungsintervall	Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf. Standardwert ist *300* Sekunden.

25.4 DHCP-Server

Sie können Ihr Gerät als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) konfigurieren.

Jeder Rechner in Ihrem LAN benötigt, wie auch Ihr Gerät, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie Ihr Gerät als DHCP-Server einrichten, vergibt es anfragenden Rechnern im LAN automatisch IP-Adressen aus einem definierten IP-Adress-Pool.

Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine DHCP-Anfrage (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server." Daraufhin erhält der Client (im Zuge einer kurzen Kommunikation) vom bintec elmeg seine IP-Adresse.

Sie müssen so den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem Ihr Gerät jeweils für einen definierten Zeitraum IP-Adressen an Hosts im LAN vergibt. Ein DHCP-Server übermittelt auch die Adressen des statisch oder per PPP-Aushandlung eingetragenen Domain-Name-Servers (DNS), des NetBIOS Name Servers (WINS) und des Standard-Gateways.

25.4.1 IP-Pool-Konfiguration

Im Menü **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration** wird eine Liste aller konfigurierten IP-Pools angezeigt. Diese Liste ist global und zeigt auch in anderen Menüs konfigurerte Pools an.

25.4.1.1 Bearbeiten oder Neu

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

Abb. 235: **Lokale Dienste**->**DHCP-Server**->**IP-Pool-Konfiguration**->**Neu**

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	**Primär**: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll. **Sekundär**: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

25.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** wird eine Liste aller konfigurierter IP-Adresspools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. deaktivieren.

Hinweis

Im Auslieferungszustand ist der DHCP-Pool mit den IP-Adressen 192.168.0.10 bis 192.168.0.49 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

25.4.2.1 Bearbeiten oder Neu

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

Abb. 236: **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu**

Das Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, über welche die in **IP-Adressbereich** definierten Adressen an anfragende DHCP-Clients vergeben werden. Wenn eine DHCP-Anfrage über diese **Schnittstelle** eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
Pool-Verwendung	Wählen Sie aus, ob der IP-Pool für DHCP-Anfragen im gleichen Subnetz verwendet werden soll oder für DHCP-Anfragen, die aus einem anderen Subnetz zu Ihrem Gerät weitergeleitet wurden. In diesem Fall ist es möglich, IP-Adressen aus einem anderen Netz zu definieren. Mögliche Werte: • *Lokal* (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet. • *Relais*: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetz verwendet. • *Lokal/Relais*: Der DHCP-Pool wird für DHCP-Anfragen im selben Subnetz und aus anderen Subnetzen verwendet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Gateway	Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll. Mögliche Werte: • *Router als Gateway verwenden* (Standardwert): Hier wird die für die **Schnittstelle** definierte IP-Adresse übertragen. • *Kein Gateway*: Hier wird keine IP-Adresse übermittelt. • *Angeben*: Geben Sie die entsprechende IP-Adresse ein.

Feld	Beschreibung
Lease Time	Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll. Nachdem **Lease Time** abgelaufen ist, kann die Adresse durch den Server neu vergeben werden. Standardwert ist *120*.
DHCP-Optionen	Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen. Mögliche Werte für **Option**: • *Zeitserver* (Standardwert): Geben Sie die IP-Adresse des Zeitservers ein, die dem Client übermittelt werden soll. • *DNS-Server*: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • *DNS-Domänenname*: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • *WINS/NBNS-Server*: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • *WINS/NBT Node Type*: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • *TFTP-Server*: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • *CAPWAP Controller*: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • *URL (Provisionierungsserver)*: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. Verwenden Sie diese Option, um anfragenden **IP1x0**-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form *http://<IP-Adresse des Provisionierungsservers>/eg_prov* haben. • *Herstellergruppe* (Vendor Specific Information): Mit dieser Option können Sie dem Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen übermittlen. Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge

Feld	Beschreibung
	mit der Schaltfläche **Hinzufügen** ein.

Bearbeiten

Im Menü **Lokale Dienste** -> **DHCP-Server** ->**DHCP-Konfiguration**->**Erweiterte Einstellungen** können Sie einen Eintrag im Feld **DHCP-Optionen** bearbeiten, wenn **Option** = *Herstellergruppe* gewählt ist.

Wählen Sie das Symbol  , um einen vorhandenen Eintrag zu bearbeiten. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server zum Beispiel für bestimmte Telefone.

Felder im Menü Basisparameter

Feld	Beschreibung
Hersteller auswählen	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen. Mögliche Werte: • *Siemens* (Standardwert) • *Sonstige*
Provisioning-Server	Nur für **Hersteller auswählen** = *Siemens* Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll. Für die Einstellung **Hersteller auswählen** = *Siemens* wird der Standardwert *sdlp* angezeigt. Sie können die IP-Adresse des gewünschten Servers ergänzen.
Herstellerbeschreibung	Nur für **Hersteller auswählen** = *Sonstige* Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Benutzerdefinierte DHCP-Optionen	Nur für **Hersteller auswählen** = *Sonstige* Fügen Sie mit **Hinzufügen** weitere Einträge hinzu. Sie können DHCP-Optionen hinzufügen.

25.4.3 IP/MAC-Bindung

Im Menü **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.

Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration** IP-Adressbereiche konfiguriert wurden.

25.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

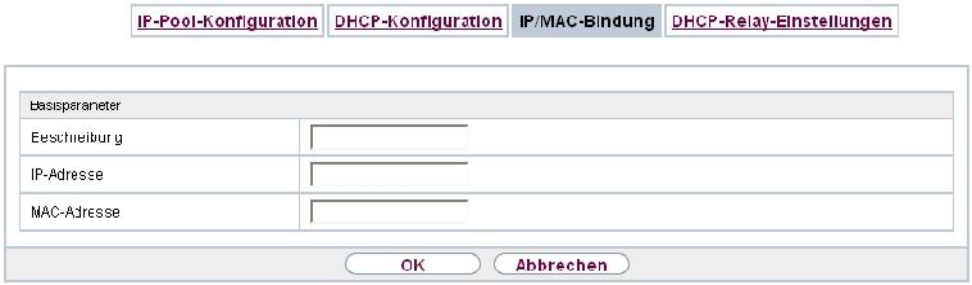


Abb. 237: **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung**->**Neu**

Das Menü **Lokale Dienste**->**DHCP-Server**->**IP/MAC-Bindung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen **MAC-Adresse** die **IP-Adresse** gebunden wird. Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.

Feld	Beschreibung
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.

25.4.4 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

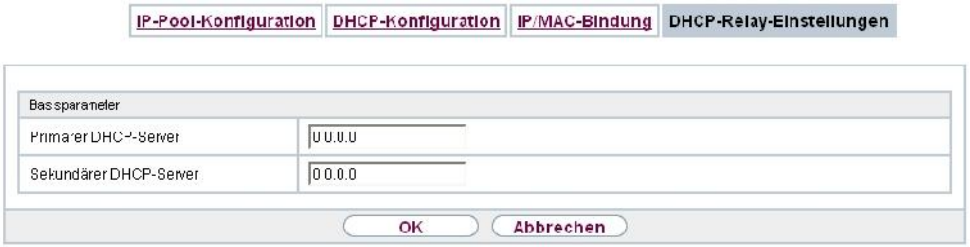


Abb. 238: **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen**

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

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

25.5 CAPI-Server

Mit der Funktion CAPI-Server können Sie an Nutzer der CAPI-Anwendungen Ihres Geräts Benutzernamen und Passwörter vergeben. So stellen Sie sicher, dass nur authorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen über CAPI aufbauen können.

Der Dienst CAPI ermöglicht eingehenden und ausgehenden Daten- und Sprachrufen die Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die Entfernte CAPI-Schnittstelle Ihres Geräts zugreifen. So können beispielsweise mit Ihrem Gerät verbundene Hosts Faxe empfangen und senden.

Hinweis

Alle eingehenden Rufe an die CAPI werden allen registrierten und "lauschenden" CAPI-Applikationen im LAN angeboten.

Im Auslieferungszustand ist für das Subsystem CAPI ein Benutzer mit dem Benutzernamen *default* ohne Passwort eingetragen.

Wenn Sie Ihre gewünschten Benutzer mit Passwort angelegt haben, sollten Sie den Benutzer *default* ohne Passwort löschen.

25.5.1 Benutzer

Im Menü **Lokale Dienste**->**CAPI-Server**->**Benutzer** wird eine Liste aller konfigurierter CAPI Benutzer angezeigt.

25.5.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

Abb. 239: **Lokale Dienste->CAPI-Server->Benutzer->Neu**

Das Menü **Lokale Dienste->CAPI-Server->Benutzer->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, für den der Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll.
Passwort	Geben Sie das Passwort ein, mit dem sich der Benutzer **Benutzername** identifizieren muss, um Zugang zum CAPI Dienst zu erhalten.
Zugriff	Wählen Sie aus, ob der Zugriff auf den CAPI-Dienst für den Benutzer erlaubt oder gesperrt werden soll. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

25.5.2 Optionen

Abb. 240: **Lokale Dienste->CAPI-Server->Optionen**

Das Menü **Lokale Dienste**->**CAPI-Server**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Server aktivieren	Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Faxkopfzeile	Nur für Geräte der **RTxxx2**-Serie Wählen Sie aus, ob am oberen Seitenrand von ausgehenden Faxen die Faxkopfzeile gedruckt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-Port des CAPI-Servers	Das Feld ist nur editierbar, wenn **Server aktivieren** aktiviert ist. Geben Sie die TCP-Port-Nummer für Remote-CA-PI-Verbindungen ein. Standardwert ist *2662*.

25.6 Scheduling

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

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

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

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

Achtung

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

Hinweis

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

25.6.1 Auslöser

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

25.6.1.1 Neu

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

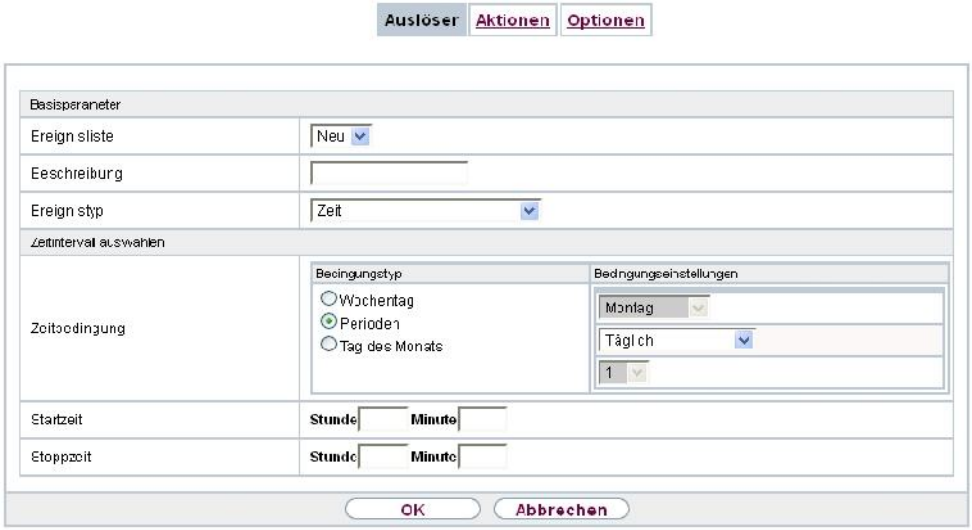


Abb. 241: **Lokale Dienste->Scheduling->Auslöser->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Ereignisliste	Mit *Neu* (Standardwert) können Sie eine neue Ereignisliste anlegen. Mit **Beschreibung** geben Sie dieser Liste einen Namen. Mit Hilfe der übrigen Parameter legen Sie das erste Ereignis in der Liste an. Wenn Sie eine bestehende Ereignisliste erweitern wollen, wählen Sie die gewünschte Ereignisliste aus und fügen ihr mindestens ein Ereignis hinzu. Über Ereignislisten können auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden. Die Ereingnisse werden in derseben Reihenfolge abgearbeitet wie sie in der Liste angelegt sind.
Beschreibung	Nur für **Ereignisliste** = *Neu* Geben Sie eine beliebige Bezeichnung für die Ereignisliste ein.
Ereignistyp	Wählen Sie den Typ des Ereignisses aus. Mögliche Werte:

Feld	Beschreibung
	• *Zeit* (Standardwert): Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden zu bestimmten Zeitpunkten ausgelöst. • *MIB/SNMP*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen. • *Schnittstellenstatus*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierten Schnittstellen einen bestimmten Status annehmen. • *Schnittstellenverkehr*: Die in **Aktionen** konfigurierten und zugewiesenenen Aktionen werden ausgelöst, wenn der Datenverkehr auf den angegebenen Schnittstellen den definierten Wert unter- oder überschreitet. • *Ping-Test*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist. • *Lebensdauer eines Zertifikats*: Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist. • *Status der GEO-Zone* :Die in **Aktionen** konfigurierten und zugewiesenene Aktionen werden ausgelöst, wenn die definierten **GEO-Zonen** einen bestimmten Status annehmen.
Überwachte GEO-Zone	Nur für **Ereignistyp** *Status der GEO-Zone* Wählen Sie eine konfigurierte GEO-Zone aus.
GEO Zone Status	Nur für **Ereignistyp** *Status der GEO-Zone* Wählen Sie den **GEO Zone Status** aus. Mögliche Werte: • *Wahr*: Die aktuelle Position liegt innerhalb der definierten Zone. • *Falsch*: Die aktuelle Position liegt außerhalb der definierten Zone.
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

Feld	Beschreibung
	System aus, in dem die MIB-Variable gespeichert ist, dann die **MIB-Tabelle** und dann die **MIB-Variable** selber. Es werden nur die MIB-Tabellen und MIB-Variablen angezeigt, die im jeweiligen Bereich vorhanden sind.
Vergleichsbedingung	Nur für **Ereignistyp** *MIB/SNMP* Wählen Sie aus, ob die MIB-Variable *Größer* (Standardwert), *Gleich*, *Kleiner*, *Ungleich* dem in *Vergleichswert* angegebenen Wert sein oder innerhalb von *Bereich* liegen muss, um die Aktion auszulösen.
Vergleichswert	Nur für **Ereignistyp** *MIB/SNMP* Geben Sie den Wert der MIB-Variable ein.
Indexvariablen	Nur für **Ereignistyp** *MIB/SNMP* Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in der **MIB-Tabelle** eindeutig zu kennzeichnen, z.B. *ConnIfIndex*. Aus der Kombination von **Indexvariable** (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und **Indexwert** ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags. Legen Sie weitere **Indexvariablen** mit **Hinzufügen** an.
Überwachte Schnittstelle	Nur für **Ereignistyp** *Schnittstellenstatus* und *Schnittstellenverkehr* Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.
Schnittstellenstatus	Nur für **Ereignistyp** *Schnittstellenstatus* Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen. Mögliche Werte: • *Aktiv* (Standardwert): Die Schnittstelle ist aktiv. • *Inaktiv*: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr*

Feld	Beschreibung
	Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen. Mögliche Werte: • *RX* (Standardwert): Der eingehende Datenverkehr wird überwacht. • *TX*: Der ausgehende Datenverkehr wird überwacht.
Bedingung des Schnittstellenverkehrs	Nur für **Ereignistyp** *Schnittstellenverkehr* Wählen Sie aus, ob der Wert für Datenverkehr *Größer* (Standardwert) oder *Kleiner* dem in *Übertragener Datenverkehr* angegebenen Wert sein muss, um die Aktion auszulösen.
Übertragener Datenverkehr	Nur für **Ereignistyp** *Schnittstellenverkehr* Geben Sie den gewünschten Wert für den Datenverkehr, mit dem verglichen werden soll, in **kBytes** ein. Standardwert ist *0*.
Ziel-IP-Adresse	Nur für **Ereignistyp** *Ping-Test* Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.
Quell-IP-Adresse	Nur für **Ereignistyp** *Ping-Test* Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll. Mögliche Werte: • *Automatisch* (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • *Spezifisch*: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Status	Nur für **Ereignistyp** *Ping-Test* Wählen Sie aus, ob **Ziel-IP-Adresse** *Erreichbar*

Feld	Beschreibung
	(Standardwert) oder *Nicht erreichbar* sein muss, um die Aktion auszulösen.
Intervall	Nur für **Ereignistyp** *Ping-Test* Geben Sie die Zeit in **Sekunden** ein, nach der erneut ein Ping gesendet werden soll. Standardwert ist *60* Sekunden.
Versuche	Nur für **Ereignistyp** *Ping-Test* Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis **Ziel-IP-Adresse** als *Nicht erreichbar* gilt. Standardwert ist *3*.
Überwachtes Zertifikat	Nur für **Ereignistyp** *Lebensdauer eines Zertifikats* Wählen Sie das Zertifikat aus, dessen Gültigkeit überprüft werden soll.
Verbleibende Gültigkeitsdauer	Nur für **Ereignistyp** *Lebensdauer eines Zertifikats* Geben Sie den gewünschten Wert für die noch verbleibende Gültigkeit des Zertifikats in Prozent ein.

Felder im Menü Zeitintervall auswählen

Feld	Beschreibung
Zeitbedingung	Nur für **Ereignistyp** *Zeit* Wählen Sie zunächst die Art der Zeitangabe in **Bedingungstyp** aus. Mögliche Werte: • *Wochentag*: Wählen Sie in **Bedingungseinstellungen** einen Wochentag aus. • *Perioden* (Standardwert): Wählen Sie in **Bedingungseinstellungen** einen bestimmten Turnus aus. • *Tag des Monats*: Wählen Sie in **Bedingungseinstellungen** einen bestimmten Tag im Monat aus. Mögliche Werte für **Bedingungseinstellungen** bei **Bedin-**

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

25.6.2 Aktionen

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

25.6.2.1 Neu

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

Abb. 242: **Lokale Dienste->Scheduling->Aktionen->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Bezeichnung für die Aktion ein.
Befehlstyp	Wählen Sie die gewünschte Aktion aus. Mögliche Werte: • *Neustart* (Standardwert): Ihr Gerät wird neu gestartet. • *MIB/SNMP*: Für eine MIB-Variable wird der gewünschte Wert eingetragen. • *Schnittstellenstatus*: Der Status einer Schnittstelle wird verändert. • *WLAN-Status*: Nur für Geräte mit Wireless LAN. Der Status einer WLAN-SSID wird verändert. • *Softwareaktualisierung*: Es wird ein Software-Update initiiert. • *Konfigurationsmanagement*: Eine Konfigurationsdatei wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert. • *Ping-Test*: Die Erreichbarkeit einer IP-Adresse wird überprüft. • *Zertifikatverwaltung*: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • *5 GHz-WLAN-Bandscan*: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt. • *5,8 GHz-WLAN-Bandscan*: Nur für Geräte mit Wireless

Feld	Beschreibung
	LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt. • *WLC: Neuer Neighbor-Scanvorgang*: Nur für Geräte mit WLAN Controller. In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • *WLC: VSS-Status*: Nur für Geräte mit WLAN Controller. Der Status eines Drahtlosnetzwerkes wird verändert. • *Betriebsmodus*: Der Betriebsmosdus eines WLAN-Radiomoduls wird verändert.
Ereignisliste	Wählen Sie die gewünschte Ereignisliste aus, die in **Lokale Dienste**->**Scheduling**->**Auslöser** angelegt ist.
Bedingung für Ereignisliste	Wählen Sie für die gewählte Ereignisliste aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird. Mögliche Werte: • *Alle* (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten. • *Eins*: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt. • *Keiner*: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt. • *Eins nicht*: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.
Neustart des Geräts nach	Nur bei **Befehlstyp** = *Neustart* Geben Sie die Zeitspanne in Sekunden an, die nach dem Eintreten des Ereignisses gewartet werden soll, bis das Gerät neu gestartet wird. Standardwert ist *60* Sekunden.
Hinzuzufügende/zu bearbeitende MIB/ SNMP-Variable	Nur bei **Befehlstyp** = *MIB/SNMP* Wählen Sie die MIB-Tabelle aus, in der die MIB-Variable gespeichert ist, deren Wert verändert werden soll. Wählen Sie zunächst das **System** aus und dann die **MIB-Tabelle**. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vorhanden sind.

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

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

Feld	Beschreibung
	Mögliche Werte: • *Konfiguration importieren* (Standardwert) • *Konfiguration exportieren* • *Konfiguration umbenennen* • *Konfiguration löschen* • *Konfiguration kopieren* Bei **Befehlstyp** = *Zertifikatverwaltung* Wählen Sie aus, welche Aktion Sie auf eine Zertifikatsdatei anwenden möchten. Mögliche Werte: • *Zertifikat importieren* (Standardwert) • *Zertifikat löschen* • *SCEP*
Protokoll	Nur für **Befehlstyp** = *Zertifikatverwaltung* und *Konfigurationsmanagement* wenn **Aktion** = *Konfiguration importieren* Wählen Sie das Protokoll für die Dateiübertragung aus. Mögliche Werte: • *HTTP* (Standardwert) • *HTTPS* • *TFTP*
CSV-Dateiformat	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren* oder *Konfiguration exportieren* Wählen Sie aus, ob die Datei im CSV-Format übertragen werden soll. Das CSV-Format kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Standardmäßig ist die Funktion aktiv.

Feld	Beschreibung
Dateiname auf Server	Nur bei **Befehlstyp** = *Konfigurationsmanagement* Für **Aktion** = *Konfiguration importieren* Geben Sie den Namen der Datei ein, unter dem sie auf dem Server, von dem sie geholt werden soll, gespeichert ist. Für **Aktion** = *Konfiguration exportieren* Geben Sie den Namen der Datei ein, unter dem sie auf dem Server gespeichert werden soll.
Lokaler Dateiname	Nur bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration importieren*, *Konfiguration umbenennen* oder *Konfiguration kopieren* Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.
Dateiname in Flash	Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration exportieren* Wählen Sie die Datei aus, die exportiert werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration umbenennen* Wählen Sie die Datei aus, die umbenannt werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration löschen* Wählen Sie die Datei aus, die gelöscht werden soll. Bei **Befehlstyp** = *Konfigurationsmanagement* und **Aktion** = *Konfiguration kopieren* Wählen Sie die Datei aus, die kopiert werden soll.
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.

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

Feld	Beschreibung
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. 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.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Zertifikat in Konfiguration schreiben	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *Zertifikat importieren* Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus. Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungsbeschreibung	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.
SCEP-Server-URL	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie die URL des SCEP-Servers ein, z. B. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.
Subjektname	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Geben Sie einen Subjektnamen mit Attributen ein. Beispiel: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA-Name	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* 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*

Feld	Beschreibung
	Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.
Schlüsselgröße	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind *1024* (Standardwert), *2048* und *4096*.
Autospeichermodus	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert. Standardmäßig ist die Funktion aktiv.
CRL verwenden	Nur bei **Befehlstyp** = *Zertifikatverwaltung* und **Aktion** = *SCEP* Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen. Mögliche Werte: • *Auto* (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatsperrlisten-Verteilungspunkt (CDP, CRL Distribution Point) vorhanden ist, soll dieser zusätzlich zu den global im Gerät konfigurierten Sperrlisten ausgewertet werden. • *Ja*: CRLs werden grundsätzlich überprüft. • *Nein*: Keine Überprüfung von CRLs.
WLAN-Modul auswählen	Nur bei **Befehlstyp** = *5 GHz-WLAN-Bandscan*, *5,8 GHz-WLAN-Bandscan* und

Feld	Beschreibung
	Betriebsmodus Wählen Sie das WLAN-Modul aus, auf dem ein Scan des Frequenzbands durchgeführt werden soll.
WLC-SSID	Nur bei **Befehlstyp** = *WLC: VSS-Status* Wählen Sie das über den WLAN Controller verwaltete Drahtlosnetzwerk aus, dessen Status verändert werden soll.
Betriebsmodus (**Aktiv**)	Nur bei **Befehlstyp** = *Betriebsmodus* Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand *Aktiv* befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Greät abweichen.
	Nur bei **Befehlstyp** = *Betriebsmodus* Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand *Inaktiv* befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Greät abweichen.

Feld	Beschreibung
)	

25.6.3 Optionen

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

Abb. 243: **Lokale Dienste**->**Scheduling**->**Optionen**

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

Felder im Menü Scheduling-Optionen

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

25.7 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Bei Geräten der **bintec WI**-Serie können Sie die Temperatur überwachen lassen.

Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

25.7.1 Hosts

Im Menü **Lokale Dienste**->**Überwachung**->**Hosts** wird eine Liste aller überwachten Hosts angezeigt.

25.7.1.1 Bearbeiten oder Neu

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

Abb. 244: **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu**

Das Menü **Lokale Dienste**->**Überwachung**->**Hosts**->**Neu** besteht aus folgenden Feldern:

Feld im Menü Hostparameter

Feld	Beschreibung
Gruppen-ID	Wenn die Erreichbarkeit einer Gruppe von Hosts bzw. des Standard-Gateways von Ihrem Gerät überwacht werden soll, wählen Sie eine ID für die Gruppe bzw. für das Standard-Gateway. Die Gruppen-IDs werden automatisch von `0` bis `255` angelegt. 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.

Feld	Beschreibung
	Die in **Schnittstelle** konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied erreichbar ist.

Felder im Menü Trigger

Feld	Beschreibung
Überwachte IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll. Mögliche Werte: • *Standard-Gateway* (Standardwert): Das Standard-Gateway wird überwacht. • *Spezifisch*: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse des zu überwachenden Hosts ein.
Quell-IP-Adresse	Wählen Sie aus, wie die IP-Adresse ermittelt werden soll, die Ihr Gerät als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird. Mögliche Werte: • *Automatisch* (Standardwert): Die IP-Adresse wird automatisch ermittelt. • *Spezifisch*: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse ein.
Intervall	Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll. Mögliche Werte sind *1* bis *65536*. Standardwert ist *10*. Innerhalb einer Gruppe wird das kleinste **Intervall** der Gruppenmitglieder verwendet.
Erfolgreiche Versuche	Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird. Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.

Feld	Beschreibung
	Mögliche Werte sind *1* bis *65536*. Standardwert ist *3*.
Fehlgeschlagene Versuche	Geben Sie ein, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird. Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird. Mögliche Werte sind *1* bis *65536*. Standardwert ist *3*.
Auszuführende Aktion	Wählen Sie aus, welche **Aktion** ausgeführt werden soll. Für die meisten Aktionen wählen Sie eine **Schnittstelle**, auf die sich die **Aktion** bezieht. Auswählbar sind alle physikalischen und virtuellen Schnittstellen. Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (*Aktivieren*), deaktiviert (*Deaktivieren*, Standardwert) oder zurückgesetzt (*Zurücksetzen*) werden soll oder ob die Verbindung erneut aufgebaut (*Erneut wählen*) werden soll. Mit **Aktion** = *Überwachen* können Sie die IP-Adresse überwachen, die unter **Überwachte IP-Adresse** angegeben ist. Diese Information kann für andere Funktionen, wie die **IP-Adresse zur Nachverfolgung**, genutzt werden.

25.7.2 Schnittstellen

Im Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

25.7.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Abb. 245: **Lokale Dienste**->**Überwachung**->**Schnittstellen**->**Neu**

Das Menü **Lokale Dienste**->**Überwachung**->**Schnittstellen**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
Trigger	Wählen Sie den Status bzw. Statusübergang von **Überwachte Schnittstelle** aus, der eine bestimmte **Schnittstellenaktion** auslösen soll. Mögliche Werte: • *Schnittstelle wird aktiviert.* (Standardwert) • *Schnittstelle wird deaktiviert.*
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in **Trigger** definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in **Schnittstelle** ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: • *Aktivieren* (Standardwert): Aktivierung der Schnittstelle(n) • *Deaktivieren*: Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter **Schnittstelle** festgelegte Aktion ausgeführt werden soll. Wählbar sind alle physikalischen und virtuellen Schnittstellen

Feld	Beschreibung
	und die Optionen *Alle PPP-Schnittstellen* und *Alle IPSec-Schnittstellen*.

25.7.3 Ping-Generator

Im Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

25.7.3.1 Bearbeiten oder Neu

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

Abb. 246: **Lokale Dienste**->**Überwachung**->**Ping-Generator**->**Neu**

Das Menü **Lokale Dienste**->**Überwachung**->**Ping-Generator**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein. 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

Feld	Beschreibung
	erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in **Entfernte IP-Adresse** angegebene Adresse abgesetzt werden soll. Mögliche Werte sind *1* bis *65536*. Standardwert ist *10*.
Versuche	Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden sollen, bis die **Ziel-IP-Adresse** als *Nicht erreichbar* gilt. Standardwert ist *3*.

25.8 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 wer-

den 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* .

25.8.1 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. 247: **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.

Feld	Beschreibung
Schnittstelle ist UPnP-kontrolliert	Legen Sie fest, ob die NAT Konfiguration dieser Schnittstelle von UPnP kontrolliert wird. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

25.8.2 Allgemein

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

Abb. 248: **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 Clients beinhalteten Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients. Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.
UPnP TCP Port	Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht. Mögliche Werte sind *1* bis *65535*, der Standardwert ist *5678*.

25.9 Hotspot-Gateway

Die **Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen (mittels WLAN oder kabelgebundenem Ethernet). Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **Hotspot Solution** besteht aus einem vor Ort installierten bintec elmeg Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

Ablauf der Anmeldeprozedur am Hotspot Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein bintec elmeg Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung**->**Remote Authentifizierung**->**RADIUS**->**Neu** mit **Gruppenbeschreibung** *Standardgruppe 0*)
- bintec elmeg Hotspot Hosting (Artikelnummer 5510000198 bzw. 5510000197)
- Zugangsdaten
- Dokumentation

- Software-Lizenzierung

  Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

  - Gehen Sie auf *www.bintec-elmeg.com* zu **Service/Support** -> **Services** -> **Online Services**.

  - Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

  - Sie erhalten daraufhin die Login-Daten des Hotspot Servers.

Hinweis

Die Freischaltung kann etwa 2-3 Werktage in Anspruch nehmen.

Zugangsdaten zur Konfiguration des Gateways

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Wird von bintec elmeg GmbH festgelegt
Domain	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Network	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Server URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Terms & Condition URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt

Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Wird durch bintec elmeg individuell festgelegt
Password	Wird durch bintec elmeg individuell festgelegt

Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf *www.bintec-elmeg.com* zum Download zur Verfügung steht.

25.9.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte bintec elmeg Gateway für die **Hotspot Solution**.

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller konfigurierter Hotspot Netzwerke angezeigt.

Abb. 249: **Lokale Dienste**->**Hotspot-Gateway**->**Hotspot-Gateway**

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktieren.

25.9.1.1 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.

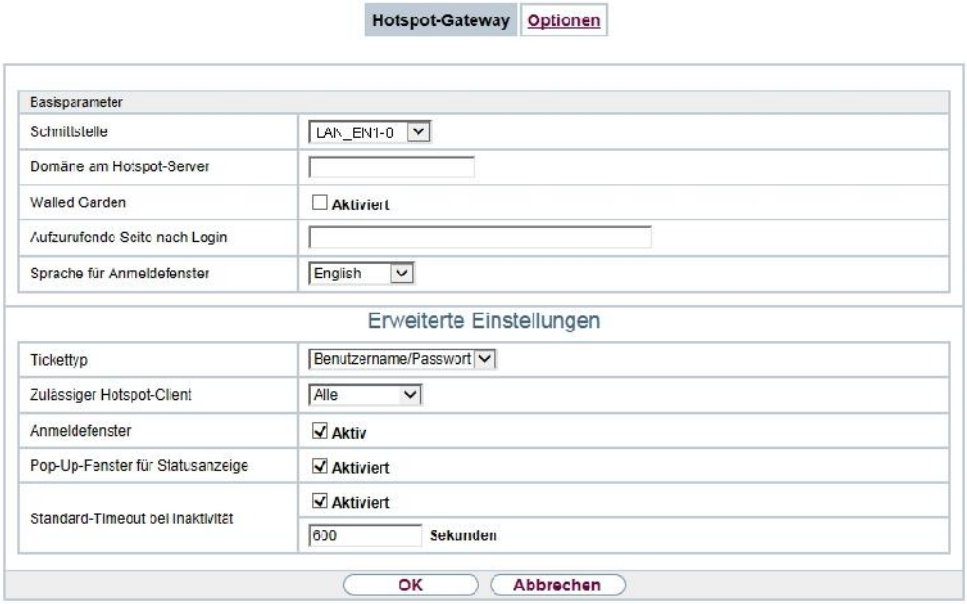


Abb. 250: **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->**

Das Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, an der das Hotspot LAN oder WLAN angeschlossen ist. Bei Betrieb über LAN tragen Sie hier die Ethernet-Schnittstelle ein (z. B. die en1-0). Bei Betrieb über WLAN muss die WLAN-Schnittstelle ausgewählt werden, an der der Access Point angeschlossen ist. **Achtung** Die Konfiguration Ihres Gerätes ist aus Sicherheitsgründen nicht über eine Schnittstelle möglich, die für den Hotspot konfiguriert ist. Wählen Sie hier daher sorgfältig die Schnittstelle aus, die Sie für den Hotspot nutzen wollen! Wenn Sie hier die Schnittstelle auswählen, über die die aktuelle Konfigurationssitzung stattfindet, geht die aktuelle Verbindung verloren. Sie müssen sich dann über eine erreichbare, nicht für den Hotspot konfigurierte Schnittstelle

Feld	Beschreibung
	zur weiteren Konfiguration Ihres Geräts erneut anmelden.
Domäne am Hotspot-Server	Geben Sie den Domänennamen ein, der bei der Einrichtung des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.
Walled Garden	Aktivieren Sie diese Funktion, wenn Sie einen abgegrenzten und kostenfreien Bereich von Webseiten (Intranet) definieren wollen. Standardmäßig ist die Funktion deaktiviert.
Walled Network / **Netzmaske**	Nur wenn **Walled Garden** aktiviert ist. Geben Sie die Netzadresse des **Walled Network** und die entsprechende **Netzmaske** des Intranet-Servers ein. Für den aus **Walled Network** / **Netzmaske** resultierenden Adressraum benötigen die Clients keine Authentifizierung. Beispiel: Geben Sie 192.168.0.0 / 255.255.255.0 ein, sind alle IP-Adressen von 192.168.0.0 bis 19.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IP-Adresse 192.168.0.1 frei.
Walled Garden URL	Nur wenn **Walled Garden** aktiviert ist. Geben Sie die **Walled Garden URL** des Intranet-Servers ein. Frei zugängliche Webseiten müssen über diese Adresse erreichbar sein.
Geschäftsbedingungen	Nur wenn **Walled Garden** aktiviert ist. Tragen Sie in das Eingabefeld **Geschäftsbedingungen** die Adresse der AGB´s auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. http://www.webserver.de/agb.htm. Die Seite muss im Adressraum des Walled Garden-Networks liegen.
Zusätzliche, frei zugängliche Domänennamen	Nur wenn **Walled Garden** aktiviert ist. Fügen Sie mit **Hinzufügen** weitere URLs oder IP-Adressen hin-

Feld	Beschreibung
	zu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.
Aufzurufende Seite nach Login	Hier können Sie eine URL angeben, zu der ein Benutzer umgeleitet wrd, wenn er sich bei der Hotspot-Lösung angemeldet hat.
Sprache für Anmeldefenster	Hier können Sie die Sprache für die Start/Login-Seite auswählen. Folgende Sprachen werden unterstützt: *English*, *Deutsch*, *Italiano*, *Français*, *Español*, *Português* und *Nederlands* . Die Sprache kann auf der Start/Login-Seite selbst jederzeit umgeschaltet werden.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Tickettyp	Wählen Sie den Tickettyp aus. Mögliche Werte: • *Voucher*: Nur der Benutzername muss eingegeben werden. Definieren Sie im Eingabefeld ein Standardpasswort. • *Benutzername/Passwort* (Standardwert): Benutzername und Passwort müssen eingegeben werden.
Zulässiger Hotspot-Client	Hier legen Sie fest, welche Art von Benutzern sich am Hotspot anmelden dürfen. Mögliche Werte: • *Alle*: Alle Clients werden zugelassen. • *DHCP-Client*: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.
Anmeldefenster	Aktivieren oder deaktivieren Sie das Anmeldefenster. Das Anmeldefenster auf der HTML-Startseite besteht aus zwei Frames. Wenn die Funktion aktiviert ist, wird auf der linken Seite das An-

Feld	Beschreibung
	melde-Formular angezeigt. Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt. Standardmäßig ist die Funktion aktiv.
Pop-Up-Fenster für Statusanzeige	Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet. Standardmäßig ist die Funktion aktiv.
Standard-Timeout bei Inaktivität	Aktivieren oder deaktivieren Sie den **Standard-Timeout bei Inaktivität** Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet. Standardmäßig ist die Funktion aktiv. Standardwert ist *600* Sekunden.

25.9.2 Optionen

Im Menü **Lokale Dienste**->**Hotspot-Gateway**->**Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

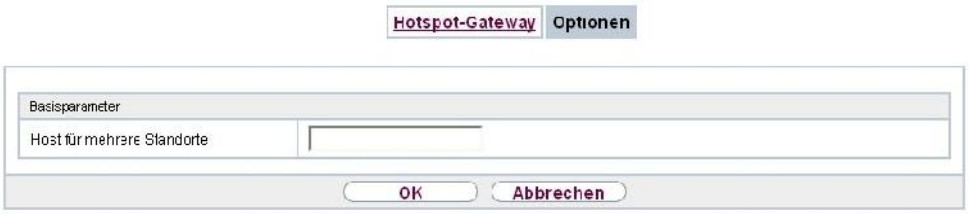


Abb. 251: **Lokale Dienste**->**Hotspot-Gateway**->**Optionen**

Das Menü **Lokale Dienste**->**Hotspot-Gateway**->**Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Host für mehrere Standorte	Wenn für einen Kunden auf dem Hotspot Server mehrere Standorte (Filialen) eingerichtet wurden, geben Sie hier den

Feld	Beschreibung
	Wert des NAS-Identifiers (RADIUS-Server Parameter) ein, der für diesen Standort auf dem Hotspot Server eingetragen wurde.

25.10 Wake-On-LAN

Mit der Funktion **Wake-On-LAN (WOL)** können Sie ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten. Die Netzwerkkarte muss weiterhin mit Strom versorgt werden, auch wenn der Computer ausgeschaltet ist. Sie können die Bedingungen, die zum Versenden des sog. Magic Packets erfüllt sein müssen, über Filter und Regelketten definieren sowie diejenigen Schnittstellen auswählen, die auf die definierten Regelketten hin überwacht werden sollen. Die Konfiguration der Filter und Regelketten entspricht weitgehend der Konfiguration von Filtern und Regelketten im Menü **Zugriffsregeln**.

25.10.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

25.10.1.1 Bearbeiten oder Neu

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

Abb. 252: **Lokale Dienste**->**Wake-On-LAN**->**Wake-on-LAN-Filter**->**Neu**

Das Menü **Lokale Dienste**->**Wake-On-LAN**->**Wake-on-LAN-Filter**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: • *activity* • *apple-qt* • *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* Standardwert ist *Beliebig*.
Protokoll	Wählen Sie ein Protokoll aus. Die Option *Beliebig* (Standardwert) passt auf jedes Protokoll.
Typ	Nur für **Protokoll** = *ICMP* Wählen Sie einen Typ aus. Mögliche Werte: *Beliebig*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Siehe RFC 792. 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.

Feld	Beschreibung
	• *Beliebig* (Standardwert): Das Filter passt auf alle TCP-Pakete.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Nur für **Protokoll** = *TCP* oder *UDP* Geben Sie eine Quell-Port-Nummer bzw. einen Bereich von Quell-Port-Nummern ein. Mögliche Werte: • *-Alle-* (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • *Port angeben*: Geben Sie einen Ziel-Port ein. • *Portbereich angeben*: Geben Sie einen Ziel-Port-Bereich ein.
DSCP/TOS-Filter (Layer 3)	Wählen Sie die Art des Dienstes aus (TOS, Type of Service). Mögliche Werte: • *Nicht beachten* (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • *DSCP-Binärwert*: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit).

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

25.10.2 WOL-Regeln

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**WOL-Regeln** wird eine Liste aller konfigurierten WOL-Regeln angezeigt.

25.10.2.1 Bearbeiten oder Neu

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

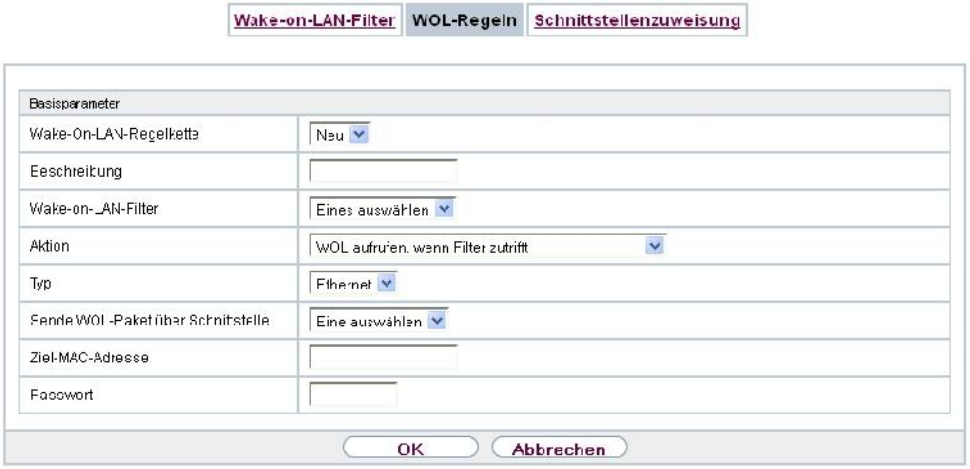


Abb. 253: **Lokale Dienste->Wake-On-LAN->WOL-Regeln->Neu**

Das Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Wake-On-LAN-Regelkette	Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen. Mögliche Werte: • *Neu* (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an. • *<Name der Regelkette>*: Zeigt eine bereits angelegte Regelkette, die Sie auswählen und bearbeiten können.
Beschreibung	Nur für **Wake-On-LAN-Regelkette** = *Neu* Geben Sie die Bezeichnung der Regelkette ein.
Wake-on-LAN-Filter	Wählen Sie ein WOL-Filter aus. Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll. Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter

Feld	Beschreibung
	im Menü **Local Services**->**Wake-On-LAN**->**WOL-Regeln** konfiguriert sein.
Aktion	Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird. Mögliche Werte: • *WOL aufrufen, wenn Filter zutrifft*: WOL ausführen, wenn der Filter zutrifft. • *Aufrufen, wenn Filter nicht zutrifft*: WOL ausführen, wenn der Filter nicht zutrifft. • *WOL verweigern, wenn Filter zutrifft*: WOL nicht ausführen, wenn der Filter zutrifft. • *WOL verweigern, wenn Filter nicht zutrifft*: WOL nicht ausführen, wenn der Filter nicht zutrifft. • *Regel ignorieren und zu nächster Regel springen*: Diese Regel wird ignoriert und die in der Kette folgende wird überprüft.
Typ	Wählen Sie aus, ob das Wake on LAN Magic Packet als UDP-Paket oder als Ethernet Frame über die Schnittstelle gesendet werden soll, die in **Sende WOL-Paket über Schnittstelle** festgelegt wird.
Sende WOL-Paket über Schnittstelle	Wählen Sie die Schnittstelle aus, über die das Wake on LAN Magic Packet gesendet werden soll.
Ziel-MAC-Adresse	Nur für **Action** = *WOL aufrufen, wenn Filter zutrifft* und *Aufrufen, wenn Filter nicht zutrifft* Geben Sie die MAC-Adresse desjenigen Netzwerkgerätes ein, das mittels WOL aktiviert werden soll.
Passwort	Nur für **Action** = *WOL aufrufen, wenn Filter zutrifft* und *Aufrufen, wenn Filter nicht zutrifft* Wenn das Netzwerkgerät, das aktiveirt werden soll, die Funktion "SecureOn" unterstützt, geben Sie hier das entsprechende Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.

25.10.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten einzelnen Schnittstellen zugeordnet, die auf diese Regelketten hin überwacht werden.

Im Menü **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

25.10.3.1 Bearbeiten oder Neu

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

Abb. 254: **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung**->**Neu**

Das Menü **Lokale Dienste**->**Wake-On-LAN**->**Schnittstellenzuweisung**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.

Kapitel 26 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.

26.1 Diagnose

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

26.1.1 Ping-Test

Abb. 255: **Wartung**->**Diagnose**->**Ping-Test**

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an. Durch Eingabe der IP-Adresse, die getestet werden soll, in **Ping-Befehl testweise an Adresse senden** und Klicken auf die **Los**-Schaltfläche wird der Ping-Test gestartet.

26.1.2 DNS-Test

Abb. 256: **Wartung**->**Diagnose**->**DNS-Test**

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

26.1.3 Traceroute-Test

Abb. 257: **Wartung**->**Diagnose**->**Traceroute-Test**

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese errreichbar ist. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an. Durch Eingabe der Adresse, die getestet werden soll, in **Traceroute-Adresse** und Klicken auf die **Los**-Schaltfläche wird der Traceroute-Test gestartet.

26.2 Software &Konfiguration

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

26.2.1 Optionen

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

Jede neue Systemsoftware beinhaltet neue Funktionen, bessere Leistung und bei Bedarf Fehlerkorrekturen der vorhergehenden Version. Die aktuelle Systemsoftware finden Sie unter *www.bintec-elmeg.com* . Hier finden Sie auch aktuelle Dokumentationen.

Wichtig

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

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

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

Flash

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

RAM

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

Aktionen

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

Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden. So können Sie mit den Aktionen "Konfiguration exportieren", "Konfiguration mit Statusinformationen exportieren" und "Konfiguration laden" Dateien sichern bzw. einspielen. Wenn Sie mit der Aktion "Konfiguration exportieren" oder "Konfiguration mit Statusinformationen exportieren" eine Konfigurationsdatei sichern wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll.

Achtung

Sollten Sie über die SNMP-Shell mit dem Kommando `put` eine Konfigurationsdatei in einem alten Format gesichert haben, kann ein Wiedereinspielen auf das Gerät nicht garantiert werden. Daher wird das alte Format nicht mehr empfohlen.

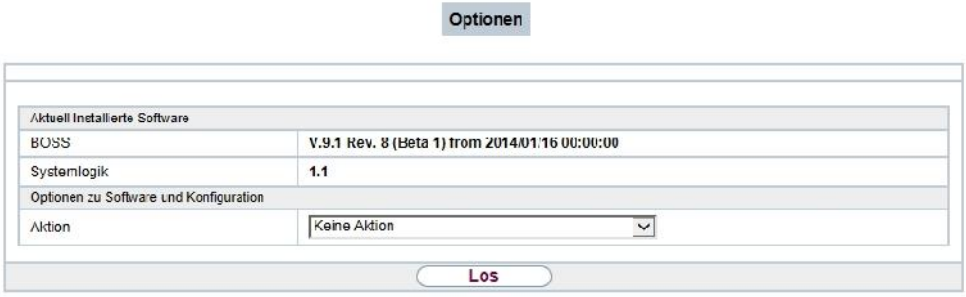


Abb. 258: **Wartung->Software &Konfiguration->Optionen**

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

Felder im Menü Aktuell Installierte Software

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

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	Wählen Sie die Aktion aus, die Sie ausführen möchten. Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden. Mögliche Werte: • *Keine Aktion* (Standardwert): • *Konfiguration exportieren*: Die Konfigurationsdatei **Aktueller Dateiname im Flash** wird zu Ihrem lokalen Host transferiert. Wenn Sie die **Los**-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.

Feld	Beschreibung
	• *Konfiguration importieren*: Wählen Sie in **Dateiname** eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken auf **Los** wird die Datei zunächst unter dem Namen *boot* in den Flash-Speicher des Geräts geladen. Zum Aktivieren müssen Sie das Gerät neu starten. Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben! • *Konfiguration kopieren*: Die Konfigurationsdatei im Feld **Name der Quelldatei** wird als **Name der Zieldatei** gespeichert. • *Konfiguration löschen*: Die Konfiguration im Feld **Datei auswählen** wird gelöscht. • *Konfiguration umbenennen*: Die Konfigurationsdatei im Feld **Datei auswählen** wird zu **Neuer Dateiname** umbenannt. • *Sicherung wiederherstellen*: Nur, wenn unter **Konfiguration speichern** mit der Einstellung *Konfiguration speichern und vorhergehende Boot-Konfiguration sichern* die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen. • *Software/Firmware löschen*: Die Datei im Feld **Datei auswählen** wird gelöscht. • *Sprache importieren*: Sie können weitere Sprachversionen des **GUI** auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von *www.bintec-elmeg.com* auf Ihren PC herunterladen und von dort aus in Ihr Gerät einspielen. • *Systemsoftware aktualisieren*: Sie können eine Aktualisierung der Systemsoftware, der ADSL-Logik und des BOOTmonitors initiieren. • *Voice Mail Wave-Dateien importieren* (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist.): Wählen Sie in **Dateiname** die Datei *vms_wavfiles.zip* aus, die Sie importieren wollen. • *Konfiguration mit Statusinformationen exportieren*: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die **Los**-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den

Feld	Beschreibung
	Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.
Aktueller Dateiname im Flash	Für **Aktion** = *Konfiguration exportieren* Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.
Zertifikate und Schlüssel einschließen	Für **Aktion** = *Konfiguration exportieren* Wählen Sie aus, ob die gewählte **Aktion** auch für Zertifikate und Schlüssel gelten soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Verschlüsselung der Konfiguration	Nur für **Aktion** = *Konfiguration exportieren*, *Konfiguration importieren*, *Konfiguration mit Statusinformationen exportieren* Wählen Sie aus, ob die Daten der gewählten **Aktion** verschlüsselt werden sollen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion aktiviert ist, können Sie in das Textfeld das **Passwort** eingeben.
Dateiname	Nur für **Aktion** = *Konfiguration importieren*, *Sprache importieren*, *Systemsoftware aktualisieren* Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit **Durchsuchen...** über den Dateibrowser aus.
Name der Quelldatei	Nur für **Aktion** = *Konfiguration kopieren* Wählen Sie die Quelldatei aus, die kopiert werden soll.
Name der Zieldatei	Nur für **Aktion** = *Konfiguration kopieren* Geben Sie den Namen der Kopie ein.

Feld	Beschreibung
Datei auswählen	Nur für **Aktion** = *Konfiguration löschen*, *Konfiguration umbenennen* oder *Software/Firmware löschen* Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.
Neuer Dateiname	Nur für **Aktion** = *Konfiguration umbenennen* Geben Sie den neuen Namen der Konfigurationsdatei ein.
Quelle	Nur für **Aktion** = *Systemsoftware aktualisieren* Wählen Sie die Quelle der Aktualisierung aus. Mögliche Werte: • *Lokale Datei* (Standardwert): Die Systemsoftware-Datei ist lokal auf Ihrem PC gespeichert. • *HTTP-Server*: Die Datei ist auf dem entfernten Server gespeichert, der in der **URL** angegeben wird. • *Aktuelle Software vom Update-Server*: Die Datei liegt auf dem offiziellen Update-Server.
URL	Nur für **Aktion** = *Systemsoftware aktualisieren* und **Quelle** = *HTTP-Server* Geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.

26.3 Aktualisierung Systemtelefone

Im Menü **Wartung**->**Aktualisierung Systemtelefone** können Sie die Software Ihrer Systemtelefone aktualisieren.

Hinweis

Bevor Sie mit der Softwareaktualisierung Ihrer Systemtelefone beginnen, müssen Sie die Software im Menü **Wartung**->**Aktualisierung Systemtelefone**->**Systemsoftware-Dateien** auf Ihre SD-Karte laden.

26.3.1 elmeg Systemtelefone

Im Menü **Wartung**->**Aktualisierung Systemtelefone**->**elmeg Systemtelefone** sehen Sie eine Liste der angeschlossenen elmeg Systemtelefone. Sie können Telefone zur sofortigen Aktualisierung der Software auswählen oder Sie können die Software zeitabhängig aktualisieren lassen.

Bei einer sofortigen Aktualisierung wird keine Versionskontrolle durchgeführt.

Bei einer zeitlgesteuerten Aktualisierung wird geprüft, ob auf der SD-Karte eine neuere Version der Systemsoftware gespeichert ist als auf dem Telefon. Nur in diesem Fall wird eine Aktualisierung durchgeführt. Die Einstellung **Aktualisiere nach Zeit** bleibt nach der Aktualisierung erhalten, d.h. im konfigurierten Zeitraum wird täglich geprüft, ob eine neuere Version der Systemsoftware auf der SD-Karte verfügbar ist.

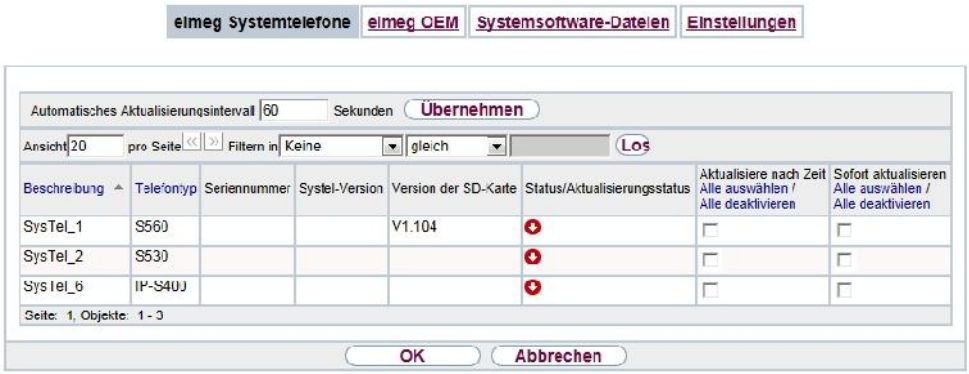


Abb. 259: **Wartung**->**Aktualisierung Systemtelefone**-> **elmeg Systemtelefone**

Werte in der Liste elmeg Systemtelefone

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung an, die für das Systemtelefon eingetragen ist.
Telefontyp	Zeigt den Typ des Systemtelefons an.
Seriennummer	Zeigt die Seriennummer des Systemtelefons an.
Systel-Version	Zeigt die Softwareversion auf dem Systemtelefon an.
Version der SD-Karte	Zeigt die Version der gesteckten SD-Karte.

Feld	Beschreibung
Status/ Aktualisierungsstatus	Zeigt den Status des Systemtelefons bzw. eine Fortschrittsanzeige während eines Aktualisierungsvorgangs an.  kennzeichnet ein Systemtelefon, das angeschlossen ist und dessen Systemsoftware von Ihrer Telefonanlage unterstützt wird.  kennzeichnet ein Systemtelefon, das entweder nicht angeschlossen ist oder dessen Systemsoftware nicht von Ihrer Telefonanlage unterstützt wird.  kennzeichnet eine Aktualisierung, die aktuell nicht durchgeführt wird, weil die Anzahl der gleichzeitig möglichen Aktualisierungsvorgänge momentan überschritten ist. Sobald ein anderer Aktualisierungsvorgang abgeschlossen ist, wird das Telefon im Zustand  aktualisiert. Für IP-Telefone gibt es keine Beschränkung gleichzeitger Aktualisierung der Systemsoftware. Bei ISDN-Telefonen ist die Anzahl gleichzeitger Aktualisierungen abhängig vom Ausbau des Systems. Pro digitalem Modul können zwei Telefone gleichzeitig aktualisiert werden. Falls die Systemsoftware eines Systemtelefons nicht von Ihrer Telefonanlage unterstützt wird, können Sie die Systemsoftware trotzdem aktualisieren. Während der Aktualisierung einer Systemsoftware sehen Sie eine Fortschrittsanzeige.
Aktualisiere nach Zeit	Zeigt an, ob die Software des Systemtelefons zu einem bestimmten Zeitpunkt aktualisiert werden soll. Die Funktion wird bei einem einzelnen Gerät durch Setzen eines Hakens aktiviert. Standardmäßig ist die Funktion nicht aktiv. Für alle angezeigten Geräte können Sie die Schaltflächen **Alle auswählen** bzw. **Alle deaktivieren** nutzen.
Sofort aktualisieren	Zeigt an, ob die Software des Systemtelefons sofort aktualisiert werden soll. Die Funktion wird bei einem einzelnen Gerät durch Setzen ei-

Feld	Beschreibung
	nes Hakens aktiviert. Standardmäßig ist die Funktion nicht aktiv. Für alle angezeigten Geräte können Sie die Schaltflächen **Alle auswählen** bzw. **Alle deaktivieren** nutzen.

26.3.2 elmeg OEM

Im Menü **Wartung**->**Aktualisierung Systemtelefone**->**elmeg OEM** sehen Sie eine Liste der angeschlossenen elmeg OEM-Telefone bzw. -Basisstationen. In dieser Ansicht werden - soweit vorhanden - sowohl elmeg IP1x-Telefone als auch elmeg DECT-Basisstationen angezeigt. Sie können Geräte zur sofortigen Aktualisierung der Software auswählen oder es diesen erlauben, sich grundsätzlich neue Software von der Anlage heruntzerzuladen.

Bei einer sofortigen Aktualisierung wird keine Versionskontrolle durchgeführt.

Hinweis

Beachten Sie, dass eine sofortige Aktualisierung der Software für DECT MultiCell-Systeme nur über den Web-Konfigurator des Systems verfügbar ist und nicht über das GUI der Telefonanlage initiiert werden kann.

Abb. 260: **Wartung**->**Aktualisierung Systemtelefone**->**elmeg OEM**

Werte in der Liste elmeg OEM

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung an, die für das Systemtelefon eingetragen ist.

Feld	Beschreibung
Telefontyp	Zeigt den Typ des Systemtelefons an.
MAC-Adresse	Zeigt die MAC-Adresse des Systemtelefons an.
Telefon-Version	Zeigt die Softwareversion des Telefons.
Version der SD-Karte	Zeigt die Version der gesteckten SD-Karte.
Status/ Aktualisierungsstatus	Zeigt den Status des Systemtelefons bzw. eine Fortschrittsanzeige während eines Aktualisierungsvorgangs an. kennzeichnet ein Systemtelefon, das angeschlossen ist und dessen Systemsoftware von Ihrer Telefonanlage unterstützt wird. kennzeichnet ein Systemtelefon, das entweder nicht angeschlossen ist oder dessen Systemsoftware nicht von Ihrer Telefonanlage unterstützt wird. Für IP-Telefone gibt es keine Beschränkung gleichzeitger Aktualisierung der Systemsoftware. Falls die Systemsoftware eines Systemtelefons nicht von Ihrer Telefonanlage unterstützt wird, können Sie die Systemsoftware trotzdem aktualisieren. Während der Aktualisierung einer Systemsoftware sehen Sie eine Fortschrittsanzeige.
Aktualisierung erlaubt	Zeigt an, ob angschlossene Telefone sich selbständig neue Software von der Anlage herunterladen können. Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** bzw. **Alle deaktivieren** markieren.
Sofort aktualisieren	Zeigt an, ob die Software des Systemtelefons sofort aktualisiert werden soll. Die Funktion wird bei einem einzelnen Gerät durch Setzen eines Hakens aktiviert. Standardmäßig ist die Funktion nicht aktiv. Für alle angezeigten Geräte können Sie die Schaltflächen **Alle auswählen** bzw. **Alle deaktivieren** nutzen.

26.3.3 Systemsoftware-Dateien

Im Menü **Wartung**->**Aktualisierung Systemtelefone**->**Systemsoftware-Dateien** sehen Sie die Systemsoftware-Dateien, die aktuell auf Ihrer SD-Karte verfügbar sind. Sie können weitere Dateien auf die SD-Karte laden.

Hinweis

Aktuelle Systemsoftware-Dateien finden Sie im Download-Bereich unter *www.bintec-elmeg.com* .

Für DECT-Systeme steht eine ZIP-Datei zur Verfügung, die Systemsoftware-Dateien und für **elmeg DECT150** auch Sprachdateien enthält.

Hinweis

Pro Telefontyp kann eine Version der Systemsoftware-Datei auf der SD-Karte gespeichert werden.

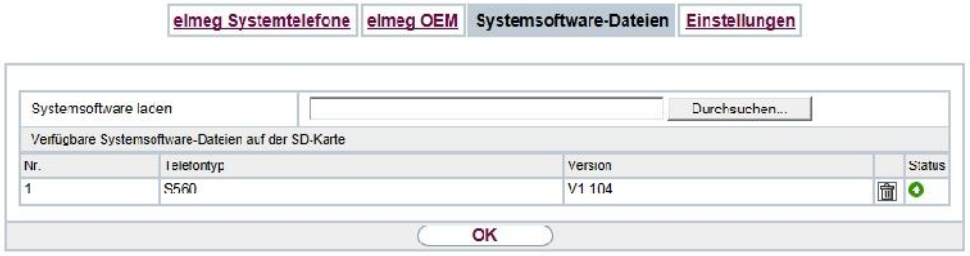


Abb. 261: **Wartung**->**Aktualisierung Systemtelefone**->**Systemsoftware-Dateien**

Werte in der Liste Systemsoftware-Dateien

Feld	Beschreibung
Systemsoftware laden	Speichern Sie die Systemsoftware-Dateien auf Ihrer SD-Karte.
Nr.	Zeigt die laufende Nummer der Systemsoftware-Datei auf Ihrer SD-Karte an.
Telefontyp	Zeigt den Typ des Systemtelefons an.

Feld	Beschreibung
Version	Zeigt die Version der Systemsoftware an.
Status	zeigt, dass eine Systemsoftware-Datei auf der SD-Karte im passenden Verzeichnis gespeichert ist.

26.3.4 Einstellungen

Im Menü **Wartung**->**Aktualisierung Systemtelefone**->**Einstellungen** können Sie einen Zeitraum für die zeitabhängige Aktualisierung der Systemsoftware festlegen. Sie können eine Telefonnummer hinterlegen, die verwendet werden kann, falls eine Aktualisierung der Systemsoftware fehlgeschlagen ist. Diese Telefonnummer können Sie mit dem Telefon wählen, um die Systemsoftware zu aktualisieren, wenn sich das Systemtelefon nach einer fehlgeschlagenen Aktualisierung im Boot-Modus befindet.

Abb. 262: **Wartung**->**Aktualisierung Systemtelefone**->**Einstellungen**

Das Menü **Wartung**->**Aktualisierung Systemtelefone**->**Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Zeiteinstellungen für Aktualisierung der Systemtelefon-Systemsoftware

Feld	Beschreibung
Interne Rufnummer	Nur für ISDN-Systemtelefone Geben Sie die Rufnummer des Update Servers der Telefonanlage ein, den Sie im Falle einer fehlgeschlagenen Aktualisierung der Systemsoftware vom Telefon aus anrufen wollen. Sie können die Aktualisierung in diesem Fall vom Telefon aus durchführen. Diese Rufnummer wird automatisch an das Systemtelefon übertragen, sobald sich das Telefon an der Telefonanlage anmeldet.

Feld	Beschreibung
	Nach der Übertragung wird die Nummer am Telefon unter **Menü**->**Service**->**Software-Update** angezeigt. Mit dem Drücken der **OK**-Taste steht die Nummer in der Wahlwiederholung zur Verfügung.
Systemsoftware-Aktualisierung	Legen Sie einen Zeitraum für die Aktualisierung der Systemsoftware fest. Wählen Sie dazu die **Startzeit** und die **Stoppzeit** aus.

26.4 Neustart

26.4.1 Systemneustart

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

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

Hinweis

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

Abb. 263: **Wartung**->**Neustart**->**Systemneustart**

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

Kapitel 27 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.

27.1 Systemprotokoll

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

Zusätzlich zu den intern auf Ihrem Gerät protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf Ihrem Gerät intern gespeicherte Systemprotokoll-Nachrichten gehen bei einem Neustart verloren.

Warnung

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

Syslog-Daemon

Die Erfassung der Systemprotokoll-Nachrichten wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (abrufbar im Download-Bereich unter *www.bintec-elmeg.com*).

27.1.1 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.

27.1.1.1 Neu

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

Abb. 264: **Externe Berichterstellung**->**Systemprotokoll**->**Syslog-Server**->**Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen. Mögliche Werte: • *Notfall* (höchste Priorität) • *Alarm* • *Kritisch* • *Fehler* • *Warnung*

Feld	Beschreibung
	• *Benachrichtigung* • *Informationen* (Standardwert) • *Debug* (niedrigste Priorität) Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden an den Host gesendet, d. h. dass beim Syslog-Level *Debug* sämtliche erzeugten Meldungen an den Host weitergeleitet werden.
Facility	Geben Sie die Syslog Facility auf dem Host an. Dieses ist nur erforderlich, wenn der **Log Host** ein Unix-Rechner ist. Mögliche Werte: *local0 - 7* (Standardwert) *local0*.
Zeitstempel	Wählen Sie das Format des Zeitstempels im Systemprotokoll aus. Mögliche Werte: • *Keiner* (Standardwert): Keine Systemzeitangabe. • *Zeit*: Systemzeit ohne Datum. • *Datum &Uhrzeit*: Systemzeit mit Datum.
Protokoll	Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss. Mögliche Werte: • *UDP* (Standardwert) • *TCP*
Nachrichtentyp	Wählen Sie den Nachrichtentyp aus. Mögliche Werte: • *System &Accounting* (Standardwert) • *System* • *Accounting*

27.2 IP-Accounting

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

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

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

27.2.1 Schnittstellen

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

Abb. 265: **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.

27.2.2 Optionen

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

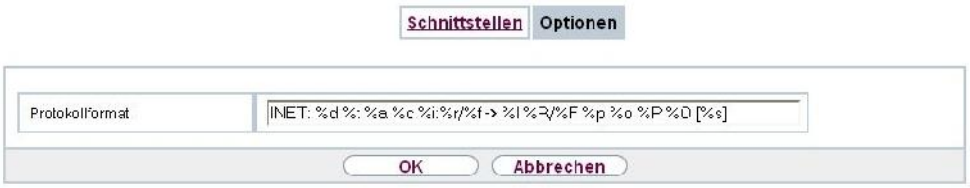


Abb. 266: **Externe Berichterstellung->IP-Accounting->Optionen**

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

Mögliche Format-Tags:

Format-Tags für IP-Accounting Meldungen

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

27.3 Benachrichtigungsdienst

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

27.3.1 Benachrichtigungsempfänger

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

27.3.1.1 Neu

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

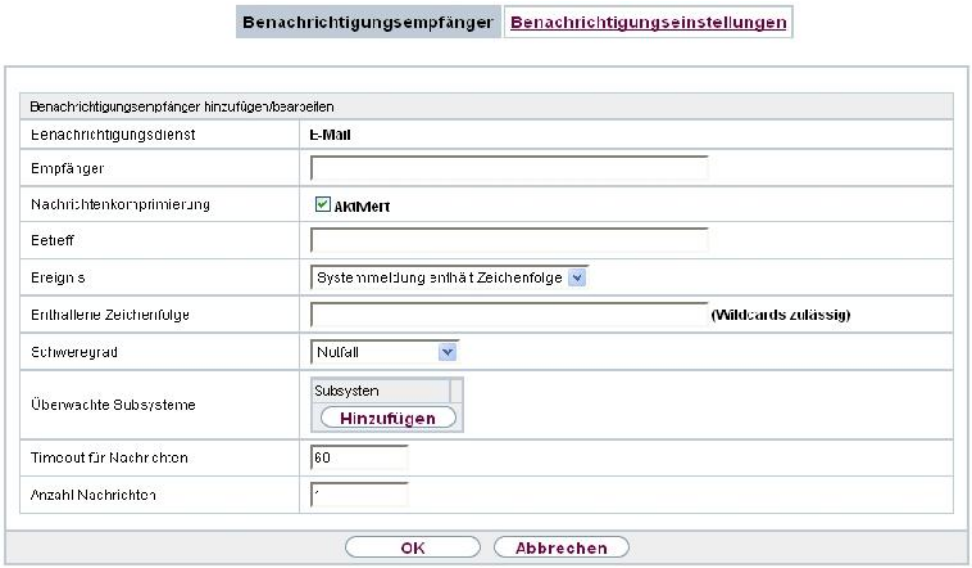


Abb. 267: **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungsempfänger->Neu**

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

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungsdienst	Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen.

Feld	Beschreibung
	Mögliche Werte: • E-Mail • SMS
Empfänger	Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Nachrichtenkomprimierung	Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse. Aktivieren oder deaktivieren Sie das Feld. Standardmäßig ist die Funktion aktiv.
Betreff	Sie können einen Betreff eingeben.
Ereignis	Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar. Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll. Mögliche Werte: • *Systemmeldung enthält Zeichenfolge* (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. • *Neuer Neighbor-AP gefunden*: Ein neuer benachbarter AP wurde gefunden. • *Neuer Rogue-AP gefunden*: Ein neuer Rough AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • *Neuer Slave-AP (WTP) gefunden*: Eine neuer unkonfigurierter AP hat sich beim WLAN Controller gemeldet. • *Verwalteter AP offline*: Ein managed AP ist nicht mehr erreichbar.
Enthaltene Zeichenfolge	Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms.

Feld	Beschreibung
	Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "*") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.
Schweregrad	Wählen Sie den Schweregrad aus, auf dem der im Feld **Enthaltene Zeichenfolge** konfigurierte String vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird. Mögliche Werte: *Notfall* (Standardwert), *Alarm*, *Kritisch*, *Fehler*, *Warnung*, *Benachrichtigung*, *Informationen*, *Debug*
Überwachte Subsysteme	Wählen Sie die Subsysteme aus, die überwacht werden sollen. Fügen Sie mit **Hinzufügen** neue Subsysteme hinzu.
Timeout für Nachrichten	Geben Sie ein, wie lange der Router nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Benachrichtigungsmails erzwungen wird. Zur Verfügung stehen Werte von *0* bis *86400*. Ein Wert von *0* deaktiviert den Timeout. Standardwert ist *60*.
Anzahl Nachrichten	Geben Sie die Anzahl der Syslog-Meldungen ein, die erreicht sein muss, ehe eine Benachrichtigungsmail für diesen Fall gesendet werden kann. Wenn Timeout konfiguriert ist, wird die Mail bei dessen Ablauf gesendet, auch wenn die Anzahl an Meldungen noch nicht erreicht ist. Zur Verfügung stehen Werte von *0* bis *99*, Standardwert ist *1*.

27.3.2 Benachrichtigungseinstellungen

Abb. 268: **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungseinstellungen**

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

Felder im Menü Basisparameter

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

Felder im Menü E-Mail-Parameter

Feld	Beschreibung
E-Mail-Adresse des Senders	Geben Sie die Mailadresse ein, die in das Absenderfeld der E-Mail eingetragen werden soll.
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der Mails verwendet werden soll.

Feld	Beschreibung
	Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Authentifizierung	Authentifizierung, die der SMTP-Server erwartet. Mögliche Werte: • *Keine* (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung. • *ESMTP*: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt. • *SMTP after POP*: Der Server verlangt, dass vor dem Versenden einer Mail Mails per POP3 von der sendenden IP aus mit dem richtigen POP3-Benutzernamen/Passwort abgerufen werden.
Benutzername	Nur wenn **SMTP-Authentifizierung** = *ESMTP* oder *SMTP after POP* Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.
Passwort	Nur wenn **SMTP-Authentifizierung** = *ESMTP* oder *SMTP after POP* Geben Sie das Passwort dieses Benutzers an.
POP3-Server	Nur wenn **SMTP-Authentifizierung** = *SMTP after POP* Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.
POP3-Timeout	Nur wenn **SMTP-Authentifizierung** = *SMTP after POP* Geben Sie ein, wie lange der Router nach dem POP3-Abruf maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird. Standardwert ist *600* Sekunden.

Felder im Menü SMS Parameter (nur für Geräte mit UMTS)

Feld	Beschreibung
SMS-Gerät	Sie können sich über Systemmeldungen per SMS informieren

Feld	Beschreibung
	lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
Maximale SMS pro Tag	Begrenzen Sie hier die Anzahl der an einem Tag versendeten SMS. Die Aktivierung von *Uneingeschränkt* erlaubt eine beliebige Anzahl an versendeten SMS. Der Standardwert beträgt 10 SMS pro Tag. Hinweis: Die Eingabe des Wertes 0 ist gleichbedeutend mit der Aktivierung von *Uneingeschränkt*.

27.4 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

27.4.1 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. 269: **Externe Berichterstellung->SNMP->SNMP-Trap-Optionen**

Das Menü **Externe Berichterstellung->SNMP->SNMP-Trap-Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
SNMP Trap Broadcasting	Wählen Sie aus, ob die Übertragung von SNMP-Traps aktiviert werden soll. Ihr Gerät sendet SNMP-Traps dann an die Broadcast-Adresse des LANs. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
SNMP-Trap-UDP-Port	Nur wenn **SNMP Trap Broadcasting** aktiviert ist. Geben Sie die Nummer des UDP-Ports ein, zu dem Ihr Gerät SNMP-Traps senden soll. Möglich ist jeder ganzzahlige Wert. Standardwert ist *162*.
SNMP-Trap-Community	Nur wenn **SNMP Trap Broadcasting** aktiviert ist. Geben Sie eine SNMP-Kennung ein. Diese muss vom SNMP-Manager mit jeder SNMP-Anforderung übergeben werden, damit sie von Ihrem Gerät akzeptiert wird. Möglich ist eine Zeichenkette mit *0* bis *255* Zeichen. Standardwert ist *SNMP-Trap*.

27.4.2 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.

27.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

Abb. 270: **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu**

Das Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

Kapitel 28 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.

28.1 Statusinformationen

In diesem Menü werden Ihnen die aktuellen Einstellungen der Endgeräte und der Teamteilnehmer angezeigt. Diese Informationen werden ständig neu ausgelesen.

28.1.1 Benutzer

Im Menü **Monitoring**->**Statusinformationen**->**Benutzer** werden die aktuellen Einstellungen für die internen Rufnummer (MSN) eines Benutzers angezeigt.

Durch Drücken der -Schaltfläche wird eine ausführliche Statistik zum jeweiligen Benutzer angezeigt.

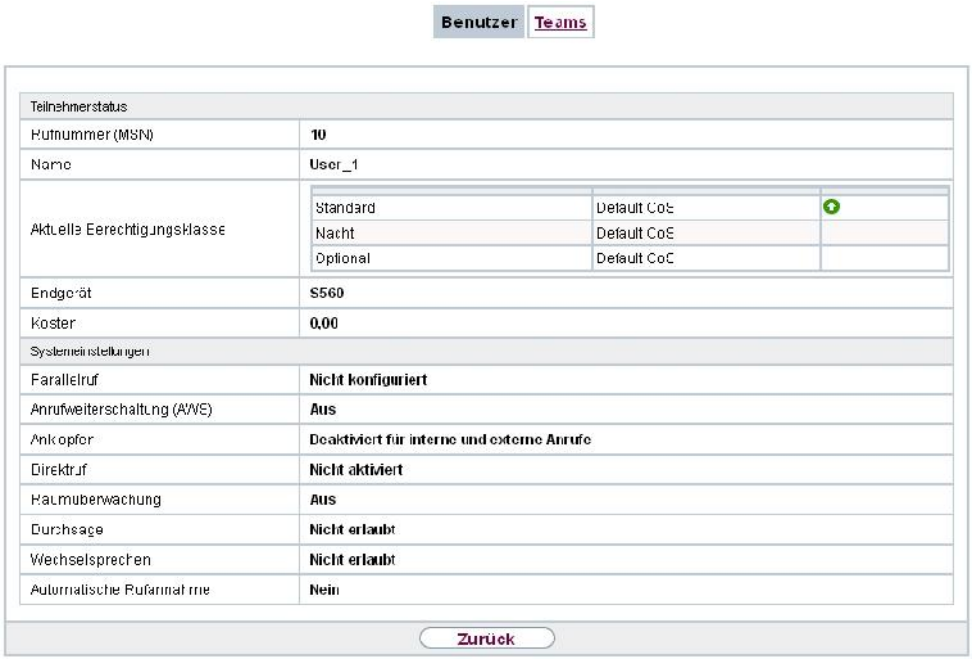


Abb. 271: **Monitoring**->**Statusinformationen**->**Benutzer**

Werte in der Liste Teilnehmerstatus

Feld	Beschreibung
Rufnummer (MSN)	Zeigt die interne Rufnummer des Benutzers an.
Name	Zeigt den für den Benutzer vergebenen Namen an. Wenn ein Voice Mail System aktiv ist, wird *Voice Mail System* angezeigt.
Aktuelle Berechtigungsklasse	Zeigt die dem Benutzer alle zugewiesenen Berechtigungsklassen an. Die aktuell Aktive Berechtigungsklasse ist entsprechend mit einem grünen Pfeil ( )gekennzeichnet.
Endgerät	Zeigt die Schnittstelle an, der dieser Teilnehmer zugewiesen ist.
Kosten	Zeigt die errechneten Kosten für die angefallenen Verbindungseinheiten an.
Status	Zeigt den Status der Schnittstelle an, an der der Teilnehmer angeschaltet ist.

Werte in der Liste Systemeinstellungen

Feld	Beschreibung
Parallelruf	Zeigt an, ob der Parallelruf für den Benutzer eingerichtet ist.
Anrufweiterschaltung (AWS)	Zeigt die zurzeit für diesen Benutzer bestehende Anrufweiterschaltung an.
Anrufschutz (Ruhe)	Zeigt an, ob der Anklopfschutz für den Benutzer eingerichtet ist. (Nur für Systemtelefone)
Anklopfen	Zeigt an, ob bei Internanrufen und / oder Externanrufen angeklopft werden darf.
Direktruf	Zeigt an, ob für den Benutzer der Direktruf nach dem Abheben des Hörers eingerichtet ist.
Raumüberwachung	Zeigt an, ob für den Benutzer die Raumüberwachung eingeschaltet ist.
Durchsage	Zeigt an, ob für den Benutzer die Durchsage erlaubt ist.
Wechselsprechen	Zeigt an, ob für den Benutzer Wechselsprechen erlaubt ist.
Automatische Rufannahme	Zeigt an, ob für den Benutzer die automatische Rufannahme eingerichtet ist.

28.1.2 Teams

Im Menü **Monitoring**->**Statusinformationen**->**Teams** werden die aktuellen Einstellungen für die Teams angezeigt.

Durch Drücken der -Schaltfläche wird eine ausführliche Statistik zu der jeweiligen Team angezeigt.

Abb. 272: **Monitoring**->**Statusinformationen**->**Teams**

Werte in der Liste Teamstatus

Feld	Beschreibung
Name	Zeigt den für das Team vergebenen Namen an.
Rufnummer (MSN)	Zeigt die interne Rufnummer für das Team an.
Zugewiesene Benutzer/eingeloggte Benutzer	Zeigt die dem Team zugewiesenen Benutzer an und wieviele dieser Benutzer eingeloggt sind.
Anrufweiterschaltung (AWS)	Zeigt die zurzeit für dieses Team bestehende Anrufweiterschaltung an.

Werte in der Liste Systemeinstellungen

Feld	Beschreibung
Aktive Variante (Tag)	Zeigt die zurzeit für das Team aktive Anrufvariante an.
Anrufvariante umschalten	Zeigt an, ob die Anrufvariante manuell, über den Kalender oder manuell und über den Kalender umgeschaltet werden kann.
Signalisieren	Zeigt die Art der Anrufsignalisierung im Team an.
Besetzt bei Besetzt (Busy on Busy)	Zeigt an, ob Besetzt bei Besetzt für das Team eingerichtet ist.
Automatische Rufannahme	Zeigt an, ob die automatische Rufannahme eingerichtet ist und welche Melodie eingespielt wird.
Abwurf bei Nichtmelden	Zeigt an, ob Abwurf bei Nichtmelden eingeschaltet ist und nach welcher Zeit der Abwurf auf welches Team erfolgt erfolgt.
Weitere Abwurffunktionen	Zeigt an, welche der Abwurffunktionen eingeschaltet ist und auf welchen Teilnehmer abgeworfen wird.

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

Werte in der Liste Erweiterte Einstellungen

Feld	Beschreibung
Zugewiesene Benutzer	Zeigt alle angemeldeten und abgemeldeteten Teilnehmer im Team an.

28.2 Internes Protokoll

28.2.1 Systemmeldungen

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

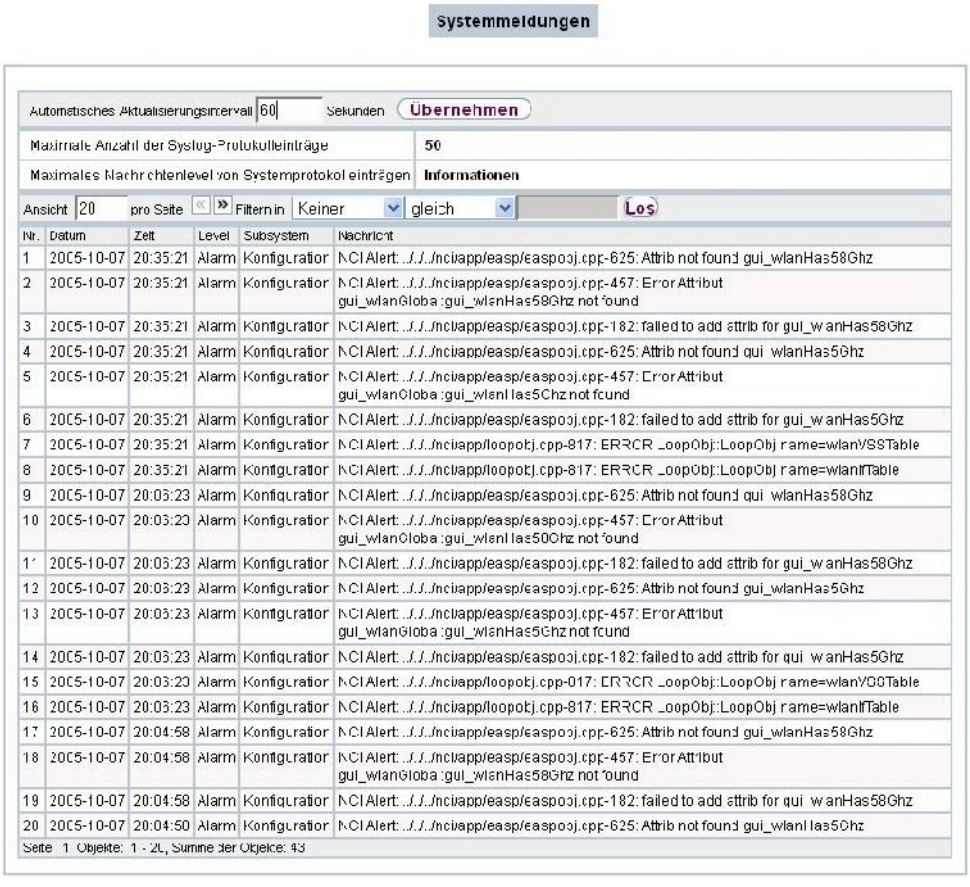


Abb. 273: **Monitoring->Internes Protokoll->Systemmeldungen**

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.

28.3 IPSec

28.3.1 IPSec-Tunnel

Im Menü **Monitoring**->**IPSec**->**IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.

Abb. 274: **Monitoring**->**IPSec**->**IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

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

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

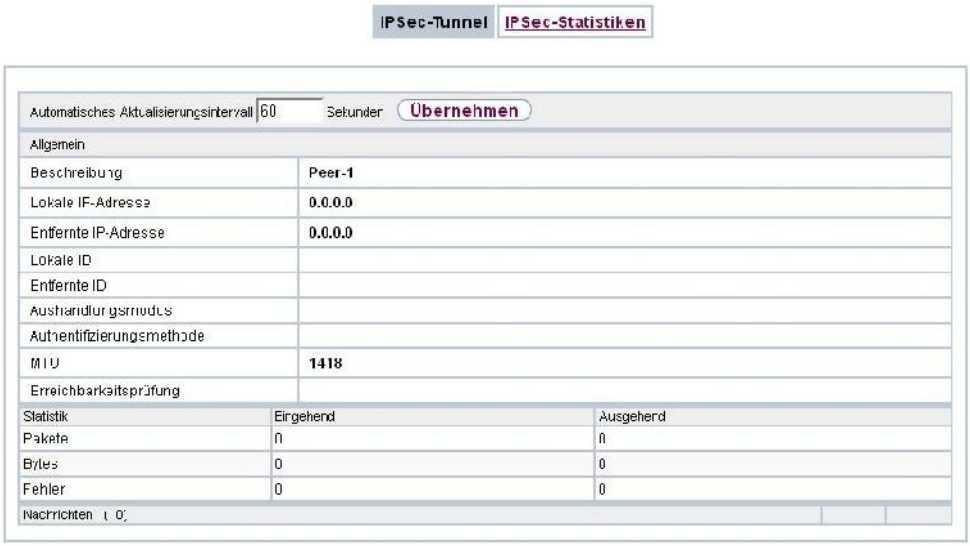


Abb. 275: **Monitoring->IPSec->IPSec-Tunnel->**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Peers an.
Lokale IP-Adresse	Zeigt die WAN-IP-Adresse Ihres Geräts an.
Entfernte IP-Adresse	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
Lokale ID	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
Entfernte ID	Zeigt die ID des Peers an.
Aushandlungsmodus	Zeigt den Aushandlungsmodus an.
Authentifizierungsmethode	Zeigt die Authentifizierungsmethode an.
MTU	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
Erreichbarkeitsprüfung	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
NAT-Erkennung	Zeigt die NAT-Erkennungsmethode an.
Lokaler Port	Zeigt den lokalen Port an.
Entfernter Port	Zeigt den entfernten Port an.
Pakete	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
Bytes	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
Fehler	Zeigt die Anzahl der Fehler an.

Feld	Beschreibung
IKE (Phase-1) SAs (x) **Rolle** / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	Zeigt die Parameter der IKE (Phase 1) SAs an.
IPSec (Phase-2) SAs (x) **Rolle** / **Algorithmus** / **Verbleibende Lebensdauer** / **Status**	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

28.3.2 IPSec-Statistiken

Im Menü **Monitoring**->**IPSec**->**IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

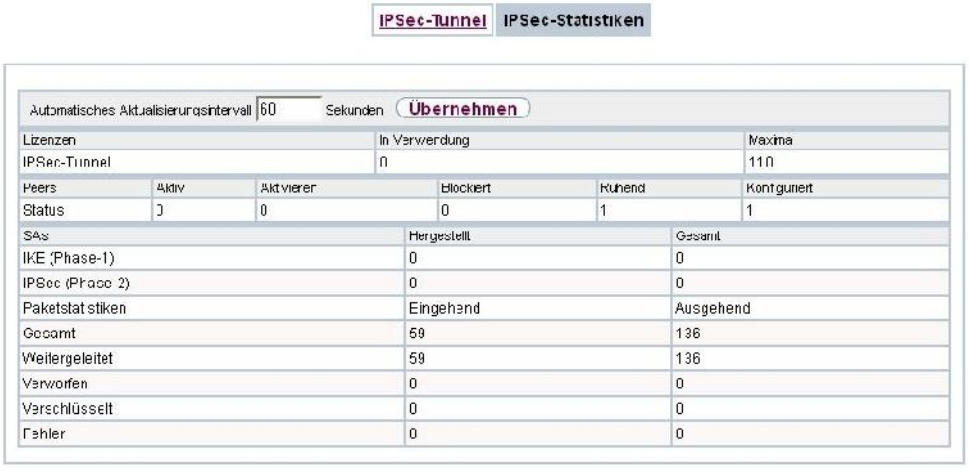


Abb. 276: **Monitoring**->**IPSec**->**IPSec-Statistiken**

Das Menü **Monitoring**->**IPSec**->**IPSec-Statistiken** besteht aus folgenden Feldern:

Feld im Menü Lizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (**In Verwendung**) und die Anzahl der maximal verwendbaren Lizenzen

Feld	Beschreibung
	(**Maximal**) an.

Feld im Menü Peers

Feld	Beschreibung
Status	Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an. • **Aktiv**: Aktuell aktive IPSec-Verbindungen. • **Aktivieren**: IPSec-Verbindungen, die sich aktuell in der Tunnelaufbau-Phase befinden. • **Blockiert**: IPSec-Verbindungen, die geblockt sind. • **Ruhend**: Aktuell inaktive IPSec-Verbindungen. • **Konfiguriert**: Konfigurierte IPSec-Verbindungen.

Felder im Menü SAs

Feld	Beschreibung
IKE (Phase-1)	Zeigt die Anzahl der aktiven Phase-1-SAs (**Hergestellt**) zur Gesamtzahl der Phase-1-SAs (**Gesamt**) an.
IPSec (Phase-2)	Zeigt die Anzahl der aktiven Phase-2-SAs (**Hergestellt**) zur Gesamtzahl der Phase-2-SAs (**Gesamt**) an.

Felder im Menü Paketstatistiken

Feld	Beschreibung
Gesamt	Zeigt die Anzahl aller verarbeiteten eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an.
Weitergeleitet	Zeigt die Anzahl der eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an, die im Klartext weitergeleitet wurden.
Verworfen	Zeigt die Anzahl der verworfenen eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an.
Verschlüsselt	Zeigt die Anzahl der durch IPSec geschützten eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an.
Fehler	Zeigt die Anzahl der eingehenden (**Eingehend**) bzw. ausgehenden (**Ausgehend**) Pakete an, bei deren Behandlung es zu Fehlern gekommen ist.

28.4 Schnittstellen

28.4.1 Statistik

Im Menü **Monitoring**->**Schnittstellen**->**Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. In der Anzeige **Transferdurchsatz** werden die Werte pro Sekunde angezeigt.

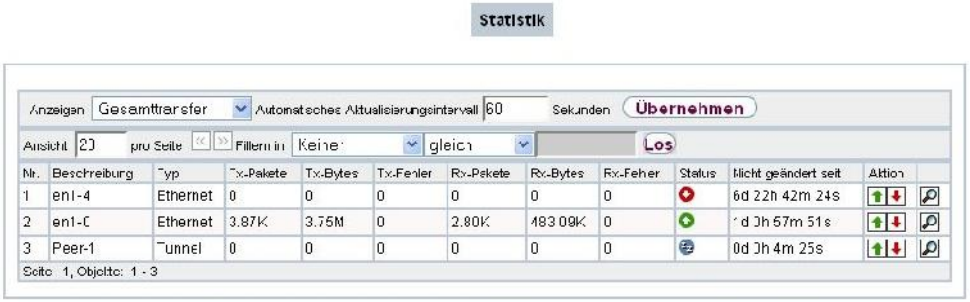


Abb. 277: **Monitoring**->**Schnittstellen**->**Statistik**

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

Werte in der Liste Statistik

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der Schnittstelle an.
Beschreibung	Zeigt den Namen der Schnittstelle an.
Typ	Zeigt den Schnittstellentyp an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.
Rx-Fehler	Zeigt die Gesamtzahl der erhaltenen Fehler an.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Nicht geändert seit	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt

Feld	Beschreibung
	zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

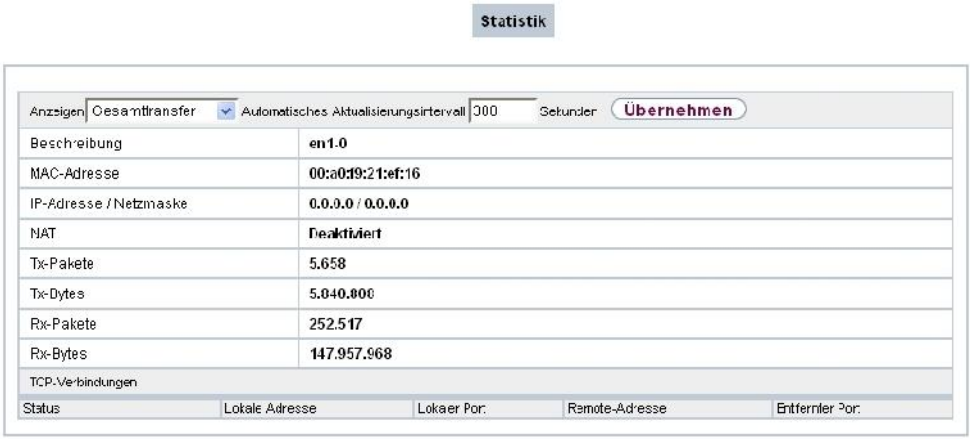


Abb. 278: **Monitoring->Schnittstellen->Statistik->**

Werte in der Liste Statistik

Feld	Beschreibung
Beschreibung	Zeigt den Namen der Schnittstelle an.
MAC-Adresse	Zeigt den Schnittstellentyp an.
IP-Adresse/Netzmaske	Zeigt die IP-Adresse und die Netzmaske an.
NAT	Zeigt an, ob NAT für diese Schnittstelle aktiviert ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.

Feld im Menü TCP-Verbindungen

Feld	Beschreibung
Status	Zeigt den Status einer aktiven TCP-Verbindung an.
Lokale Adresse	Zeigt die lokale IP-Adresse der Schnittstelle für eine aktive TCP-Verbindung an.
Lokaler Port	Zeigt den lokalen Port der IP-Adresse für eine aktive TCP-Verbindung an.

Feld	Beschreibung
Remote-Adresse	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

28.5 Bridges

28.5.1 br<x>

Im Menü **Monitoring**->**Bridges**-> **br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

Abb. 279: **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.

28.6 Hotspot-Gateway

28.6.1 Hotspot-Gateway

Im Menü **Monitoring**->**Hotspot-Gateway**->**Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

Abb. 280: **Monitoring**->**Hotspot-Gateway**->**Hotspot-Gateway**

Werte in der Liste Hotspot-Gateway

Feld	Beschreibung
Benutzername	Zeigt den Namen des Benutzers an.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Physische Adresse	Zeigt die Physische Adresse des Benutzers an.
Anmeldung	Zeigt den Zeitpunkt der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

28.7 QoS

Im Menü **Monitoring**->**QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

28.7.1 QoS

Im Menü **Monitoring**->**QoS**->**QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

Abb. 281: **Monitoring**->**QoS**->**QoS**

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.

Feld	Beschreibung
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

Kapitel 29 Benutzerzugang

Der Administrator des Systems kann den Benutzern einen individuellen Oberflächen-Konfigurationszugang einrichten. So können Sie sich als Benutzer die wichtigsten persönlichen Einstellungen anzeigen lassen und bestimmte individuell anpassen.

Um sich mit den Ihnen zugewiesenen Zugangsdaten an der Konfigurationsoberfläche anzumelden, geben Sie im Login-Fenster **Benutzername** und **Passwort** ein.

Nach erfolgreichem Anmelden wird die **Status**-Seite angezeigt. Diese enthält eine Übersicht über Ihre wichtigsten Einstellungen.

Im Menü **Telefonbuch** können Sie das **System-Telefonbuch** einsehen und Einträge in einem benutzerspezifischen Telefonbuch anlegen, bearbeiten sowie löschen.

Im Menü **Verbindungsdaten** erhalten Sie eine detaillierte Übersicht über die von Ihnen geführten und angenommenen Gespräche.

Das Menü **Einstellungen** enthält eine Übersicht über die aktuellen Einstellungen der Leistungsmerkmale **Direktruf**, **Anrufweiterschaltung (AWS)** und **Parallelruf**. Diese können Sie hier individuell anpassen. Weiterhin können Sie allgemeine Einstellungen einsehen und Zugangs- und Kontaktdaten anpassen.

Die Einstellungen der Ihnen zugewiesenen **elmeg Systemtelefone** können Sie ebenfalls einsehen und nach Ihren Bedürfnissen verändern.

Im Menü **Voice Mail System**->**Einstellungen** sehen Sie die aktuelle Konfiguration Ihrer individuellen Voice Mail Box sowie die Anzahl der hinterlassenen Nachrichten. Einige häufig benutzte Parameter der Voice Mail Box können Sie hier ändern. Das Menü **Voice Mail System**->**Nachrichten** zeigt Ihnen eine detaillierte Übersicht über alle eingegangenen Anrufe.

29.1 Status

Im Menü **Benutzerzugang**->**Status** werden die wichtigsten Einstellungen angezeigt, die vom Administrator des Systems für Sie vorgenommen wurden.

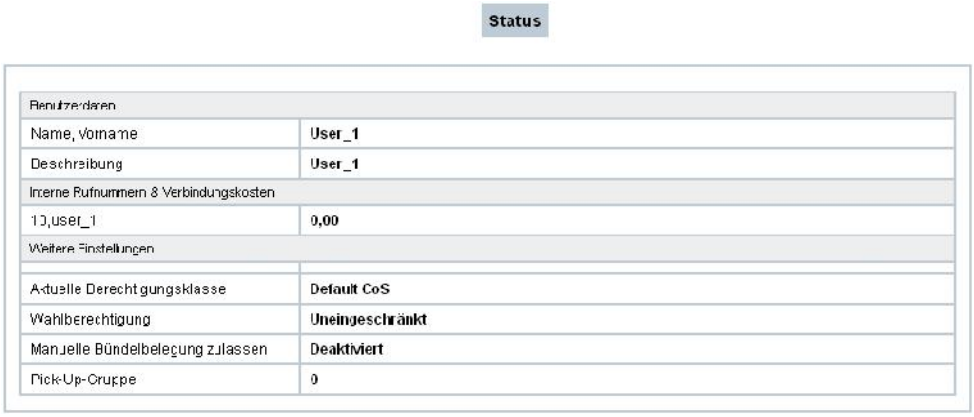


Abb. 282: **Benutzerzugang->Status**

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

Werte in der Liste Benutzerdaten

Feld	Beschreibung
Name, Vorname	Zeigt den konfigurierten Namen und ggf. Vornamen Ihres Benutzers an.
Beschreibung	Zeigt die konfigurierte zusätzliche Beschreibung für Ihren Benutzer an.

Werte in der Liste Interne Rufnummern &Verbindungskosten

Feld	Beschreibung
<Interne Rufnummer>	Zeigt die Verbindungskosten für die internen Rufnummern an, die Ihrem Benutzer zugeordnet wurden.

Werte in der Liste Weitere Einstellungen

Feld	Beschreibung
Aktuelle Berechtigungsklasse	Zeigt den Namen der Berechtigungsklasse an, zu der Ihr Benutzer zugeordnet ist.
Wahlberechtigung	Zeigt die Wahlberechtigung Ihrer Telefone an. Diese leitet sich ab aus der Einstellung für die entsprechende Benutzerklasse. Mögliche Werte: • *International* : Die Telefone haben uneingeschränkte Be-

Feld	Beschreibung
	rechtigungen für die Wahl und können alle Verbindungen selbst einleiten. • *National*: Die Telefone können außer internationalen Gesprächen alle Gespräche selbst einleiten. Beginnt eine Rufnummer mit der Kennziffer für internationale Wahl, kann diese Rufnummer nicht gewählt werden. • *Kommend*: Die Telefone sind kommend für externe Gespräche erreichbar, können aber selbst keine externen Gespräche einleiten. Interne Gespräche sind möglich. • *Region*: Die Telefone können keine nationalen und internationalen Gespräche führen. Für diese Wahlberechtigung sind 10 Ausnahmerufnummern konfigurierbar, über die eine nationale oder internationale Wahl ermöglicht werden kann. Eine Ausnahmerufnummer kann aus vollständigen Rufnummern oder Teilen einer Rufnummer (z. B. die ersten Ziffern) bestehen. • *Ort*: Die Telefone können Ortsgespräche führen. Nationale und internationale Gespräche sind nicht möglich. • *Intern*: Die Telefone sind kommend und gehend nicht für externe Gespräche berechtigt. Es können nur interne Gespräche geführt werden.
Manuelle Bündelbelegung zulassen	Zeigt an, ob Ihr Benutzer einer Berechtigungsklasse zugeordnet ist, für die die manuelle Bündelbelegung erlaubt wurde. Wenn ja, werden die zulässigen Bündel bzw. externen Anschlüsse angezeigt. Neben der allgemeinen Amtsbelegung kann ein Telefon auch gezielt ein Bündel belegen. Hierbei wird eine externe Verbindung mit der entsprechenden Kennziffer zur gezielten Belegung des Bündels eingeleitet und nicht durch die Wahl der Amtskennziffer. Um eine gezielte Bündelbelegung durchführen zu können, muss die Berechtigungsklasse die Berechtigung dafür besitzen. Diese Berechtigung kann auch Bündel umfassen, die die Berechtigungsklasse sonst nicht belegen kann. Hat ein Telefon nicht die Berechtigung zur gezielten Bündelbelegung oder ist das gewählte Bündel belegt, hört es nach Wahl der Kennziffer den Besetztton. Ist für eine Berechtigungsklasse die **Automatische Amtsholung** eingerichtet, müssen Benutzer dieser Berechtigungsklasse vor einer gezielten Bündelbelegung die Stern-Tas-

Feld	Beschreibung
	te betätigen und anschließend die externe Wahl durch die Kennziffer zur Bündelbelegung einleiten.
Pick-Up-Gruppe	Zeigt die Nummer der Gruppe an, in der Rufe herangeholt werden dürfen.

29.2 Telefonbuch

Im Menü **Telefonbuch** werden die Telefonbucheinträge getrennt nach **System-Telefonbuch** und **Benutzertelefonbuch** angezeigt. Im **Benutzertelefonbuch** kann der Benutzer bis zu 50 eigene Einträge anlegen, ändern oder löschen. Diese Einträge können ausschließlich vom jeweiligen Benutzer eingesehen werden. Die Pflege dieser Einträge erfolgt über das **GUI**.

29.2.1 System-Telefonbuch

Im **System-Telefonbuch** werden die Einträge des Gesamtsystems angezeigt, die vom Administrator angelegt wurden. Sie können sie nicht ändern.

Werte in der Liste Systemtelefonbuch

Feld	Beschreibung
Beschreibung	Zeigt eine Beschreibung des Teilnehmers an. Das **System-Telefonbuch** ist nach diesen Einträgen sortiert.
Telefonnummer	Zeigt die Telefonnummer an.
Kurzwahl	Zeigt die Kurzwahl an.
Call Through	Zeigt, ob die Telefonnummer für die Funktion **Call Through** freigegeben ist.

29.2.2 Benutzertelefonbuch

Im **Benutzertelefonbuch** werden Ihre Benutzereinträge angezeigt. Sie können Einträge hinzufügen, bearbeiten oder löschen.

29.2.2.1 Bearbeiten oder Neu

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

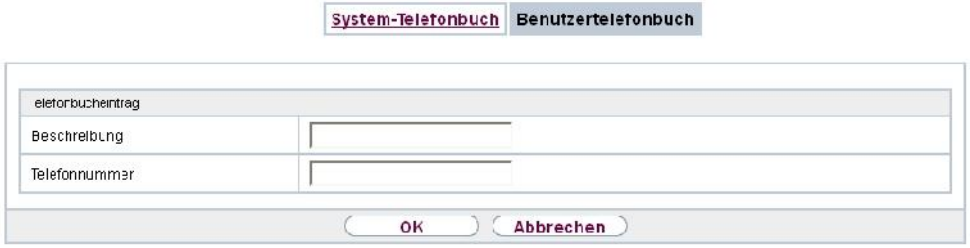


Abb. 283: **Benutzerzugang->Telefonbuch->Benutzertelefonbuch->Neu**

Das Menü **Benutzerzugang->Telefonbuch->Benutzertelefonbuch->Neu** besteht aus folgenden Feldern:

Felder im Menü Telefonbucheintrag

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den Eintrag ein. Die Sortierung im **Benutzertelefonbuch** erfolgt nach den ersten Buchstaben der Einträge.
Telefonnummer	Geben Sie die Telefonnummer ein (intern oder extern).

29.3 Verbindungsdaten

im Menü **Verbindungsdaten** werden die bisher erfassten ausgehenden und eingehenden Verbindungen Ihres Benutzers angezeigt.

29.3.1 Gehend

Abb. 284: **Verbindungsdaten->Gehend**

Das Menü **Verbindungsdaten->Gehend** besteht aus folgenden Feldern:

Werte in der Liste Gehend

Feld	Beschreibung
Datum	Zeigt das Datum der Verbindung an.
Zeit	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
Dauer	Zeigt die Dauer der Verbindung an.
Benutzer	Zeigt den Benutzer an, der angerufen hat.
Int. Rufnr.	Zeigt die interne Rufnummer des Benutzers an.
Gewählte Rufnummer	Zeigt die gewählte Rufnummer an.
Projektnummer	Zeigt ggf. die Projektnummer des Gesprächs an.
Schnittstelle	Zeigt die Schnittstelle an, über die die Verbindung nach Extern geleitet wurde.
Kosten	Zeigt die Kosten der Verbindung an, jedoch nur, wenn der Provider die ensprechenden Informationen übermittelt.

29.3.2 Kommend

Abb. 285: **Verbindungsdaten->Kommend**

Das Menü **Verbindungsdaten->Kommend** besteht aus folgenden Feldern:

Werte in der Liste Kommend

Feld	Beschreibung
Datum	Zeigt das Datum der Verbindung an.
Zeit	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
Dauer	Zeigt die Dauer der Verbindung an.
Benutzer	Zeigt den Benutzer an, der angerufen wurde.
Int. Rufnr.	Zeigt die interne Rufnummer des Benutzers an.
Externe Rufnummer	Zeigt die Rufnummer des Anrufers an.
Projektnummer	Zeigt ggf. die Projektnummer des Gesprächs an.
Schnittstelle	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.

29.4 Einstellungen

Im Menü **Einstellungen** können Sie persönliche Einstellungen zu den Leistungsmerkmalen "Direktruf", "Anrufweiterschaltung (AWS)", "Parallelruf" und "Anrufschutz" vornehmen und allgemeinen Einstellungen anpassen.

29.4.1 Einstellungen von Features

Im Menü **Einstellungen**->**Einstellungen von Features** können die Einstellungen für die Leistungsmerkmale "Direktruf", "Anrufweiterschaltung (AWS)", "Parallelruf" und "Anrufschutz" angepasst werden.

29.4.1.1 Anrufweiterschaltung (AWS)

Im Menü **Einstellungen**->**Einstellungen von Features**->**Anrufweiterschaltung (AWS)** konfigurieren Sie Weiterleitungen von kommenden Rufen auf Ihre interne Rufnummer auf die eingetragene Zielrufnummer.

Sie sind vorübergehend nicht in Ihrem Büro und möchten dennoch keinen Anruf verpassen. Mit einer Anrufweiterschaltung zu einer anderen Rufnummer, z. B. Ihr Handy, können Sie ihre Anrufe auch annehmen, wenn Sie nicht am Platz sind. Sie können Anrufe für Ihre Rufnummer zu einer beliebigen Rufnummer weiterschalten. Sie kann *Sofort*, *Bei Nichtmelden* oder *Bei Besetzt* erfolgen. Anrufweiterschaltungen *Bei Nichtmelden* und *Bei Besetzt* können gleichzeitig bestehen. Sind Sie z. B. nicht in der Nähe Ihres Telefons, wird der Anruf nach einer kurzen Zeit zu einer anderen Rufnummer (z. B. Ihr Handy) weitergeschaltet. Führen Sie bereits ein Telefongespräch an Ihrem Arbeitsplatz, erhalten weitere Anrufer möglicherweise Besetzt. Diese Anrufer können Sie mit einer Anrufweiterschaltung bei Besetzt z. B. zu einem Kollegen oder dem Sekretariat weiterschalten.

Die Anrufweiterschaltung kann zu internen Teilnehmer-Rufnummern, internen Team-Rufnummern oder externen Rufnummern erfolgen. Bei der Eingabe der Rufnummer, zu der die Anrufe weitergeschaltet werden sollen, prüft das System automatisch, ob es sich um eine interne oder um eine externe Rufnummer handelt.

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

Wählen Sie die Schaltfläche  , um Web-Konfigurator des **IP1x0**-Telefons zu gelangen. Dieser wird in der Bedienungsanleitung zum Telefon beschrieben.

Abb. 286: **Einstellungen->Einstellungen von Features->Anrufweiterschaltung (AWS)**

Das Menü **Einstellungen->Einstellungen von Features->Anrufweiterschaltung (AWS)** besteht aus folgenden Feldern:

Felder im Menü Anrufweiterschaltung (AWS)

Feld	Beschreibung
Aktive Funktion	Wählen Sie aus, ob Sie für Ihr Telefon die Funktion Anrufweiterschaltung (AWS) aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv.
Typ	Wählen Sie aus, wann kommende Anrufe auf die angegebene interne Rufnummer weitergeschaltet werden sollen. Mögliche Werte: • *Sofort* • *Bei Besetzt* • *Bei Nichtmelden* (Standardwert) • *Bei Besetzt / Bei Nichtmelden*
Ziel bei Nichtmelden	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei Nichtmelden weitergeschaltet werden sollen.
Ziel bei Besetzt	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei Besetzt weitergeschaltet werden sollen.
Ziel Sofort	Geben Sie die Rufnummer ein, auf die kommende Anrufe sofort weitergeschaltet werden sollen.

29.4.1.2 Parallelruf

Im Menü **Einstellungen**->**Einstellungen von Features**->**Parallelruf** konfigurieren Sie, welche Anrufe an Ihrem Endgerät signalisiert werden sollen.

Abb. 287: **Einstellungen**->**Einstellungen von Features**->**Parallelruf**

Das Menü **Einstellungen**->**Einstellungen von Features**->**Parallelruf** besteht aus folgenden Feldern:

Felder im Menü Anrufschutz

Feld	Beschreibung
Aktive Funktion	Wählen Sie aus, ob Sie für Ihr Telefon die Funktion Parallelruf aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv.
Externe Rufnummer	Geben Sie zu *Individuelle Rufnummer* die externe Telefonnummer ein, auf der ein Anruf parallel signalisiert werden soll. Sind eine Mobilnummer oder eine Rufnummer privat eingerichtet, werden diese unter *Konfigurierte Rufnummer privat* oder *Konfigurierte Mobilnummer* angezeigt und können ausgewählt werden.

29.4.1.3 Direktruf

Sie möchten Ihr Telefon so einrichten, dass die Verbindung zu einer bestimmten Rufnummer auch ohne die Eingabe der Rufnummer aufgebaut wird (z. B. Notruftelefon). Sie befinden sich außer Haus. Es gibt jedoch jemanden zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Haben Sie für ihr Telefon die Funktion Direktruf eingerichtet, braucht nur der Hörer des Telefons abgehoben zu werden. Nach einer in der Konfigurierung eingestellten Zeit ohne weitere Eingaben wählt das System automatisch die festgelegte Direktrufnummer.

Wählen Sie nach dem Abheben des Hörers nicht innerhalb der vorgegebenen Zeit, wird die automatische Wahl eingeleitet.

Abb. 288: **Einstellungen->Einstellungen von Features->Direktruf**

Das Menü **Einstellungen->Einstellungen von Features->Direktruf** besteht aus folgenden Feldern:

Felder im Menü Direktruf

Feld	Beschreibung
Aktive Funktion	Wählen Sie aus, ob Sie für Ihr Telefon die Funktion "Direktruf" aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv.
Rufnummer (MSN)	Wählen Sie aus, welche Nummer Sie für den Direktruf verwenden wollen. Mögliche Werte: • *Vorkonfigurierte Nummer*: Wählen Sie aus der Drop-

Feld	Beschreibung
	down-Liste die gewünschte Rufnummer aus, zu der der Direktruf aufgebaut werden soll. • *Individuelle Rufnummer*: Geben Sie in das Eingabefeld die gewünschte Rufnummer ein, zu der der Direktruf aufgebaut werden soll.

29.4.1.4 Anrufschutz

Mit dem Leistungsmerkmal „Anrufschutz" (Ruhe vor der Telefon) konfigurieren Sie, welche Anrufe an Ihrem Endgerät signalisiert werden sollen.

Abb. 289: **Einstellungen->Einstellungen von Features->Anrufschutz**

Das Menü **Einstellungen->Einstellungen von Features->Anrufschutz** besteht aus folgenden Feldern:

Felder im Menü Anrufschutz

Feld	Beschreibung
Aktive Funktion	Wählen Sie aus, ob Sie für Ihr Telefon die Funktion „Anrufschutz“ aktivieren wollen. Mit *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Anrufschutz	Mit dem Leistungsmerkmal Anrufschutz können Sie die Signalisierung von Anrufen an Ihrem Endgerät schalten. Analoge Endgeräte nutzen dafür Kennziffern des Systems. Wählen Sie aus, für welche Anrufe Sie das Leistungsmerkmal nutzen wollen. Mögliche Werte:

Feld	Beschreibung
	• *Kein Signal für interne Anrufe* • *Kein Signal für externe Anrufe* • *Keine Anrufe*

29.4.1.5 Einloggen/Ausloggen

Es ist lediglich mit Systemtelefonen möglich sich über die Funktionstaste **Einloggen/Ausloggen** aus einem Team auszuloggen. Bei Standardtelefonen muss diese Funktion der Team-Administrator manuell ausführen.

Abb. 290: **Einstellungen->Einstellungen von Features->Einloggen/Ausloggen**

Das Menü **Einstellungen->Einstellungen von Features->Einloggen/Ausloggen** besteht aus folgenden Feldern:

Felder im Menü Einloggen/Ausloggen

Feld	Beschreibung
Beschreibung	Zeigt an, welchen Teams der Benutzer angehört.
Status	Wählen Sie aus, ob das Teammitglied am Team an- oder abgemeldet sein soll. Mit Auswahl von *Angemeldet* ist die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

29.4.2 Allgemeine Einstellungen

Im Menü **Einstellungen**->**Allgemeine Einstellungen** werden die wichtigsten Einstellungen Ihres Benutzers aufgelistet. Die persönlichen Zugangsdaten (Konfigurationspasswort und Passwort für IP-Telefon) und Mobil- und Home-Office-Nummer können angepasst werden.

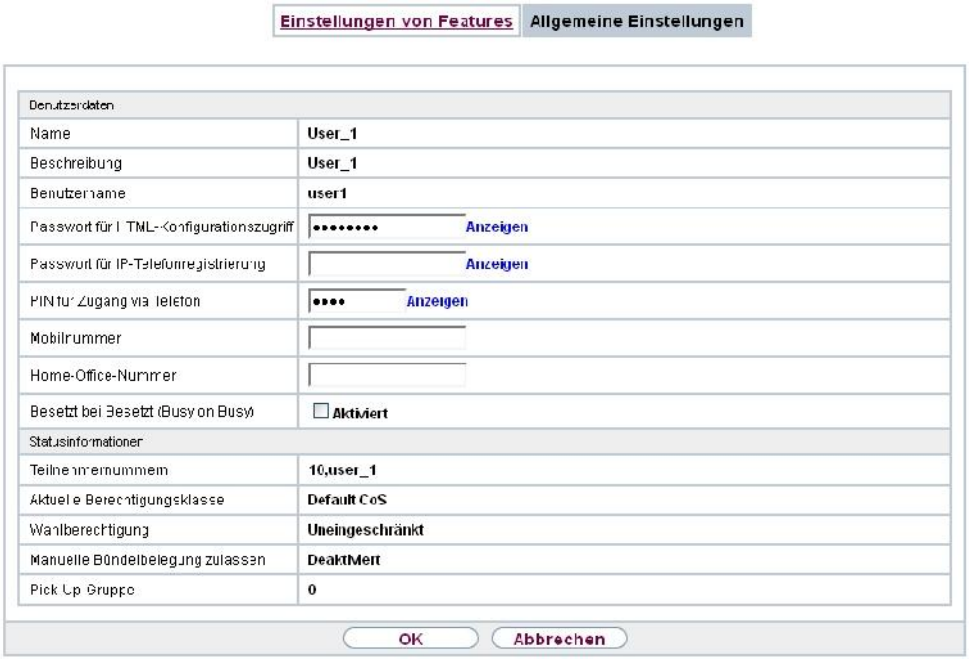


Abb. 291: **Einstellungen**->**Allgemeine Einstellungen**

Das Menü **Einstellungen**->**Allgemeine Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Benutzerdaten

Feld	Beschreibung
Name	Zeigt den Namen Ihres Benutzers an.
Beschreibung	Zeigt die zusätzliche Beschreibung Ihres Benutzers an.
Benutzername	Zeit Ihren Benutzernamen für das Login zur Benutzer-Konfigurationsoberfläche an.
Passwort für HTML-Konfigurationszugriff	Wenn Sie Ihr Passwort für den Zugang zur Benutzer-Konfigurationsoberfläche ändern wollen, geben Sie hier ein

Feld	Beschreibung
	neues Passwort ein. Zur Überprüfung können Sie das Passwort durch Klicken der Option **Anzeigen** im Klartext anzeigen lassen.
Passwort für IP-Telefonregistrierung	Wenn Sie Ihr Passwort für die Registrierung eines IP-Telefons ändern wollen, geben Sie hier ein neues Passwort ein. Zur Überprüfung können Sie das Passwort durch Klicken der Option **Anzeigen** im Klartext anzeigen lassen.
PIN für Zugang via Telefon	Wenn Sie die PIN für Ihre persönliche Voice Box ändern wollen, geben Sie hier eine neue PIN ein. Zur Überprüfung können Sie das Passwort durch Klicken der Option **Anzeigen** im Klartext anzeigen lassen.
Mobilnummer	Hier können Sie Ihre Mobilfunknummer, unter der Sie erreichbar sein sollen, eingeben.
Home-Office-Nummer	Hier können Sie Ihre Home-Office-Nummer, unter der Sie erreichbar sein sollen, eingeben.
Besetzt bei Besetzt (Busy on Busy)	Zeigt, ob für den aktuell gewählten Benutzer das Leistungsmerkmal Busy on Busy aktiviert ist. Führt ein Benutzer, für den mehrere Telefonnummern eingerichtet sind, ein Gespräch, so können Sie entscheiden, ob weitere Anrufe für diesen Benutzer signalisiert werden sollen. Ist die Funktion »Busy on Busy« für diesen Benutzer eingerichtet, so erhalten weitere Anrufer **Besetzt** signalisiert, wenn der Benutzer auf einer seiner Nummern telefoniert. Mit Auswahl von `Aktiviert` wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Statusinformationen

Feld	Beschreibung
Teilnehmernummern	Zeigt die internen Rufnummern an, die Ihnen zugewiesen wurden.
Aktuelle Berechtigungsklasse	Zeigt die Berechtigungsklasse an, der Sie aktuell zugewiesen sind.

Feld	Beschreibung
Wahlberechtigung	Zeigt Ihre Wahlberechtigung an.
Manuelle Bündelbelegung zulassen	Zeigt an, ob Sie manuell weitere Bündel für Leitungen nach extern belegen dürfen und welche.
Pick-Up-Gruppe	Zeigt die Nummer der Gruppe an, in der Rufe herangeholt werden dürfen.

29.5 Zugeordnete elmeg-Telefone

Das Menü **Zugeordnete elmeg-Telefone** zeigt die Telefone an, die Ihnen vom Administrator des Systems zugewiesen sind.

Hinweis

Das Menü **Zugeordnete elmeg-Telefone** wird nur dann angezeigt, wenn Ihnen vom Administrator bereits Systemtelefone zugewiesen sind.

29.5.1 Zugeordnete elmeg-Telefone

Das Menü **Zugeordnete elmeg-Telefone->Zugeordnete elmeg-Telefone** zeigt eine Liste mit den wichtigsten Informationen über Ihr Telefon an. Mit dem Symbol gelangen Sie auf die Benutzeroberfläche des **IP1x0**-Telefons.

Wählen Sie das Symbol , um das Benutzerpasswort des Telefons zurückzusetzen.

Abb. 292: **Zugeordnete elmeg-Telefone->Zugeordnete elmeg-Telefone**

Das Menü **Zugeordnete elmeg-Telefone->Zugeordnete elmeg-Telefone** besteht aus folgenden Feldern:

Felder im Menü Systemtelefon

Feld	Beschreibung
Benutzerpasswort	Wählen Sie aus, ob das Benutzerpasswort zurückgesetzt werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Sobald Sie die Schaltfläche **OK** wählen, wird das Passwort auf die Standardeinstellung zurückgesetzt.

29.6 elmeg Systemtelefone

Das Menü **elmeg Systemtelefone** zeigt die Systemtelefone an, die Ihnen vom Administrator des Systems zugewiesen sind.

Hinweis

Das Menü **elmeg Systemtelefone** wird nur dann angezeigt, wenn Ihnen vom Administrator bereits Systemtelefone zugewiesen sind.

29.6.1 Zugewiesene Systemtelefone

Das Systemtelefon stellt Ihnen in Verbindung mit bintec elmeg-Systemen systemtypische Leistungsmerkmale zur Verfügung. Zum Beispiel:

- Wahl aus dem Telefonbuch des Systems
- Durchsage und Wechselsprechen mit anderen Systemtelefonen am System
- Funktionstasten zur Steuerung von Leistungsmerkmalen des Systems (Anrufvarianten schalten, Ein-/Ausloggen in Teams, Linientasten, Leitungstasten). Der Status eingestellter Leistungsmerkmale kann über Leuchtdioden, die den einzelnen Funktionstasten zugeordnet sind, angezeigt werden.

Hinweis

Konfigurationsänderungen werden frühestens 30 Sekunden nach Bestätigung der Änderung mit der **Übernehmen**-Schaltfläche in die Systemtelefone übertragen.

29.6.1.1 Einstellungen

Im Menü **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Einstellungen** können Sie bestimmte Leistungsmerkmale und Funktionen für Ihre Systemtelefone freischalten.

Abb. 293: **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Einstellungen**

Das Menü **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Headset Unterstützung	Nicht für **S530** und **S560**. Wählen Sie aus, ob das Headset Anrufe automatisch entgegennehmen soll.

Feld	Beschreibung
	 **Hinweis** Wenn Sie ein Headset verwenden wollen, müssen Sie in Ihrer Telefonanlage eine Headset-Taste und eine Taste für die automatische Rufannahme konfigurieren. Am Systemtelefon müssen Sie einen Headset-Typ auswählen und die Taste für die automatische Rufannahme aktivieren.
Anklopfen	Wählen Sie aus, ob ein weiterer Anruf für dieses Telefon durch einen Anklopfton oder eine Displayanzeige signalisiert werden soll. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn **Anklopfen** aktiviert ist, wählen Sie aus, für welche Gespräche Sie Anklopfen zulassen wollen. Mögliche Werte: • *Internanrufe* • *Externanrufe* • *Intern- und Externanrufe* Entscheiden Sie unter **Anklopfwiederholung** außerdem, ob der Anklopfton oder die Displayanzeige nur einmal signalisiert oder wiederholt werden soll.
Anrufschutz (Ruhe)	Nur für Telefone der **CS4xx**-Serie, die Telefone **S530** und **S560** und das Telefon **IP-S400**. Für die Telefone **S530** und **S560** konfigurieren Sie hier lediglich die Funktion. Aktivieren Sie sie bei diesen Telefonen über die Funktionstaste *Anrufschutz*. Wählen Sie aus, ob Sie das Leistungsmerkmal Anrufschutz (Ruhe vor der Telefon) nutzen wollen. Mit diesem Leistungsmerkmal können Sie die Signalisierung von Anrufen an Ihrem Endgerät schalten. Wählen Sie aus, für welche Rufnummern Sie das Leistungs-

Feld	Beschreibung
	merkmal Anrufschutz nutzen wollen. Mögliche Werte: • *Nur erste Rufnummer* (nur **CS4xx**-Serie): Der Anrufschutz gilt nur für die erste konfigurierte MSN. • *Alle Rufnummern* (nur **CS4xx**-Serie): Der Anrufschutz gilt für alle konfigurierten MSNs. Wählen Sie aus, ob kommende Anrufe signalisiert werden sollen: • *Aus*: Anrufe werden signalisiert. • *Ein* (nur **CS4xx**-Serie): Anrufe werden nicht signalisiert. • *Nur Bestätigungston* (nur **CS4xx**-Serie): Bei einem Anruf ist einmalig ein Aufmerkton zu hören. • *Aufmerkton 1* (nur **S530** und **S560**) • *Aufmerkton 2* (nur **S530** und **S560**) • *Aufmerkton 3* (nur **S530** und **S560**) • *Aufmerkton 4* (nur **S530** und **S560**) • *Kein Aufmerkton* (nur **S530** und **S560**)

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Status-LED	Wählen Sie aus, ob und welche Ereignisse die Status-LED am Systemtelefon signalisieren soll. Mögliche Werte: • *Aus*: Die Funktion der Status-LED wird nicht genutzt. • *Anruferliste*: Die Status-LED signalisiert Anrufe und neue Nachrichten. • *Nur Nachrichten*: Die Status-LED signalisiert nur neue Nachrichten (MWI). • *Neue Nachricht* (nur **S5x0**) • *Neue Anrufe* (nur **S5x0**) • *Aktiver Anruf* (nur **S5x0**)

Feld	Beschreibung
	Die Optionen *Neue Nachricht*, *Neue Anrufe* und *Aktiver Anruf* können Sie einzeln verwenden oder beliebig kombinieren.
Softkey Telefonbuch	Nur für die Telefone der **CS4xx**-Serie Wählen Sie aus, ob mit dem Softkey Einträge aus dem System-Telefonbuch (*System*) oder aus dem Telefonbuch des Telefons (*Telefon*) aufgerufen werden.
Gesprächsanzeige	Nicht für **S5x0** Wählen Sie aus, welche Informationen während eines Telefonats im Display des Systemtelefons angezeigt werden sollen. Mögliche Werte: • *Rufnummer und Kosten oder Dauer* • *Rufnummer und Kosten* • *Rufnummer und Dauer* • *Rufnummer und Zeit* • *Nur Rufnummer* • *Nur Datum und Uhrzeit*
Eingabe während einer Verbindung	Wählen Sie aus, ob im Gesprächszustand DTMF-Signale oder Keypad-Funktionen in das System gesendet werden sollen. Während einer Verbindung können Sie durch die Eingabe von Zeichen- und Ziffernfolgen besondere Funktionen nutzen. Diese Eingaben müssen je nach zu steuernder Funktion als Keypad- oder MFV-Sequenz erfolgen. Sie können festlegen, ob in der Grundeinstellung während einer Verbindung MFV- oder Keypad-Sequenzen möglich sind. Mögliche Werte: • *DTMF* (Standardwert) • *Keypad*
Automatische Rufannahme	Wählen Sie aus, nach welcher Zeit Rufe an diesem Systemtelefon automatisch angenommen werden sollen, ohne dass Sie den Hörer abheben oder die Lautsprechertaste betätigen müssen.

Feld	Beschreibung
	Beachten Sie, dass mindestens eine Taste des Telefons mit Automatische Rufannahme belegt sein muss, um diese Funktion nutzen zu können. Mögliche Werte: • *Sofort* • *Nach 5 Sekunden* • *Nach 10 Sekunden* • *Nach 15 Sekunden* (nur **S5x0**) • *Nach 20 Sekunden* (nur **S5x0**) • *Aus* (nur **S5x0**)
Stumm nach Freisprechanwahl	Nicht für **S5x0**, **CS290**, **CS290-U** Sie können die Rufnummer eines Teilnehmers wählen, ohne dabei den Hörer abzuheben (z. B. Freisprechen). Sie haben dabei die Wahl, ob das eingebaute Mikrofon sofort oder erst nach Betätigung des entsprechenden Softkeys eingeschaltet wird. Ist das Mikrofon während der Anwahl ausgeschaltet, muss der entsprechende Softkey gedrückt werden, auch wenn die Verbindung bereits hergestellt ist. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
UUS empfangen	Wählen Sie aus, ob an diesem Telefon das Leistungsmerkmal UUS (User to User Signalling) genutzt werden kann. Mit diesem Leistungsmerkmal können Sie kurze Textnachrichten von anderen Telefonen empfangen. Innerhalb des Systems können Sie auf diese Weise schriftliche Informationen, wie z. B. *Besprechung um 09:30 Uhr* oder *Bin bis zum Montag im Urlaub*, versenden. Mögliche Werte: • *Aus, UUS blockiert*: Das Leistungsmerkmal UUS wird nicht genutzt. • *Nur intern*: Textnachrichten können nur intern empfangen werden. • *Nur extern*: Textnachrichten können nur extern empfangen werden.

Feld	Beschreibung
	• *Intern und extern* (Standardwert): Textnachrichten können intern und extern empfangen werden.
Wechselsprechen empfangen	Wählen Sie aus, ob das zugewiesene Systemtelefon Wechselsprech-Verbindungen annehmen darf. Hat das System mehrere Rufnummern so wird die Einstellung ausschließlich für die erste MSN übernommen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Durchsage	Wählen Sie aus, ob das zugewiesene Systemtelefon Durchsagen empfangen darf. Hat das System mehrere Rufnummern so wird die Einstellung ausschließlich für die erste MSN übernommen. Mit Auswahl von *Aktiviert* wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

29.6.1.2 Tasten / T400 / T400/2 / T500

Im Menü **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Tasten** wird die Konfiguration der Tasten Ihres Systemtelefons angezeigt.

Ihr Telefon verfügt über mehrere Funktionstasten, die Sie in zwei Ebenen mit verschiedenen Funktionen belegen können. Die Funktionen, die auf den Tasten programmiert werden können, sind bei den einzelnen Telefonen unterschiedlich.

Jede Funktionstaste mit automatischen Leuchtdiodenfunktionen (z. B. Leitungstasten, Linientasten) darf nur einmal je System (Telefon und Tastenerweiterungen) programmiert werden.

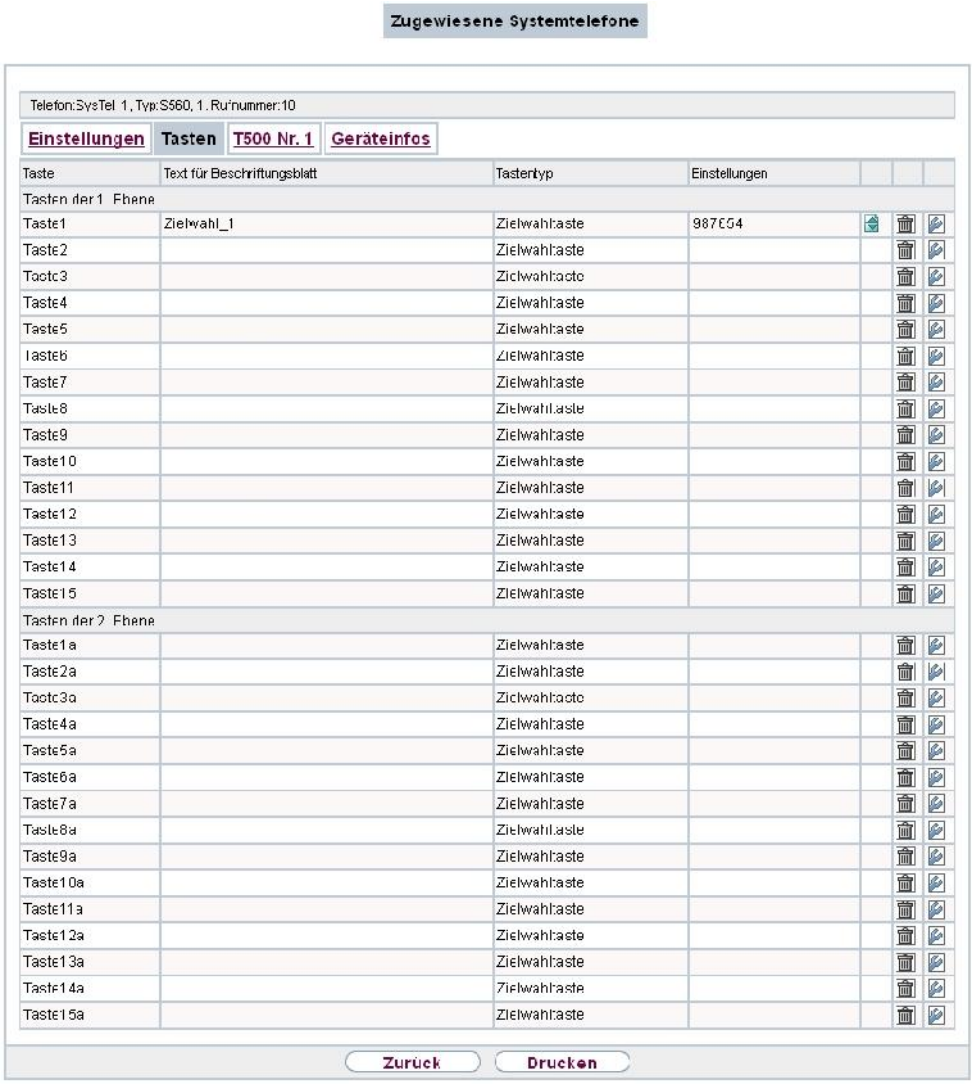


Abb. 294: **elmeg Systemtelefone->Zugewiesene Systemtelefone->Tasten**

Werte in der Liste Tasten

Feld	Beschreibung
Taste	Zeigt den Namen der Taste an.
Text für Beschriftungsblatt	Zeigt den Text an, den Sie für das Beschriftungsblatt eingegeben haben. Der Text enthält den konfigurierten Tastennamen.
Tastentyp	Zeigt den Tastentyp an.

Feld	Beschreibung
Einstellungen	Zeigt die zusätzlichen Einstellungen in einer Zusammenfassung an.

Mithilfe von **Drucken** können Sie ein Beschriftungsblatt für das Beschriftungsfeld Ihres Systemtelefons oder Ihrer Tastenerweiterung Drucken.

Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Im Popup-Menü konfigurieren Sie die Funktionen der Tasten Ihres Systemtelefons

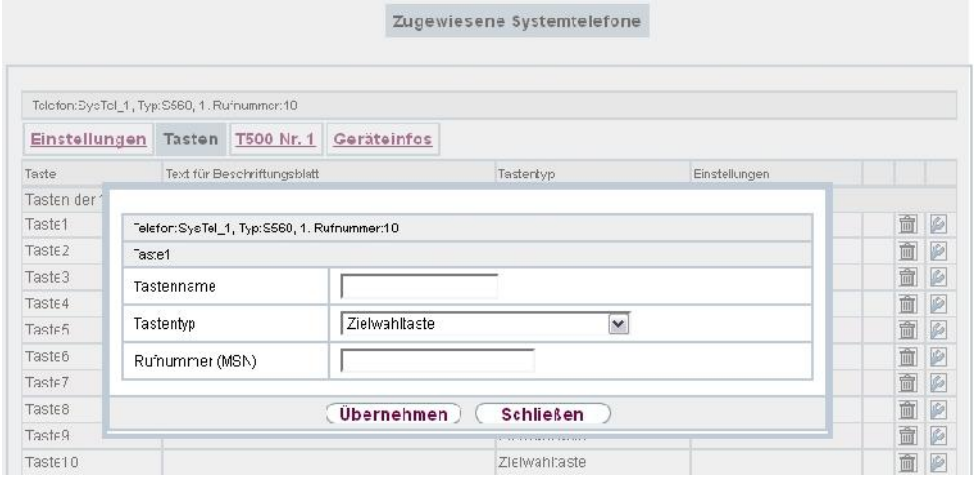


Abb. 295: **elmeg Systemtelefone->Zugewiesene Systemtelefone->Tasten-> Bearbeiten**

Folgende Funktionen können Sie mit Systemtelefonen nutzen:

- *Zielwahltaste*: Sie können auf jeder Funktionstaste eine Rufnummer speichern.
- *Zielwahltaste (DTMF)*: Sie können auf jeder Funktionstaste MFV-Sequenz speichern.
- *Zielwahltaste (Keypad)*: Sie können auf jeder Funktionstaste eine Keypadsequenz speichern.
- *Linientaste Teilnehmer*: Unter einer Linientaste können Sie eine Wahl zu einem internen Teilnehmer einrichten. Nach Betätigen der entsprechenden Taste wird das Freisprechen eingeschaltet und der eingetragene interne Teilnehmer gewählt. Wird ein Anruf an dem eingetragenen internen Teilnehmer signalisiert, können Sie diesen durch Betätigen der Linientaste heranholen.
- *Linientaste Team*: Unter einer Linientaste können Sie eine Wahl zu einem Team einrichten. Nach Betätigen der entsprechenden Taste wird das Freisprechen eingeschaltet

und das eingetragene Team wird gemäß seiner aktiven Anrufvariante gerufen. Wird ein Anruf an dem eingetragenen Team signalisiert, können Sie diesen durch Betätigen der Linientaste heranholen.

- *Leitungstaste*: Unter einer Leitungstaste wird ein ISDN-Anschluss oder ein VoIP-Provider eingerichtet. Wird diese Taste betätigt, wird automatisch Freisprechen eingeschaltet und der entsprechende ISDN-Anschluss belegt. Sie hören dann den externen Wählton. Wird ein externer Anruf an einem anderen internen Telefon signalisiert, können Sie diesen durch Betätigen der Leitungstaste heranholen.
- *Ein-/Ausloggen, Team*: Sind Sie als Teilnehmer in den Anrufvarianten eines oder mehrerer Teams eingetragen, können Sie eine Taste so einrichten, dass Sie die Rufsignalisierung Ihres Telefons kontrollieren können. Sind Sie eingeloggt, werden Teamanrufe an Ihrem Telefon signalisiert. Sind Sie ausgeloggt, werden keine Teamanrufe signalisiert.

  Das Ein-/ Ausloggen aus einem Team durch eine eingerichtete Funktionstaste ist für die im Telefon eingetragenen Rufnummern (**MSN**-1... **MSN**-9) möglich. Vor der Eingabe der Teamrufnummer müssen Sie daher den Index der Rufnummer (MSN) des Telefons wählen,die in der entsprechenden Team-Anrufvarianten eingetragen ist.
- *Durchsage Benutzer*: Sie können eine Verbindung zu einem anderen Telefon aufbauen, ohne dass diese Verbindung aktiv angenommen werden muss. Sobald das Telefon die Durchsage angenommen hat, wird die Verbindung hergestellt und die Leuchtdiode der Durchsage-Taste wird eingeschaltet. Das Beenden der Durchsage ist durch erneutes Betätigen der Durchsage-Taste oder durch Betätigen der Lautsprecher-Taste möglich. Nach Beenden der Durchsage wird die Leuchtdiode wieder ausgeschaltet.
- *Durchsage Team*: Sie können eine Durchsage zu einem Team durch eine eingerichtete Funktionstaste aufbauen. Die Funktionsweise ist wie oben beschrieben.
- *Durchsage erlauben ein/aus*: Sie können die Durchsage durch eine Funktionstaste gezielt sperren oder erlauben. Um Durchsagen verwenden zu können, müssen sie in der entsprechenden Berechtigungsklasse erlaubt sein.
- *Wechselsprechen*: Sie können eine Taste so einrichten, dass eine Verbindung zu dem angegebenen Telefon aufgebaut wird, ohne dass diese Verbindung aktiv angenommen werden muss.
- *Wechselsprechen erlauben ein/aus*: Sie können eine Taste so einrichten, dass die Funktion Wechselsprechen erlaubt bzw. untersagt ist. Um Wechselsprechen verwenden zu können, muss die Funktion in der entsprechenden Berechtigungsklasse erlaubt sein.
- *Chef* / *Sekretariat*: Sie können eine Taste als besondere Linien-Taste einrichten. Durch diese Tasten werden in den beiden Telefonen die Eigenschaften Chef-Telefon und Sekretariats-Telefon hinterlegt.
- *Umleitung Sekretariat*: Sie können eine Taste so einrichten, dass kommende Anrufe auf das Chef-Telefon automatisch auf das Sekretariat-Telefon umgeleitet werden.

- *Anrufweiterschaltung verzögert (CFNR)*: Sie können eine Taste so einrichten, dass eine verzögerte Rufumleitung für eine bestimmte Rufnummer (MSN) Ihres Telefons eingerichtet wird. Im Ruhezustand des Telefons wird durch Betätigen der Taste die Rufumleitung ein- oder ausgeschaltet. Das Einrichten einer Rufumleitung über eine programmierte Taste ist nur für die Rufnummern 1 bis 9 (MSN-1...MSN-9) des Telefons möglich. Um die Rufumleitung nutzen zu können, müssen Sie mindestens eine Rufnummer eingerichtet haben.
- *Anrufweiterschaltung sofort (CFU)*: Sie können eine Taste so einrichten, dass eine sofortige Rufumleitung für eine bestimmte Rufnummer (MSN) Ihres Telefons eingerichtet wird. Im Ruhezustand des Telefons wird durch Betätigen der Taste die Rufumleitung ein- oder ausgeschaltet. Das Einrichten einer Rufumleitung über eine programmierte Taste ist nur für die Rufnummern 1 bis 9 (MSN-1...MSN-9) des Telefons möglich. Um die Rufumleitung nutzen zu können, müssen Sie mindestens eine Rufnummer eingerichtet haben.
- *Anrufweiterschaltung bei Besetzt (CFB)*: Sie können eine Taste so einrichten, dass eine Rufumleitung bei Besetzt für eine bestimmte Rufnummer (MSN) Ihres Telefons eingerichtet wird. Im Ruhezustand des Telefons wird durch Betätigen der Taste die Rufumleitung ein- oder ausgeschaltet. Das Einrichten einer Rufumleitung über eine programmierte Taste ist nur für die Rufnummern 1 bis 9 (MSN-1...MSN-9) des Telefons möglich. Um die Rufumleitung nutzen zu können, müssen Sie mindestens eine Rufnummer eingerichtet haben.
- *Makro*: Sie können eine Taste so einrichten, dass bei Betätigen der Taste ein hinterlegtes Makro ausgeführt wird.

  Die Makro-Funktion kann nur am Telefon programmiert werden.
- *Headset* (nicht bei **S5x0**): Haben Sie an Ihrem Telefon ein Headset über eine separate Headsetbuchse angeschlossen und eingerichtet, erfolgt die Bedienung des Headsets über eine Funktionstaste. Zum Einleiten oder Annehmen von Gesprächen betätigen Sie die Headsettaste. Haben Sie bereits eine aktive Verbindung über das Headset, können Sie das Gespräch durch Betätigen der Headsettaste beenden.
- *Automatische Rufannahme*: Ihr Telefon kann Anrufe automatisch annehmen, ohne dass Sie den Hörer abheben oder die Lautsprechertaste betätigen müssen. Die automatische Rufannahme wird durch eine eingerichtete Funktionstaste ein- oder ausgeschaltet. Sie können für jede Rufnummer (»MSN-1«...»MSN-9«) eine separate Funktionstaste oder eine Funktionstaste für alle Rufnummern einrichten. Die Zeit, nach der Anrufe automatisch angenommen werden, wird einmal für alle Rufnummern des Telefons eingerichtet.
- *Bündelauswahl*: Im System können mehrere externe ISDN- oder IP-Anschlüsse zu Bündeln zusammengefasst werden. Durch eine Bündeltaste können Sie diese Anschlüsse auf einer Funktionstaste hinterlegen. Wird diese Taste betätigt, wird automatisch Freisprechen eingeschaltet und ein freier B-Kanal des entsprechenden Bündels belegt. Sie hören dann den externen Wählton.

- *Verbindungstaste* (nicht bei **S5x0**): Für die Bedienung beim Makeln können zusätzlich zu den Softkeys »Verbindung 1.. « Funktionstasten am Systemtelefon oder der Erweiterung eingerichtet werden. Es müssen mindestens zwei Verbindungstasten eingerichtet werden.
- *Hotelzimmer*: Sie können eine Taste so belegen, dass bei Betätigung der Taste der Gast ein- oder ausgecheckt wird (erste Ebene) oder das ausgewählte Hotelzimmer-Telefon gerufen wird (zweite Ebene). Sie müssen diese Taste auf der ersten Ebene einrichten, die zugehörige Taste auf der zweiten Ebene wird automatisch belegt und ihr Inhalt gegebenenfalls überschrieben.
- *Offene Rückfrage*: Der angerufene Teilnehmer geht in Rückfrage und wählt eine Kennziffer. Das Telefon ist jetzt für andere Bedienungen, z. B. eine Durchsage oder Ansage frei. Ein anderer Teilnehmer kann das Gespräch annehmen, wenn er den Hörer abhebt und die entsprechende Kennziffer für das gehaltene Gespräch wählt. Die von der TK-Anlage vorgegebenen Kennziffern können auch in die Funktionstasten eines oder mehrerer Systemtelefone eingetragen werden. Wird ein Gespräch durch Betätigen der Funktionstaste in die offene Rückfrage gelegt, wird dieses durch Blinken an den LEDs der Funktionstasten der hierfür eingerichteten Systemtelefone angezeigt. Durch Drücken der entsprechenden Funktionstaste wird das Gespräch übernommen. Dieses Leistungsmerkmal ist nur möglich, wenn nur ein Gespräch gehalten wird.
- *Nachbereitungszeit des Agent*: Sie können eine Taste so einrichten, dass beim Betätigen dieser Taste die Nachbearbeitungszeit eines Agents in einem Team Call Center ein- oder ausgeschaltet wird (erste Ebene) oder diese verlängert wird (zweite Ebene).
- *Nachtbetrieb*: Sie können eine Taste so einrichten, dass beim Betätigen dieser Taste der Nachtbetrieb ein oder ausgeschaltet wird.

Hinweis

Um den Nachbetrieb manuell wieder ausschalten zu können, muss für die Berechtigungsklasse **Anrufvarianten manuell umschalten** akiviert sein.

- *Parallelruf* (nur **S5x0**): Wenn ein Parallelruf zu einem anderen Telefon eingerichtet ist, klingelt es bei einem Anruf an beiden Anschlüssen. Das Gespräch wird dort angenommen, wo zuerst abgehoben wird.
- *Umschalttaste* (nur **S5x0**): Mit dieser Taste können Sie die Funktionen der zweiten Ebene erreichen.
- *Anrufschutz* (nur **S5x0**): Mit dieser Taste schalten Sie die Funktion Ruhe vor dem Telefon ein oder aus, die Sie unter **Endgeräte**->**elmeg Systemtelefone**->**Systemtelefon**->**Einstellungen** konfiguriert haben.

Das Menü **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Tasten**-> **Bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Telefon: Typ x

Feld	Beschreibung
Tastenname	Geben Sie einen Namen für die Taste ein, der beim Drucken der Beschriftungsschilder als Text für die entsprechende Taste verwendet wird.
Tastentyp	Die Telefone verfügen je nach Ausführung über fünf bis 15 Tasten, die in zwei Ebenen mit Funktionen belegt werden können. Die zweite Ebene der Funktionstasten erreichen Sie durch einen doppelten Tastendruck. Dieser muss in kurzem Abstand ausgeführt werden. Bei **S5x0**-Geräten können Sie alternativ die Funktionstaste *Umschalttaste* verwenden. Mit den optionalen bintec elmeg-Tastenerweiterungen stehen Ihnen weitere zweifach belegbare Funktionstasten zur Verfügung. Mögliche Werte: • *MSN-Auswahltaste* • *Zielwahltaste* • *Zielwahltaste (DTMF)* • *Zielwahltaste (Keypad)* • *Linientaste Teilnehmer* • *Linientaste Team* • *Leitungstaste* • *Ein-/Ausloggen, Team* • *Durchsage Benutzer* • *Durchsage Team* • *Durchsage Benutzer* • *Durchsage erlauben ein/aus* • *Wechselsprechen* • *Wechselsprechen erlauben ein/aus* • *Chef* • *Sekretariat* • *Umleitung Sekretariat* • *Anrufweiterschaltung verzögert (CFNR)* • *Anrufweiterschaltung sofort (CFU)* • *Anrufweiterschaltung bei Besetzt (CFB)* • *Makro* • *Headset*

Feld	Beschreibung
	• *Automatische Rufannahme* • *Bündelauswahl* • *Verbindungstaste* • *Hotelzimmer* • *Offene Rückfrage* • *Nachbereitungszeit des Agent* • *Nachtbetrieb* • *Umschalttaste* (nur **S5x0**) • *Parallelruf* (nur **S5x0**) • *Anrufschutz (Ruhe)* (nur **S5x0**)
Rufnummer (MSN)	Nur bei **Tastentyp** = *Zielwahltaste*, *Zielwahltaste (DTMF)* und *Zielwahltaste (Keypad)* Sie können auf jeder Funktionstaste eine Rufnummer, eine MFV-Sequenz oder eine Keypadsequenz speichern. Geben Sie die Rufnummer oder die Zeichen für die MFV-/ Keypadsequenz ein.
Interne Rufnummer	Bei **Tastentyp** = *Linientaste Teilnehmer* Wählen Sie die interne Rufnummer eines Benutzers aus, der bei Betätigung dieser Taste gerufen werden soll. Bei **Tastentyp** = *Durchsage Benutzer* Wählen Sie die interne Rufnummer eines Benutzers aus, an dessen Telefon eine Durchsage gesendet soll. Bei **Tastentyp** = *Ein-/Ausloggen, Team* Wählen Sie die interne Rufnummer eines Teams aus, in das bei Betätigung dieser Taste eingeloggt bzw. davon ausgeloggt werden soll. Bei **Tastentyp** = *Durchsage* Wählen Sie die interne Rufnummer eines Benutzers aus, an dessen Telefon eine Durchsage ertönen soll. Bei **Tastentyp** = *Wechselsprechen*

Feld	Beschreibung
	Wählen Sie die interne Rufnummer eines Benutzers aus, mit dem Sie Wechselgespräche führen wollen. Bei **Tastentyp** = *Anrufweiterschaltung verzögert (CFNR)*, *Anrufweiterschaltung sofort (CFU)*, *Anrufweiterschaltung bei Besetzt (CFB)* Wählen Sie die interne Rufnummer einer MSN des Telefons aus, von der aus an die angegebene Zielrufnummer weitergeleitet werden soll. Bei **Tastentyp** = *Automatische Rufannahme* Wählen Sie die interne Rufnummer dieses Telefons aus, auf der kommende Rufe automatisch angenommen werden sollen. Bei **Tastentyp** = *Hotelzimmer* Wählen Sie die interne Rufnummer eines Hotelgastes aus. Bei **Tastentyp** = *Nachbereitungszeit des Agent* Wählen Sie die interne Rufnummer eines Benutzers aus, dessen Nachbearbeitungszeit bei Betätigung dieser Taste intervallweise verändert werden soll. Bei **Tastentyp** = *Parallelruf* Wählen Sie die interne Rufnummer eines Benutzers aus, bei dem das Telefon ebenfalls klingeln soll, wenn bei Ihnen ein Anruf eingeht.
Automatische Rufannahme	Bei **Tastentyp** = *Automatische Rufannahme* Wählen Sie aus, wann ein Ruf automatisch beim eingetragenen internen Teilnehmer angenommen werden soll. Mögliche Werte: • *Sofort*: Der Ruf wird sofort automatisch angenommen. • *Nach 5 Sekunden*: Der Ruf wird nach 5 Sekunden automatisch angenommen. • *Nach 10 Sekunden*: Der Ruf wird nach 10 Sekunden automatisch angenommen. • *Nach 15 Sekunden* (nur **S5x0**): Der Ruf wird nach 15 Se-

Feld	Beschreibung
	kunden automatisch angenommen. • *Nach 20 Sekunden* (nur **S5x0**): Der Ruf wird nach 20 Sekunden automatisch angenommen. • *Aus* (nur **S5x0**): Der Ruf wird nicht automatisch angenommen.
Team	Bei **Tastentyp** = *Linientaste Team* Wählen Sie die interne Rufnummer eines Teams aus, mit dem bei Betätigung dieser Taste verbunden werden soll. Bei **Tastentyp** = *Durchsage Team* Wählen Sie die interne Rufnummer eines Teams aus, an dessen Telefon eine Durchsage gesendet soll. Bei **Tastentyp** = *Ein-/Ausloggen, Team* Wählen Sie die interne Rufnummer eines Teams aus, bei dem bei Betätigung dieser Taste ein- bzw. ausgeloggt werden soll.
Trunk-Leitung	Nur bei **Tastentyp** = *Trunk-Leitung* Wählen Sie den externen Anschluss aus, über den bei Betätigung dieser Taste eine externe Verbindung aufgebaut werden soll.
Rufnummer des Sekretariat-Telefones	Nur bei **Tastentyp** = *Chef* Wählen Sie die interne Rufnummer des Sekretariat-Telefons aus. Bei Betätigung dieser Taste wird das Sekretariat-Telefon gerufen.
Rufnummer des Chef-Telefones	Nur bei **Tastentyp** = *Sekretariat* Wählen Sie die interne Rufnummer des Chef-Telefons aus. Bei Betätigung dieser Taste wird das Chef-Telefon gerufen.
Zielrufnummer "Bei Nichtmelden"	Nur bei **Tastentyp** = *Anrufweiterschaltung verzögert (CFNR)* Geben Sie die Rufnummer ein, auf die bei Anrufweiterschaltung sofort weitergeleitet werden soll.

Feld	Beschreibung
Zielrufnummer "Sofort"	Nur bei **Tastentyp** = *Anrufweiterschaltung sofort (CFU)* Geben Sie die Rufnummer ein, auf die bei Anrufweiterschaltung bei Besetzt weitergeleitet werden soll.
Zielrufnummer "Bei besetzt"	Nur bei **Tastentyp** = *Anrufweiterschaltung bei Besetzt (CFB)* Geben Sie die Rufnummer ein, auf die bei Anrufweiterschaltung bei Nichtmelden weitergeleitet werden soll.
Trunk-Gruppeneinwahl	Nur bei **Tastentyp** = *Bündelauswahl* Wählen Sie das Bündel aus, über das eine Verbindung nach extern aufgebaut werden soll.
Wartefeld	Nur bei **Tastentyp** = *Offene Rückfrage* Wählen Sie das Wartefeld aus, in dem die aktuelle Verbindung gehalten werden soll.

Verschieben

Wählen Sie das Symbol , um konfigurierte Funktionstasten zu verschieben.

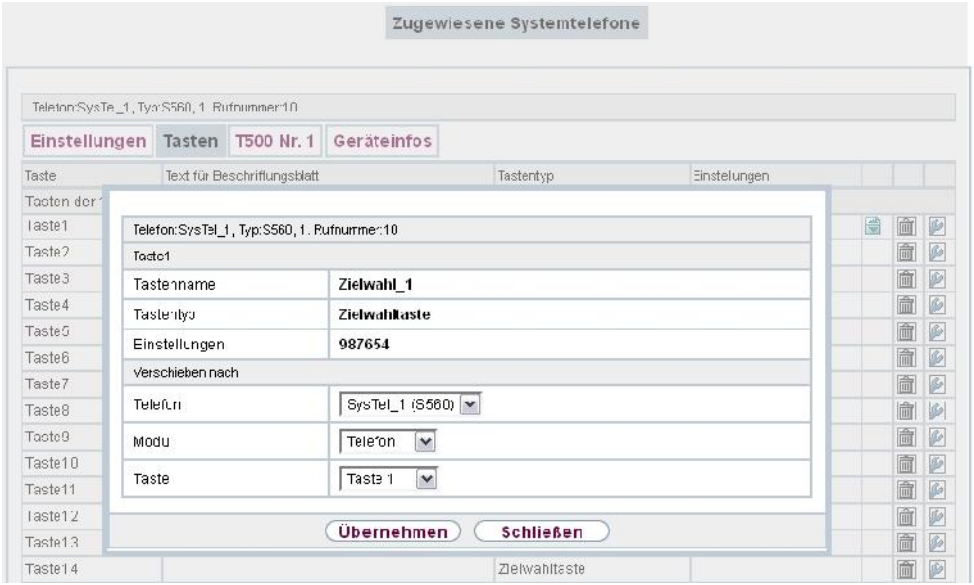


Abb. 296: **elmeg Systemtelefone->Zugewiesene Systemtelefone->Tasten->Verschieben**

Felder im Menü Telefon

Feld	Beschreibung
Tastenname	Zeigt den Namen der Taste an.
Tastentyp	Zeigt den Tastentyp an.
Einstellungen	Zeigt die zusätzlichen Einstellungen in einer Zusammenfassung an.

Felder im Menü Verschieben nach

Feld	Beschreibung
Telefon	Zeigt Ihr Systemtelefon an. Sie können im **Benutzerzugang** nur Tasten innerhalb Ihrer eigenen Telefon-Tastenerweiterung-Kombination verschieben.
Modul	Wählen Sie Telefon oder ein Tastenerweiterungsmodul aus.
Taste	Wählen Sie die Taste aus, auf die Sie die konfigurierte Funktion verschieben möchten.

29.6.1.3 Geräteinfos

Im Menü **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Geräteinfos** werden die aus dem Systemtelefon ausgelesenen Systemdaten angezeigt.

Abb. 297: **elmeg Systemtelefone**->**Zugewiesene Systemtelefone**->**Geräteinfos**

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Beschreibung	Zeigt die eingetragene Beschreibung des Telefons an.
Telefontyp	Zeigt den Typ des Telefons an.
Seriennummer	Zeigt die Seriennummer des Telefons an.
Softwareversion	Zeigt den aktuellen Stand der Telefon-Software an.
Datum und Uhrzeit des Release	Zeigt Datum und Uhrzeit des Telefon-Software-Standes an.
Letzte Gerätekonfiguration	Zeigt Datum und Uhrzeit der letzten Konfigurierung des Telefons an.
Anrufbeantworter	Zeigt an, ob ein Anrufbeantwortermodul im Telefon gesteckt ist

Beschreibung	Bedeutung
	(Ja) oder nicht (Nein).

Bedeutung der Tastenerweiterungen

Beschreibung	Bedeutung
Modul 1: Typ/ Seriennummer **Modul 2: Typ/ Seriennummer** **Modul 3: Typ/ Seriennummer**	Zeigt den Typ und die Seriennummer der angeschlossenen Tastenerweiterung an.
Modul 1: Softwareversion **Modul. 2: Softwareversion** **Modul 3: Softwareversion**	Zeigt die aktuelle Softwareversion der angeschlossenen Tastenerweiterung an.

29.7 Voice Mail System

Im Menü **Voice Mail System** können Sie Informationen zu Ihrer Voice Mail Box einsehen.

Hinweis

Das Menü **Voice Mail System** wird nur dann angezeigt, wenn für Sie eine persönliche Voice Mail Box eingerichtet ist.

29.7.1 Einstellungen

Im Menü **Voice Mail System** ->**Einstellungen** werden die Einstellungen Ihrer Voice Mail Box angezeigt.

Abb. 298: **Voice Mail System ->Einstellungen**

Werte in der Liste Einstellungen

Feld	Beschreibung
Interne Rufnummer	Zeigt Ihre interne Rufnummer an.
Benutzer	Zeigt Ihren Benutzernamen an.
Status des Mail-Box-Besitzers	Zeigt Ihren Status an.
PIN überprüfen	Zeigt an, ob der Zugang zu Ihrer Voice Mail Box mit einer PIN geschützt ist.
Modus für Status "Im Büro"	Zeigt an, in welchem Modus Ihre Voice Mails Box für den Status "Im Büro" betrieben wird.
Modus für Status "Außer Haus"	Zeigt an, in welchem Modus Ihre Voice Mails Box für den Status "Außer Haus" betrieben wird.
Neue Anrufe	Zeigt die Anzahl der neuen Anrufe an.
Alte Anrufe	Zeigt die Anzahl der alten Anrufe an.
Gespeicherte Anrufe	Zeigt die Anzahl der gespeicherten Anrufe an.

29.7.1.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Sie können die Einstellungen ausgewählter Parameter ändern.

Abb. 299: **Voice Mail System ->Einstellungen**

Das Menü**Voice Mail System ->Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Status des Mail-Box-Besitzers	Bestimmen Sie, mit welchem Modus Ihre Mail Box beim Start des Voice Mail Systems benutzt werden soll. Mögliche Werte: • *Im Büro* (Standardwert): Wählen Sie diese Einstellung, wenn Sie sich im Büro befinden, wenn das Voice Mail System gestartet wird. • *Außer Haus*: Wählen Sie diese Einstellung, wenn Sie sich außer Haus befinden, wenn das Voice Mail System gestartet wird.
PIN überprüfen	Wählen Sie, ob Ihre Voice Mail Box durch eine PIN geschützt werden soll.
Modus für Status "Im Büro"	Ihre Voice Mail Box kann während der Bürozeiten mit zwei verschiedenen Einstellungen betrieben werden. Mögliche Werte: • *Nur Ansage*: Ein Anrufer hört einen Ansagetext, kann aber selbst keine Nachricht hinterlassen. • *Ansage und Aufnahme* : Ein Anrufer hört einen Ansagetext

Feld	Beschreibung
	und kann eine Nachricht hinterlassen.
Modus für Status "Außer Haus"	Ihre Voice Mail Box kann außerhalb der Bürozeiten mit zwei verschiedenen Einstellungen betrieben werden. Mögliche Werte: • *Nur Ansage*: Ein Anrufer hört einen Ansagetext, kann aber selbst keine Nachricht hinterlassen. • *Ansage und Aufnahme* : Ein Anrufer hört einen Ansagetext und kann eine Nachricht hinterlassen.

Felder im Menü Voice Mail über E-Mail

Feld	Beschreibung
E-Mail-Benachrichtigung	Wenn eine Nachricht auf der Voice Mail Box hinterlassen wurde, kann der Teilnehmer benachrichtigt werden. Mögliche Werte: • *Keiner* (Standardwert): Der Teilnehmer wird nicht benachrichtigt. • *E-Mail*: Der Teilnehmer wird per E-Mail über eine hinterlassene Nachricht informiert. • *E-Mail mit Anhang*: Wenn ein Anrufer eine Nachricht hinterlassen hat, erhält der Teilnehmer eine E-Mail mit einer Aufzeichnung der Nachricht im Anhang.  **Hinweis** Nachdem ein Teilnehmer per E-Mail über eine neue Nachricht informiert wurde, ändert sich der **Status** der Mitteilung entsprechend den Einstellungen im Menü **Benutzerzugang**->**Voice Mail System** ->**Einstellungen** unter **Verhalten der E-Mail-Weiterleitung** .
Verhalten der E-Mail-Weiterleitung	Nur bei **E-Mail-Benachrichtigung** = *E-Mail* oder *E-Mail mit Anhang* Wählen Sie ein Option für weitergeleitete Nachrichten aus. Mögliche Werte:

Feld	Beschreibung
	• *Nach Weiterleitung Nachricht in 'neu' behalten*: Die Voice-Mail-Nachricht wird nach einer E-Mail-Benachrichtigung oder Weiterleitung auf den Status *Neu* gesetzt. • *Nach Weiterleitung Nachricht nach 'alt' verschieben*: Die Voice-Mail-Nachricht wird nach einer E-Mail-Benachrichtigung oder Weiterleitung auf den Status *Alt* gesetzt. • *Nach Weiterleitung Nachricht entfernen*: Die Voice-Mail-Nachricht wird nach einer E-Mail-Benachrichtigung oder Weiterleitung gelöscht.

29.7.2 Nachrichten

Im Menü **Voice Mail System** ->**Nachrichten** wird eine Liste mit Ihren Nachrichten angezeigt. Außerdem haben Sie die Möglichkeit, Voice-Mail-Nachrichten abzuspielen oder auf ihren PC herunterzuladen. Zum Speichern einer Nachricht klicken Sie auf das -Symbol. Daraufhin öffnet sich der Download-Dialog. Um die Voice-Mail-Nachricht anzuhören, klicken Sie auf das -Symbol.

Durch Anklicken der Checkbox **Alle auswählen** / **Alle deaktivieren** und anschließendem Drücken von **Auswahl löschen** können einzelne oder alle Wave-Dateien gelöscht werden.

Abb. 300: **Voice Mail System** ->**Nachrichten**

Werte in der Liste Nachrichten

Feld	Beschreibung
Interne Rufnummer	Zeigt die interne Rufnummer einer Voice Mail Box an. Einem Benutzer können mehrere interne Rufnummern zugewiesen sein. Unter jeder internen Rufnummer kann der Benutzer eine separate Voice Mail Box betreiben.

Feld	Beschreibung
Benutzer	Zeigt den Namen des Benutzers der Voice Mail Box an.
Anruf von	Zeigt die Rufnummer des Anrufers an.
Datum/Uhrzeit	Zeigt Datum und Uhrzeit des Anrufs an.
Anrufstatus	Zeigt an, ob der Anruf *Neu*, *Alt* oder *Gespeichert* ist.
Alle auswählen / **Alle deaktivieren**	Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** bzw. **Alle deaktivieren** markieren. Durch Drücken der Option **Auswahl löschen** können Sie die gewählten Einträge löschen.

Glossar

2G Siehe GSM.

3DES Siehe DES.

3G Siehe UMTS.

4G Siehe LTE.

802.11 Die Norm 802.11 beschreibt Wireless LAN (WLAN). Es existieren verschiedene Erweiterungen: 802.11a: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 5 GHz, 802.11b: Brutto-Datentransferrate: 11 Mbit/s, Frequenzband: 2,4 GHz, 802.11g: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 2,4 GHz, 802.11n: Brutto-Datentransferrate: 600 Mbit/s, Frequenzband: 2,4 GHz (optional: 5 GHz)

A-Teilnehmer Der A-Teilnehmer ist der Anrufer.

a/b-Schnittstelle Eine a/b-Schnittstelle dient zum Anschluss eines analogen Endgeräts. Bei einem ISDN-Endgerät (Terminaladapter) mit a/b-Schnittstelle wird ein angeschlossenes analoges Endgerät in die Lage versetzt, die unterstützten ISDN-Leistungsmerkmale zu nutzen.

Abwurf / Abwurffunktion Bei der Wahl einer nicht-eingerichteten Rufnummer innerhalb der Telefonanlage oder falls der Anschluss des angerufenen Teilnehmers besetzt ist oder dieser den Anruf nicht entgegennimmt, bestimmt die Abwurffunktion, wie mit dem Gespräch verfahren wird. Der Anruf kann zu einem anderen Ziel weitergeleitet oder verworfen werden.

Access Client Der Client Mode ist eine Betriebsart eines Wireless Access Points (AP), bei dem sich dieser gegenüber dem übergeordneten AP wie ein Wireless Adapter verhält. Mit einem im Client Mode betriebenen AP können einzelne Rechner oder ganze Subnetze an übergeordnete Netze angebunden werden.

Access Point Ein Access Point (AP) ist ein Gerät zur drahtlosen Verbindung von Clients (Computern). Der AP dient somit zum Aufbau eines Funknetzwerks (WLAN) sowie der Verbindung dieses WLANs mit einem kabelgebundenen Ethernet-Netzwerk (Bridging).

Accounting Beim Accounting werden Verbindungsdaten aufgezeichnet, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und An-

zahl der übertragenen Datenpakete.

Activity Monitor Mithilfe des Activity Monitors kann der Status physikalischer und virtueller Geräteschnittstellen überwacht werden.

Ad-Hoc-Netzwerk In einem Ad-Hoc-Netzwerk verbinden sich einzelne Clients über einen Wireless Adapter zu einem unabhängiges Wireless LAN. Ad-Hoc-Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer-Basis. Der Ad-Hoc-Modus wird auch als IBSS-Modus (Independent Basic Service Set) bezeichnet und ist in kleinsten Netzen sinnvoll, z. B. bei der Vernetzung zweier Notebooks ohne Access Point.

ADSL Asymmetric Digital Subscriber Line. Siehe DSL.

AES Advanced Encryption Standard (AES, Rijndael) ist ein Verschlüsselungsverfahren (siehe Cipher). AES verwendet eine feste Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit. AES ist ein sehr schneller und sicherer Algorithmus.

Agent Der Callcenter-Agent ist Mitglied eines Callcenters.

Aggressive Mode Beim Aufbau einer IPSec-Verbindung wird der Aggressive Mode zur Realisierung eines Phase-1-Austausches verwendet. Der Aggressive Mode bietet keinen Schutz der Identität für aushandelnde Knoten, da sie ihre Identitäten übertragen müssen, bevor sie einen sicheren Kanal aufbauen können. Siehe auch Main Mode.

AH Der Authentication Header (AH) wird bei IPSec verwendet, um die Authentizität und Integrität der übertragenen Pakete sicherzustellen sowie den Sender zu authentisieren.

Amtsberechtigung In der Telefonanlage werden die folgenden Amtsberechtigungen unterschieden: Uneingeschränkt: Alle internationalen, nationalen und internen Verbindungen sind erlaubt. Nationale Ferngespräche: Es dürfen nur Verbindungen ins Inland aufgebaut werden - also die Wahl aller Rufnummer die mit 0 aber nicht mit 00 beginnen. Von extern eingehende Anrufe können ohne Einschränkung entgegengenommen werden. Ort: Es dürfen nur Verbindungen zur gleichen Ortsvorwahl aufgebaut werden. Die Rufnummer darf also nicht mit einer 0 beginnen. Von extern eingehende Anrufe können ohne Einschränkung entgegengenommen werden. Kommend: Es dürfen nur Verbindungen zu anderen Endgeräten der Telefonanlage aufgebaut werden. Von extern eingehende Anrufe können ohne Einschränkung entgegengenommen werden. Intern: Nur Verbindungen innerhalb der Telefonanlage sind erlaubt.

Analog Analoge Signale werden zur Datenübertragung eingesetzt. Im Gegensatz zu digitalen Signalen sind sie störanfälliger.

Analoge Endgeräte Endgeräte, die Sprache oder andere Informationen analog übertragen, z. B. Telefone, Faxgeräte, Anrufbeantworter und Modems. Leistungsmerkmale lassen sich nur mit Endgeräten nutzen, die mit dem MFV-Wahlverfahren wählen und eine R- bzw. eine Flash-Taste besitzen.

Anklopfen Anklopfen ist ein Leistungsmerkmal. Während eines Telefonats wird ein weiterer Anrufer signalisiert.

Anklopfsperre Bei aktiviertem Anklopfschutz wird ein weiterer Anrufer nicht am Endgerät signalisiert. Der Anrufer hört den Besetztton.

Anlagenanschluss Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, …) Siehe auch Mehrgeräteanschluss.

Anlagenanschluss-Rufnummer Siehe Anlagenanschluss.

Annex A Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.

Annex B Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.

Annex J Annex J ist eine DSL-Variante zur reinen Datenübertragung, ohne Sprachinformationen (entbündelter Anschluss). Annex J ist eine Ergänzung zur Spezifikation G.992. Diese DSL-Anschlüsse benötigen keinen Splitter und haben eine höhere Reichweite und eine schnellere Übertragungsgeschwindigkeit.

Annex L Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrate vergrößert.

Annex M Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.

Anrufbeantworter Analoge Anrufbeantworter werden als analoges Endgerät konfigu-

riert und über den Endgerätetyp ausgewählt. Daneben dient das Voice Mail System der TK-Anlage als Anrufbeantworter.

Anruferliste In Systemtelefonen werden entgangene Anrufe in einer Anruferliste gespeichert. Dazu muss die Übermittlung der Telefonnummer des Anrufers (CLIP) aktiviert sein.

Anrufschutz Bei aktiviertem Anrufschutz ist die akustische Anrufsignalisierung ausgeschaltet. Diese Funktion wird auch als Ruhe vor dem Telefon bezeichnet.

Anrufvariante Die Anrufvariante legt fest, an welchen Endgeräten ein Anruf signalisiert wird. Die einzelnen Anrufvarianten können über den Kalender zeitgesteuert umgeschaltet werden.

Anrufweiterschaltung Anrufweiterschaltung ist ein Leistungsmerkmal. Mithilfe der Anrufweiterschaltung (AWS) können ankommende Anrufe zu einer anderen, internen oder externen Telefonnummer weitergeleitet werden. Die Anrufweiterschaltung kann in der Telefonanlage oder in der Vermittlungsstelle bzw. beim SIP-Provider erfolgen.

ANSI T1.413 ANSI T1.413 ist eine ADSL-Variante.

ARP Das Address Resolution Protocol (ARP) liefert zu IPv4-Adressen die zugehörigen MAC-Adressen. Die notwendigen Informationen werden zwischen den Netzwerkknoten ausgetauscht, im Cache des Geräts gespeichert und nach Ablauf der ARP Lifetime wieder gelöscht. Für IPv6 wird diese Funktionalität durch das Neighbor Discovery Protocol (NDP) bereitgestellt.

ARS Mithilfe der Automatic Route Selection (ARS) bestimmt die TK-Anlage die optimale Route zum angerufenen Teilnehmer, in Abhängigkeit von Provider, Dienst, QoS, …

ATM Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge kodiert und über asynchrones Zeitmultiplexing übertragen wird.

Authentifikation Überprüfung der Identität des Nutzers (Authentisierung).

Automatische Amtsholung Bei automatischer Amtsholung kann sofort (ohne Eingabe einer Kennziffer) die Telefonnummer eines externen Gesprächspartners gewählt werden.

Automatische Wahlwiederholung Ist der Anschluss der angerufenen Seite besetzt, kann eine automatische Wahlwiederholung eingeleitet werden. Diese informiert den

Anrufer sobald die Leitung frei ist.

Automatischer Rückruf bei besetzt (CCBS) Rückruf bei besetzt ist ein Leistungsmerkmal. Ist der Anschluss des angerufenen Teilnehmers besetzt, kann ein Rückruf angefordert werden. Sobald das Gespräch des angerufenen Teilnehmers beendet ist, wird der Anrufer gerufen und automatisch mit dem Angerufenen verbunden.

Automatischer Rückruf bei Nichtmelden (CCNR) Rückruf bei Nichtmelden ist ein Leistungsmerkmal. Nimmt der angerufene Teilnehmer den Anruf nicht entgegen, kann ein Rückruf angefordert werden. Sobald der angerufene Teilnehmer ein Gespräch beendet, wird der Anrufer gerufen und automatisch mit dem Angerufenen verbunden.

Autorisierung Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.

AUX AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.

B-Kanal Siehe Basisanschluss und Primärmultiplexanschluss.

B-Teilnehmer Der B-Teilnehmer ist der angerufene Teilnehmer.

Backbone Area Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.

Basisanschluss Der Basisanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Basic Rate Interface (BRI). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle) mit je 64 kbit/s und einen Steuerkanal (D-Kanal) mit 16 kbit/s. Für den Basisanschluss existieren zwei Betriebsarten: Anlagenanschluss und Mehrgeräteanschluss. Für größere Installationen wird der Primärmultiplexanschluss verwendet.

Beacon Zum Aufbau eines Wireless LAN im Infrastruktur-Modus versendet der zentrale Access Point Beacons. Diese Mitteilungen enthalten den Netzwerknamen (SSID), eine Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung.

Berechtigungsklasse Siehe CoS.

Besetzt bei besetzt Siehe Busy on Busy.

Bit Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.

Black / White List Einträge in der Black List werden blockiert, Einträge in der White List werden durchgelassen. (Beispiel: Alle Telefonnummern, die mit 01234 beginnen, werden in der Black List blockiert. Die Telefonnummer 01234987 kann trotzdem in der White List freigegeben werden.)

Blowfish Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.

BootP Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.

Bps Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.

BRI Siehe Basisanschluss.

Bridge Eine Bridge ist eine Netzwerkkomponente zum Verbinden gleichartiger Netze auf Schicht 2 des OSI-Modells. Datenpakete werden anhand von MAC-Adressen übertragen. Durch Bridges wird das Netzwerk aufgeteilt und entlastet.

Broadcast Bei einem Broadcast werden Datenpakete von einem Punkt an alle Teilnehmer eines Netzes übertragen, z. B. falls der Empfänger noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP und DHCP. Die Kommunikation erfolgt über Broadcast-Adressen: MAC-Netzwerke: FF:FF:FF:FF:FF:FF, IPv4-Netzwerke: 255.255.255.255, IPv6-Netzwerke: ff00::/8

BRRP BRRP ist eine Implementierung des Virtual Router Redundancy Protocol (VRRP). Ziel des Verfahrens ist es den Ausfall des Standardgateways zu kompensieren. Mehrere Router werden zu einem virtuellen Router zusammengefasst. Fällt einer dieser Router aus, können die Restlichen diesen ersetzen.

Bündel Die externen Anschlüsse einer Telefonanlage können zu Bündeln zusammengefasst werden.

Busy On Busy Ist Busy On Busy (Besetzt bei besetzt) aktiviert, hört ein Anrufer eines besetzten Teilnehmers den Besetztton. Anklopfen oder Anrufweiterschaltung an ein Team ist nicht möglich.

CA Certificate Authority. Siehe Zertifikat.

Cache Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.

Call Deflection (CD) Siehe Rufumleitung.

Call Through Unter Call Through versteht man die Einwahl über einen externen Anschluss in das System und die Weiterwahl aus dem System zu einem anderen externen Anschluss. Dies kann zur Senkung der Gesprächskosten führen.

Callcenter Ein Callcenter bietet Beratung, Informationsaustausch und Verkauf über das Telefon.

Called Party's Number Rufnummer des angerufenen Teilnehmers.

Calling Party's Number RufnNummer des Anrufers.

CAPI Das Common ISDN Application Programming Interface (CAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch TAPI.

CAPWAP Das Control And Provisioning of Wireless Access Points Protocol (CAPWAP) dient zur Überwachung von Wireless Access Points (Slaves) durch einen WLAN-Controller (Master). Es verwendet die UDP-Ports 5246 zur Kontrolle und 5247 zur Datenübertragung.

CAST CAST ist ein Verschlüsselungsverfahren (siehe Cipher). CAST verwendet eine fixe Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 40 und 128 Bit gewählt werden. Alternative Bezeichnungen sind CAST-128 oder CAST5.

CFB Call Forwarding Busy (CFB) ist ein Leistungsmerkmal. CFB schaltet Anrufer an einen anderen Anschluss weiter, wenn der Anschluss des Angerufenen besetzt ist (Anrufweiterschaltung bei besetzt).

CFNR Call Forwarding No Reply (CFNR) ist ein Leistungsmerkmal. CFNR schaltet Anrufer an einen anderen Anschluss weiter, wenn der Anruf nicht entgegengenommen wird (Anrufweiterschaltung bei Nichtmelden).

CHAP Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentifizierungsprotokoll für PPP-Verbindungen. Neben dem Standard-CHAP existieren noch die Varianten MS-CHAPv1 und MS-CHAPv2 der Firma Microsoft. Man wählt sich über PPP in ein Netzwerk ein und authentifiziert sich mit Benutzername und Passwort. Benutzername und Passwort werden verschlüsselt übertragen. Siehe auch PAP.

Cipher Eine Blockchiffre (Block Cipher) ist ein Verschlüsselungsalgorithmus. In diesem Verschlüsselungsverfahren wird ein Datenblock mit fester Größe (normalerweise 64 Bit) mithilfe eines sogenannten Schlüssels zu einem Block derselben Größe umgeschrieben. Je länger der Schlüssel ist, umso sicherer ist der Algorithmus.

CLID Calling Line Identification (CLID), auch Caller ID, wird zur Authentifizierung verwendet. Ein Anrufer wird anhand seiner ISDN-Rufnummer erkannt, bevor die Verbindung aufgebaut wird.

Client Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.

CLIP Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).

CLIP no Screening Siehe auch Telefonnummer des Anrufers anzeigen (CLIP / CLIR). Bei CLIP no Screening wird neben der normalen Rufnummer des Anrufers eine weitere Rufnummer, z. B. Rufnummer der Telefonzentrale oder eine Servicerufnummer, mitgesendet. Die normale Rufnummer kann zusätzlich über CLIR unterdrückt werden, sodass der Angerufene nur die weitere Rufnummer sieht.

CLIP off Hook Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).

CLIR Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).

COLP Siehe Telefonnummer des Angerufenen anzeigen (COLP / COLR).

COLP no Screening Siehe auch Telefonnummer des Angerufenen anzeigen (COLP / COLR). Bei COLP no Screening wird neben der normalen Rufnummer des Angerufenen eine weitere Rufnummer, z. B. Rufnummer der Telefonzentrale oder eine Servicerufnummer, mitgesendet. Die normale Rufnummer kann zusätzlich über COLR unterdrückt werden, sodass der Anrufer nur die weitere Rufnummer sieht.

COLR Siehe Telefonnummer des Angerufenen anzeigen (COLP / COLR).

CoS Der Begriff Class of Service (CoS) hat je nach Anwendungsgebiet verschiedene Bedeutungen. In der Telekommunikation wird unter CoS die dem Benutzer zugeteilte Berechtigungsklasse verstanden. Die Berechtigungsklasse legt die Rechte des Benutzers fest, wie z. B. Amtsberechtigung, nutzbare Leistungsmerkmale, Zugriff auf Anwendungen, … In der Netzwerktechnologie versteht man unter CoS die Klassifizierung bestimmter Dienste gemäß IEEE 802.1p. CoS ermöglicht eine gezielte Priorisierung, während mit Quality of Service (QoS) explizite Bandbreitengarantien oder -beschränkungen einge-

	richtet werden. Die Einteilung der Datenpakete erfolgt mittels eines DSCP-Werts (Differentiated Services Code Point).
CRC	Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.
CRL	Siehe Zertifikat.
D-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.
Daemon	Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.
Datagramm	Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.
Datenkompression	Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.
DDI	Direct Dial In (DDI) bedeutet Durchwahl. Siehe Anlagenanschluss und Durchwahl (VoIP).
Dead Peer Detection	In IPSec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.
DECT	Digital Enhanced Cordless Telecommunications (DECT) ist ein Standard für Schnurlostelefone sowie für kabellose Telefonanlagen.
Default Gateway	An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.
Default Route	Siehe Standardroute.
Deffie-Hellman	Diffie-Hellman ist ein Public-Key-Algorithmus zur Aushandlung und Etablierung von Schlüsseln. Da Daten weder verschlüsselt noch signiert werden, ist das Verfahren nur sicher, falls sich die Verbindungspartner über andere Mechanismen, wie RSA oder DSA, authentifizieren.
Denial-Of-Service Attack	Bei einem Denial-of-Service-Angriff (DoS) wird eine Netzwerkkomponente mit Anfragen überflutet, sodass diese völlig überlastet wird. Das System oder ein bestimmter Dienst ist in Folge dessen nicht mehr funktionsfähig.
DES	Data Encryption Standard (DES) ist ein Verschlüsselungsverfahren (siehe Cipher). DES verwendet eine feste Blocklänge von 64 Bit.

Die Schlüssellänge beträgt 56 Bit. Triple-DES oder 3DES basiert auf der dreimaligen Anwendung von DES (drei verschiedene unabhängige Schlüssel).

DFÜ DFÜ steht für Datenfernübertragung.

DHCP Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die dynamische Zuweisung von IP-Adressen. Ein DHCP-Server vergibt an jeden Client im Netzwerk eine IP-Adresse aus einem definierten Adress-Pool. Die Clients müssen dazu entsprechend konfiguriert sein.

Digital Digitale Signale werden zur Datenübertragung eingesetzt. Im Gegensatz zu analogen Signalen sind sie weniger störanfällig.

DIME Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.

Direktruf Falls die Funktion Direktruf eingerichtet ist, muss lediglich der Telefonhörer abgehoben werden, um nach einer kurzen Wartezeit eine Verbindung zu einer bestimmten Telefonnummer automatisch einzuleiten.

DISA DISA steht für Direct Inward System Access. Ein Anruf wird, nachdem er von der Telefonanlage angenommen wurde, nach Eingabe einer Kennziffer automatisch weitervermittelt. Der Kennziffer ist in der Telefonanlage eine Telefonnummer zugeordnet.

DNS Mithilfe des Domain Name System (DNS) wird der Domänenname (z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).

Domäne Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).

Downstream Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.

Dreierkonferenz Die Dreierkonferenz ist ein Leistungsmerkmal. Drei Teilnehmer können gleichzeitig miteinander telefonieren.

DSA Mithilfe des Digital Signature Algorithm (DSA) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über Signaturen können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. DSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch RSA. DSA ist schneller in der Schlüsselerzeugung aber langsamer in der Schlüsselverarbeitung

als RSA.

DSCP Datenpakete können mit einem Differentiated Services Codepoint (DSCP) ausgezeichnet werden. DSCP-Werte teilen Datenpakete in Klassen ein, sodass wichtige Pakete schneller durch das Netzwerk geleitet werden können. Siehe auch QoS.

DSL-Modem Siehe Modem.

DSP Ein digitaler Signalprozessor (DSP) wandelt analoge, ISDN- und VoIP-Signale ineinander um. Analoge Endgeräte können somit z. B. auch an einem SIP-Anschluss verwendet werden.

DSS1 Digital Subscriber Signalling System No. 1 (DSS1) ist ein Signalisierungsprotokoll für den D-Kanal des ISDN. Es ist auch bekannt als Euro-ISDN.

DTIM Eine Delivery Traffic Indication Message informiert die Clients über auf dem Access Point vorhandene Multicast- bzw. Broadcast-Daten.

DTMF Siehe Mehrfrequenzwahlverfahren.

DTMF Inband / Outband Siehe auch Mehrfrequenzwahlverfahren. Bei Inband wird das DTMF-Signal im Sprachband übertragen (G.711). Bei Outband wird das DTMF-Signal entsprechend RFC 2833 übertragen.

Durchsage Die Durchsage ist ein Leistungsmerkmal. Die Durchsage-Funktion ermöglicht es, eine Verbindung zu anderen Telefonen aufzubauen, die von den angerufenen Teilnehmern automatisch angenommen wird. Der Anrufer spricht und die Angerufenen hören die Durchsage. Hebt ein Angerufener den Hörer ab, wird eine normale Verbindung hergestellt.

Durchwahl (VoIP) Beim Durchwahl-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer IP-TK-Anlage. Man erhält eine Basisrufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Basisrufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, …)

Durchwahlausnahme Siehe Anlagenanschluss und Durchwahl (VoIP).

Durchwahlbereich Siehe Rufnummernblock bei Anlagenanschluss und Durchwahl (VoIP).

Durchwahlnummer Siehe Anlagenanschluss und Durchwahl (VoIP).

Dynamische IP-Adresse Im Gegensatz zu einer statischen IP-Adresse wird die dynamische IP-Adresse temporär per DHCP zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.

DynDNS Mithilfe eines DynDNS-Providers kann ein Domänenname auch mit einer dynamisch wechselnden IP-Adresse verknüpft werden.

Einzelrufnummer (VoIP) Beim Einzelrufnummer-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von VoIP-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Durchwahl (VoIP).

Encapsulation Enkapsulierung (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.

Encryption Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.

ESP Encapsulating Security Payload (ESP) ist ein Protokoll für IPSec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.

Ethernet Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.

Euro-ISDN In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.

Eurofile-Transfer EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.

Fax Mithilfe eines Telefax (Kurzform Fax) können Texte, Grafiken und Dokumente über das Telefonnetz übertragen werden. Man unterscheidet zwischen Faxgeräten der Gruppe 3 für das analoge Netz (Übertragungsrate: 9,6 bzw. 14,4 kbit/s) und Faxgeräten der Gruppe 4 für das ISDN (Übertragungsrate: 64 kbit/s). Für den Anschluss von Faxgeräten der Gruppe 3 an ISDN benötigt man einen Terminaladapter oder eine entsprechende Telefonanlage.

Filter Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll,

	Port-Nummer, Quell- und Zieladresse). Treffen diese Kriterien für ein Datenpaket zu, kann das Datenpaket einer bestimmten Aktion (weiterleiten, ablehnen, …) unterworfen werden. Dadurch entsteht eine Filterregel.
Filterregel	Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.
Firmware	Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts bereitgestellt.
Flash-Taste	Die Flash-Taste bei Telefonen entspricht der R-Taste. Die Taste unterbricht die Leitung für einen kurzen Moment, um bestimmte Funktionen wie z. B. eine Rückfrage einzuleiten.
Follow-me	Follow-me ist ein Leistungsmerkmal. Mit dieser Funktion können eingehende Anrufe einer anderen Nebenstelle zum eigenen Endgerät umgeleitet werden.
Fragmentierung	Falls die Gesamtlänge des Datenpakets größer als die Maximum Transmission Unit (MTU) der Netzwerkschnittstelle ist, muss das Datenpaket durch IP-Fragmentierung auf mehrere physikalische Datenblöcke aufgeteilt werden. Der umgekehrte Prozess wird Reassembly genannt.
Frame	Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells
Frame Relay	Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.
Freisprechen	Beim Freisprechen kann man bei aufgelegtem Hörer telefonieren. Dabei können weitere Personen im Raum über Mikrofon und Lautsprecher am Gespräch teilnehmen.
FTP	Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.
Full-Duplex	Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.
Funktionstasten	Funktionstasten sind spezielle Tasten bei Systemtelefonen, die mit Telefonnummern oder Funktionen belegt werden können.

FXO Foreign Exchange Office (FXO) bezeichnet den Anschluss am analogen Endgerät. Siehe auch FXS.

FXS Foreign Exchange Station (FXS) bezeichnet den analogen Anschluss an der Anschlussdose oder der Telefonanlage. Siehe auch FXO.

G.711 G.711 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 300 Hz bis 3400 Hz werden mit einer Abtastrate von 8 kHz erfasst. Der Codec erreicht bei einer Datenübertragungsrate von 64 kbit/s eine sehr gute Sprachqualität (MOS-Wert: 4,4). In Europa wird das alaw- und in den USA das µlaw-Quantisierungsverfahren verwendet.

G.722 G.722 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 50 Hz bis 7000 Hz werden mit einer Abtastrate von 16 kHz erfasst. Der Codec erreicht bei einer Datenübertragungsrate von 64 kbit/s eine hervorragende Sprachqualität (MOS-Wert: 4,5).

G.726 G.726 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 200 Hz bis 3400 Hz werden mit einer Abtastrate von 8 kHz erfasst. Der Codec erreicht eine ordentliche Sprachqualität. MOS-Wert: 3,7 (16 kbit/s), 3,8 (24 kbit/s), 3,9 (32 kbit/s), 4,2 (40 kbit/s). Es existieren zwei unterschiedliche Kodierverfahren: I.366 und X.420

G.729 G.729 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 300 Hz bis 2400 Hz werden mit einer Abtastrate von 16 kHz erfasst. Der Codec erreicht bei einer Datenübertragungsrate von 8 kbit/s eine ordentliche Sprachqualität (MOS-Wert: 3,9).

G.991.1 Datenübertragungsempfehlung für HDSL.

G.991.2 Datenübertragungsempfehlung für SHDSL.

G.992.1 Datenübertragungsempfehlung für ADSL (G.DMT). Es existieren zwei länderspezifische Ausprägungen G.992.1 Annex A und G.992.1 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)

G.992.2 Datenübertragungsempfehlung für ADSL (G.LITE / ADSL-Lite). Es existieren zwei Varianten G.992.2 Annex A und G.992.2 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)

G.992.3 Datenübertragungsempfehlung für xDSL2. Es existieren drei Varianten: G.992.3 Annex A/B (G.DMT bis ADSL2) mit Datenübertra-

	gungsraten von 12 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.3 Annex L (RE-ADSL2) mit Datenübertragungsraten von 5 Mbit/s im Downstream und 0,8 Mbit/s im Upstream und G.992.3 Annex M (ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 2,5 Mbit/s im Upstream.
G.992.4	Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)
G.992.5	Datenübertragungsempfehlung für xDSL2+. Es existieren drei Varianten: G.992.5 Annex A/B (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.5 Annex L (RE-ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream und G.992.5 Annex M (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 3,5 Mbit/s im Upstream.
G.993.1	Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)
G.993.2	Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)
G.DMT	Siehe F.992.1.
G.Lite	Siehe F.992.2.
G.SHDSL	Siehe G.991.2.
Gateway	Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.
GPRS	General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.
GRE	Generic Routing Encapsulation (GRE) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. GRE verwendet die Protokollnummer 47.
GSM	Das Global System for Mobile Communications (GSM), auch als 2G bezeichnet, ist ein Mobilfunkstandard. Dieser erreicht zusammen mit GPRS eine spezifizierte max. Datenübertragungsrate von 171,2 kbit/s.
Half-Duplex	Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.

Halten Ein Telefongespräch wird auf Wartestellung geschaltet, ohne die Verbindung zu verlieren (Rückfragen/Makeln). Man unterscheidet zwischen dem Halten der Verbindung in der Telefonanlage (Halten im System) und der Wartestellung in der Vermittlungsstelle bzw. beim SIP-Provider.

Hash Zur Sicherstellung der Datenintegrität muss die Information vor unautorisierter Manipulation während der Übertragung geschützt werden. Um dies zu gewährleisten, muss jede empfangene Kommunikation mit der ursprünglich gesendeten Information übereinstimmen. Deshalb werden mathematische Streuwertfunktionen (Hashfunktionen) zur Berechnung von Prüfsummen (Hashwerten) verwendet. Diese werden verschlüsselt und mit der Nachricht als digitale Signatur versendet. Der Empfänger prüft wiederum die Signatur, bevor er das Paket öffnet. Falls sich die Signatur und damit der Inhalt des Datenpakets geändert hat, wird das Paket verworfen. Die am häufigsten verwendeten Hash-Algorithmen sind Message Digest Version 5 (MD5) und Secure Hash Algorithm (SHA1).

HDSL High Data Rate Digital Subscriber Line. Siehe DSL.

Heartbeat Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.

Heranholen von Rufen Siehe Pick-Up

Hop Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.

Host Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.

Host-Name Domänenname eines Host. Siehe DNS.

Hostroute Eine Hostroute bezeichnet die Route zu einem einzelnen Host.

Hotspot Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.

HSDPA High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.

HTTP Das HyperText Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. Es verwendet standardmäßig den Port 80.

HTTPS Das HyperText Transfer Protocol Secure (HTTPS) ist ein Protokoll zur abhörsicheren Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. HTTPS ist schematisch identisch zu HTTP. Für die zusätzliche Verschlüsselung der Daten wird SSL / TLS verwendet. Der Standard-Port für HTTPS-Verbindungen ist 443.

Hyperchannel Beim Hyperchannel haben mehrere Teilnehmer Zugriff auf das Übertragungsmedium. Ein Teilnehmer kann seine Informationen nur übertragen, wenn kein anderer Teilnehmer das Medium belegt. Ein Hyperchannel-Netzwerk dient hauptsächlich für Kurzstreckenbetrieb mit höchsten Datenraten.

IAE IAE bezeichnet die standardisierte Steckdose (ISDN-Anschlusseinheit), an der ISDN-Endgeräte angeschlossen werden.

ICMP Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.

IGMP Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.

IKE Das Internet-Key-Exchange-Protokoll (IKE) dient der automatischen Schlüsselverwaltung bei IPSec-Verbindungen. Der IKE-Prozess verläuft in zwei Phasen. Während Phase 1 authentifizieren sich die IKE-Teilnehmer gegenseitig und etablieren einen sicheren Kanal. In Phase 2 handeln die beiden IPSec-Teilnehmer die SAs aus. Es existieren zwei Versionen des IKE-Mechanismus.

Impulswahlverfahren Das Impulswahlverfahren (IWV) ist ein Signalisierungsverfahren zur automatischen Telefonvermittlung. Tastatureingaben werden durch eine definierte Anzahl von Gleichstromimpulsen dargestellt. Siehe auch Mehrfrequenzwahlverfahren (MFV).

Infrastruktur-Netzwerk In einem Infrastruktur-Netz bilden die einzelnen Endgeräte (Clients) über einen zentralen Knotenpunkt (Access Point) ein Wireless LAN. Dieser zentrale Access Point kann dabei auch ein Vermittler in weitere Netze sein.

Interne Telefonnummern Die internen Telefonnummern werden für Gespräche innerhalb der Telefonanlage verwendet.

Internrufton Der Internrufton dient als besondere Signalisierung in Telefonanlagen zur Unterscheidung von Intern- und Externanrufen.

IP Das Internet Protocol (IP) ist ein Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es arbeitet auf der Vermittlungsschicht des OSI-Modells. Auf IP bauen die Protokolle TCP und UDP auf. Es existieren zwei Versionen Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6).

IP-Adresse IP-Adressen werden zur Navigation in einem IP-Netzwerk verwendet, um Quelle und Ziel eindeutig zu bestimmen. IPv4-Adressen bestehen aus 32 Bits, IPv6-Adressen aus 128 Bits. Damit sind bei IPv4 232, also 4.294.967.296 Adressen darstellbar, bei IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen. Für IPv4 wird die Dezimaldarstellung (dotted decimal notation) verwendet, z. B. 192.168.0.250. Für IPv6 wird die Hexadezimaldarstellung verwendet, z. B. 2001:db8:85a3::8a2e:370:7344. Siehe auch Netzmaske.

IPCP Das Internet Protocol Control Protocol (IPCP) dient, analog zu DHCP, zur Konfiguration eines Host mit IP-Adresse, Gateway und DNS-Server, falls eine PPP-Netzwerkverbindung verwendet wird. Mithilfe der Erweiterung Robust Header Compression over PPP kann der Header für eine schnellere Datenübertragung komprimiert werden. Analog wird in IPv6-Netzwerken die Funktionalität durch das Internet-Protocol-Version-6-Control-Protokoll (IPV6CP) bereitgestellt.

IPSec IPSec (Internet Protocol Security) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. Die Protokollnummer für IPSec ist dabei vom verwendeten Protokoll abhängig. Der Authentification-Header (AH) verwendet die Protokollnummer 51, das Encapsulating-Security-Payload (ESP) die Nummer 50.

IPv6 Siehe IP.

ISDN Integrated Services Digital Network (ISDN) ist ein Datenübertragungsstandard, der Telefonie, Telefax und Datenübertragung umfasst. Es existieren zwei ISDN-Anschluss-Varianten: Basisanschluss und Primärmultiplexanschluss.

ISDN-Adresse Die ISDN-Adresse eines ISDN-Geräts setzt sich zusammen aus einer ISDN-Nummer gefolgt von weiteren Ziffern, die sich auf das spezifische Endgerät beziehen.

ISDN-BRI Siehe BRI.

ISDN-Intern/-Extern Alternative Bezeichnung für den S0-Bus.

ISDN-Login Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.

ISDN-Nummer Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.

ISDN-PRI Siehe PRI.

ISDN-Router Siehe Router.

ISP Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.

ITU Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.

IWV Siehe Impulswahlverfahren.

Kanal Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.

Kanalbündelung Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.

Keepalive Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.

Keepalive Keepalive ist ein Mechanismus zur Aufrechterhaltung der Netzwerkverbindung und zur Überprüfung der Erreichbarkeit der Kommunikationspartner. Dazu werden in der Regel spezifische Pakete ins Netzwerk gesendet.

Kennzifferprozedur Über die Telefontastatur kann man eine Sequenz (Kennzifferprozedur) eingeben (bestehend aus 0 - 9, *, # und R), um Funktionen der Telefonanlage aufzurufen.

Keypad Das Keypad-Protokoll (Netz-Direkt) wird zum Aufruf und zur Steuerung von Leistungsmerkmalen, die von der Vermittlungsstelle bereitgestellt werden, verwendet.

Konferenzschaltung Bei einer Konferenzschaltung können mehrere interne Gesprächsteilnehmer gleichzeitig miteinander telefonieren.

Konfiguration Alle Einstellungen des Geräts werden als Konfiguration bezeichnet. Diese Konfiguration ist intern in MIB-Tabellen gespeichert. Diese Informationen können extern gesichert, von extern geladen oder ge-

löscht werden. Bearbeitet wird die Konfiguration über die HTTP(S)-Benutzeroberfläche, einen SNMP-Client oder angeschlossene Telefone.

Kurzwahl Jeder Telefonnummern im Telefonbuch ist ein Kurzwahl-Index (000...999) zugeordnet. Dieser Kurzwahl-Index kann anstelle der langen Telefonnummer für die Wahl verwendet werden.

L2TP Das Layer 2 Tunneling Protocol (L2TP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über verschiedene Protokolle zu transportieren. L2TP verwendet standardmäßig die Protokollnummer 1701. Die Architektur eines L2TP-Netzwerks besteht aus einem L2TP-Access-Concentrator (LAC), der auch fest in den Client integriert sein kann, und dem L2TP-Network-Server (LNS). Der LAC stellt die Verbindungen zum LNS her und verwaltet diese. Die Autorisierung wird über einen Network-Access-Server (NAS), der im LAC oder LNS implementiert sein kann, geregelt. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Die eigentlichen Nutzdaten werden unverschlüsselt ausgetauscht, während Kontrollnachrichten zu Aufrechterhaltung der Erreichbarkeit der Tunnelendpunkte abgesichert übertragen werden.

LAC Siehe L2TP.

LAN Ein Local Area Network (LAN) bezeichnet ein räumlich eng begrenztes Netzwerk und umspannt meist ein Gebäude oder einen Firmensitz.

Lastverteilung Bei der Lastverteilung werden Daten über unterschiedliche Schnittstellen gesendet, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. Im Unterschied zu Multilink funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.

Lauthören Beim Lauthören können im Raum anwesende Personen ein Telefongespräch mithören.

Layer Ein Layer bezeichnet eine Schicht im OSI-Modell.

LCP Das Link Control Protocol (LCP) wird in PPP-Verbindungen verwendet, um die Enkapsulierung automatisch auszuhandeln, Grenzen für variierende Paketgrößen zu verarbeiten, den Verbindungspartner zu authentifizieren, einen defekten Link zu bestimmen, Verbindungsfehler zu erkennen und die Verbindung zu beenden.

LDAP Das Lightweight Directory Access Protocol (LDAP) regelt die Kom-

	munikation zwischen einem Client und dem Directory-Server. LDAP wird für den Austausch und die Aktualisierung von Verzeichnissen, z. B. ein Telefonbuch, verwendet.
Lease Time	Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.
Leased Line	Siehe Standleitung.
LLC	Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.
LNS	Siehe L2TP.
Loopback	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
LTE	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
MAC-Adresse	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
Main Mode	Beim Aufbau einer IPSec-Verbindung wird der Main Mode zur Realisierung eines Phase-1-Austausches verwendet, indem ein sicherer Kanal eingerichtet wird. Siehe auch Aggressive Mode.
Makeln	Makeln erlaubt es, zwischen zwei Gesprächspartnern hin und her zu schalten, ohne dass der wartende Teilnehmer mithören kann.
Man-in-the-Middle Attack	Im Man-in-the-middle-Angriff befindet sich der Angreifer physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kann somit den Datenverkehr einsehen und sogar manipulieren.
MD5	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Media Gateway	Ein Media Gateway wandelt den Netzwerktyp von digitalen Sprach-, Audio- oder Bildinformationen um. Beispielsweise können die Signale eines ISDN-Netzwerks auf ein IP-Netzwerk umgesetzt werden.
Mehrfachrufnummer (MSN)	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
Mehrfrequenzwahl-	Das Mehrfrequenzwahlverfahren, auch als Tonwahlverfahren, MFV,

verfahren MFC oder DTMF bezeichnet, ist ein Signalisierungsverfahren zur automatischen Telefonvermittlung. Tastatureingaben werden durch überlagerte, sinusförmige Signale dargestellt. Siehe auch Impulswahlverfahren (MFV).

Mehrgeräteanschluss Beim Mehrgeräteanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von ISDN-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Anlagenanschluss.

Metrik Die Metrik ist eine Maß für die Güte der Route. Die schnellste Route weist dabei die geringste Metrik (costs, »Kosten«) auf. Vereinfacht ist dies die Verbindung mit der kleinsten Anzahl an Knotenpunkten (Routern).

MFC Siehe Mehrfrequenzwahlverfahren.

MFV Siehe Mehrfrequenzwahlverfahren.

MIB Die Management Information Base (MIB) beschreibt die Informationen, die über ein Netzwerk-Management-Protokoll (z. B. SNMP) abgefragt oder modifiziert werden können. Die MIB ist eine Datenbank, die alle Geräte und Funktionen im Netzwerk beschreibt.

MLP Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.

Mobiler Teilnehmer Falls der mobile Teilnehmer aktiviert ist, kann ein externes Telefon, z. B. ein Mobiltelefon, parallel gerufen (Parallelruf) werden. Ebenso können die Funktionen der Anlage, z. B. ein Rückruf, extern genutzt werden. Für diese Funktionen wird die Sterntaste des externen Telefons als R-Taste interpretiert.

Modem Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.

MOH Siehe Music On Hold.

MPDU Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.

MPPC Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.

MPPE Microsoft Point-To-Point Encryption (MPPE) wird zur Verschlüsselung von Daten, die über PPP übertragen werden, eingesetzt. Es wurde von Microsoft und Cisco entwickelt und als RFC 3078 spezifiziert.

MS-CHAP Das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) ist ein Authentisierungsverfahren. MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für PPTP-Verbindungen (VPN).

MSDU Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.

MSN Siehe Mehrfachrufnummer.

MSS Die Maximum Segment Size (MSS) definiert die maximale Anzahl an Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Die MSS muss kleiner als die Maximum Transmission Unit (MTU) sein, um eine Fragmentierung der IP-Pakete zu vermeiden.

MSS Clamping Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.

MTU Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.

Multicast Bei einem Multicast werden Datenpakete von einem Punkt an bestimmte Teilnehmer eines Netzes übertragen. In IPv4 wird dies über den Adress-Bereich 224.0.0.0 bis 239.255.255.255 und das Protokoll IGMP gesteuert, in IPv6 über ff00::/8-Adressen und ICMPv6.

Multilink Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, …) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.

Music On Hold Der Begriff Music On Hold (MOH) steht für automatische Ansagen oder Wartemusik über die Telefonanlage.

MWI Über den Message Waiting Indicator (MWI) wird das Vorhandensein einer neuen Nachricht signalisiert.

NAPT Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.

NAT Mithilfe von Network Address Translation (NAT) werden die Quell- und Ziel-IP-Adressen eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch PAT.

NBNS NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.

Nebenstelle Eine Nebenstelle bezeichnet bei Telefonanlagen das mit der Anlage verbundene Endgerät.

Netz-Direkt Siehe Keypad.

Netzabschluss Der Netzabschluss (Network Termination, NT) bezeichnet einen Anschluss bzw. eine Betriebsart. Am NT-Anschluss (Anschlussdose) wird einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt. Beim analogen Anschluss wird die Steckdose TAE genannt, beim ISDN-Basisanschluss NTBA und beim ISDN-Primärmultiplexanschluss NTPMGF. Im NT-Betrieb wird das Gateway am externen S0 der Telefonanlage angeschlossen und stellt für diese einen externen Amtsanschluss dar. Siehe auch TE.

Netzmaske Die Netzmaske, auch Netzwerkmaske oder Subnetzmaske, definiert bei IPv4 in Verbindung mit der IP-Adresse das Netzwerk, indem sie die IP-Adresse in einen Netzwerk- und einen Geräteanteil aufteilt und somit bestimmt, welche Adressen geroutet werden müssen. Beispiel einer Netzmaske: 255.255.255.0. Bei IPv6 spricht man von der Präfixlänge.

Netzwerkadresse Eine Netzadresse (Präfix) bezeichnet die Adresse des gesamten Netzwerks. Die Netzwerkmaske bzw. Präfixlänge unterteilt die IP-Adresse in die Netzadresse und Host-Adresse (Geräteadresse). Beispiel für eine Netzadresse: 192.168.0.250/24

Netzwerkroute Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.

NT Siehe Netzabschluss.

NTBA Siehe Netzabschluss.

NTP Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.

NTPMGF Siehe Netzabschluss.

Nutzkanal Siehe B-Kanal.

OAM OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.

Offene Rückfrage Bei der offenen Rückfrage wird ein Gespräch in einen Wartezustand versetzt und kann von jedem Teilnehmer wieder angenommen werden.

OSI-Modell Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.

OSPF OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.

PABX Private Automatic Branch Exchange (PABX) ist eine andere Bezeichnung für eine Telefonanlage.

PAP Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.

Parallelruf Siehe Mobiler Teilnehmer.

Parken Beim Parken wird eine Telefonverbindung gehalten, selbst wenn beim beteiligten Endgerät der Hörer aufgelegt oder die Kabelverbindung getrennt ist.

PAT Mithilfe von Port and Address Translation (PAT) werden die Quell- und Ziel-IP-Adressen sowie die Quell- und Ziel-Ports eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch NAT.

PBX Private Branch Exchange (PBX) ist eine andere Bezeichnung für eine Telefonanlage.

Peer Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.

Phase-1/2 Siehe IKE.

Pick-Up Bei Pick-Up werden Anrufe über Kennzifferprozeduren an einem internen Endgerät entgegengenommen, das sich nicht in der aktiven Rufverteilung befindet.

PIM Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.

PIN Mithilfe einer persönlichen Identifikationsnummer (PIN) kann man sich am Gerät authentisieren und dadurch Funktionen des Geräts nutzen.

Ping Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist. Daneben wird die Zeitspanne zwischen dem Aussenden eines Datenpakets (ICMP(v6)-Echo-Request-Paket) und dem Empfangen eines daraufhin unmittelbar zurückgeschickten Antwortpakets gemessen. Dadurch kann die Qualität der Verbindung ermittelt werden.

PKCS Die Public-Key Cryptography Standards (PKCS) beinhalten Standards für Public-Key-Kryptografie. Die PKCS sind konzipiert für binäre und ASCII-Daten und sind kompatibel mit dem X.509-Standard. Die veröffentlichten Standards sind PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, und #15. PKCS #10 beschreibt die Syntax für Zertifizierungsanfragen.

PKI Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.

PMTU Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.

Point-to-Multipoint Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).

Point-to-Point Siehe Anlagenanschluss und Durchwahl (VoIP).

Pool Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.

POP3 Das Post Office Protocol Version 3 (POP3) ist ein Übertragungsprotokoll, um den E-Mail-Abruf von einem E-Mail-Server durch einen Client zu steuern.

Port Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, …) ein ankommendes Datenpaket weitergeleitet wird.

POTS Plain Old Telephone System (POTS) bezeichnet das analoge Telefonnetz.

PPP Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.

PPPoA Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.

PPPoE Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.

PPTP Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. PPTP verwendet die Protokollnummer 1723. Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP-Access-Concentrator (PAC) und den PPTP-Network-Server (PNS). Der PAC ist üblicherweise in den Windows Client integriert. Er stellt die Verbindung zum PNS her und verwaltet diese. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.

Präfix Siehe Netzwerkadresse.

Präfixdelegation In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.

Präfixlänge Siehe Netzmaske.

Preshared Key Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.

PRI Siehe Primärmultiplexanschluss.

Primärmultiplexanschluss Der Primärmultiplexanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Primary Rate Interface (PRI) oder S2M-Anschluss. Ein Primärmultiplexanschluss bietet in Europa 30 und in den USA 23 Nutzkanäle (B-Kanäle) mit je 64 kbit/s, einen Steuerkanal (D-Kanal) mit 64 kbit/s und einen Synchronisationskanal mit 64 kbit/s in Europa und 8 kbit/s in den USA. Siehe auch Basisanschluss.

Proposal Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.

Protokoll Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP

Proxy Ein Proxy ist eine Netzwerkkomponente. Der Proxy ist ein Vermittler. Er leitet eine Anfrage der Quelle mit seiner eigenen IP-Adresse an das Ziel weiter.

PVID Der Port VLAN Identifier (PVID) ist die Standard-VLAN-ID des jeweiligen Ports. Ein Paket, das ohne VLAN-Tag diesen Port erreicht, wird mit dieser ID versehen.

Q-SIG Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.

QoS Quality of Service (QoS) beschreibt die Qualität (Güte) des Kommunikationsdienstes. Diese wird anhand von Bandbreite, Verzögerung, Paketverlusten und Jitter definiert. Um zeitkritische Datenpakete für VoIP oder Videostreaming möglichst schnell zu übertragen, werden alle Datenpakete bei QoS in Gruppen sortiert und entsprechend ihrer Priorität im Netzwerk schneller oder langsamer weitergeleitet.

Queue In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.

RADIUS Remote Authentication Dial-In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen. Der RADIUS-Server authentifiziert den Client z. B. mittels der Überprüfung von Benutzername und Kennwort. Siehe auch TACACS+.

Raumüberwachung Die Raumüberwachung ist ein Leistungsmerkmal. Die Geräusche eines Zimmers können mitgehört werden.

RE-ADSL2 Siehe G.992.5.

Real Time Jitter Control Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.

Regelkette In einer Regelkette sind unterschiedliche Filterregeln zusammengefasst. Eine Filterregel wählt einen Teil des Datenverkehrs aufgrund bestimmter Merkmale, z. B. der Quell-IP-Adresse, aus und wendet auf diese Teilmenge eine Aktion an, z. B. blockieren.

Registrar Der SIP-Server (Registrar) muss eingesetzt werden, falls die Teilnehmer eines VoIP-Gesprächs keine statischen IP-Adressen verwenden. Der SIP-Server registriert die IP-Adressen der Clients und sendet diese Informationen an den SIP-Proxy, der die Anrufe vermittelt. Meistens sind SIP-Proxy und SIP-Registrar identisch.

Repeater Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.

Reset Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.

RFC Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.

Rijndael Siehe AES.

RIP Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.

RipeMD 160 RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.

RJ45 RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.

Roaming Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.

Router Ein Router ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze auf der Vermittlungsschicht des OSI-Modells. Datenpakete werden anhand von IP-Adressen übertragen. Über Routing-Tabellen werden die besten Wege (Routen) durch das Netzwerk festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle, z. B. OSPF oder RIP, aus.

Router Advertisement Router Advertisements sind Nachrichten, die der Router ins Netzwerk sendet. Diese verkünden die Anwesenheit des Routers im Netz. Ferner werden mithilfe von Router Advertisments Präfixe verteilt, die Autokonfiguration organisiert und der Standardrouter festgelegt.

Routing Routing bezeichnet das Festlegen von Wegen für die Nachrichtenübermittlung.

RSA Mithilfe des RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über die Signatur können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. RSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch DSA. RSA ist langsamer in der Schlüsselerzeugung aber schneller

	in der Schlüsselverarbeitung als DSA.
RTP	Mit dem Real-Time Transport Protocol (RTP) werden Audio- und Video-Daten (Streams) über IP-basierte Netzwerke übertragen.
RTS Threshold	Sobald die Anzahl der Frames im Datenpaket über der RTS-Schwelle (RTS Threshold) liegt, wird vor dem Senden eines Datenpakets eine Verbindungsüberprüfung (RTS/CTS-Handshake) durchgeführt.
RTSP	Das Real-Time Streaming Protocol (RTSP) steuert die Übertragung von Audio- und Videodaten (Streams) über IP-basierte Netzwerke. Während das Real-Time Transport Protocol (RTP) zur Übertragung der Nutzdaten dient, besteht die Funktion von RTSP hauptsächlich in der Steuerung der Datenströme.
Rückfrage	Bei der Rückfrage wird das Telefongespräch mit dem ersten Gesprächspartner gehalten, während man ein zweites Gespräch führt.
Rückruf bei besetzt	Siehe automatischer Rückruf bei besetzt (CCBS).
Rückruf bei Nichtmelden	Siehe automatischer Rückruf bei Nichtmelden (CCNR).
Rufnummernband	Siehe Rufnummernblock beim Anlagenanschluss.
Rufnummernblock	Siehe Anlagenanschluss und Durchwahl (VoIP).
Rufumleitung	Rufumleitung (Call Deflection, CD) ist ein Leistungsmerkmal. Ein Anruf kann weitergeleitet werden, ohne ihn vorher angenommen zu haben.
Rufverteilung	Bei der Rufverteilung in der Telefonanlage werden eingehende Telefongespräche bestimmten Rufnummern oder Anwendungen (Fernzugang, ISDN-Login, …) zugeordnet.
Ruhe vor dem Telefon	Siehe Anrufschutz.
S0-Bus	Der S0-Bus ist eine Schnittstelle beim ISDN-Basisanschluss und verbindet mehrere ISDN-Endgeräte mit dem NTBA. Der Bus wird über eine Vierdraht-Verkabelung realisiert. Siehe auch UP0.
S2M-Anschluss	Siehe Primärmultiplexanschluss.
SA	Eine sogenannte Sicherheitsverbindungen (Security Associations, SA) enthält Informationen über die Maßnahmen zur Sicherung der

Kommunikationsverbindung. Mindestens eine SA ist die Voraussetzung für den Aufbau einer gesicherten Verbindung. Eine SA enthält die IP-Adresse des Teilnehmers, das verwendete Authentifizierungsprotokoll, den verwendeten Verschlüsselungsalgorithmus, den Sicherheits-Parameter-Index (SPI), den Selektor und die Gültigkeitsdauer.

SAD Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die SAD enthält Informationen über jede Sicherheitsverbindung. Also welche Verschlüsselungsalgorithmen, Schlüssel, Protokolle, Sitzungsnummern oder Gültigkeitszeiträumen verwendet werden sollen. Für eine ausgehende Verbindung zeigt ein Eintrag der SPD auf einen Eintrag der SAD. Dadurch kann die SPD festlegen, welcher SA für ein bestimmtes Paket verwendet wird. Bei einer eingehende Verbindung wird die SAD angesprochen, um festzulegen, wie das Paket verarbeitet wird.

SCEP Das Simple Certificate Enrollment Protocol (SCEP) dient zur Verwaltung digitaler Zertifikate.

Schaltkontakt Über ein Telefon kann eine am Schaltkontakt angeschlossene Anlage, z. B. ein Türöffner, ein- und ausgeschaltet werden.

Scheduling Unter Scheduling versteht man einen Aufgabenplan. Bestimmte Aktionen (z. B. Deaktivierung einer Schnittstelle) werden durch Ereignisse (z. B. Zeit oder Änderung einer MIB-Variablen) ausgelöst.

Serielle Schnittstelle Die serielle Schnittstelle dient dem Datenaustausch zwischen Computern und Peripheriegeräten. Sie kann zur Konfiguration des Geräts oder zur Datenübertragung über eine IP-Infrastruktur verwendet werden (Serial over IP).

Server Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden.

SFP Small Form-factor Pluggable (SFP) ist eine Steckverbindung, die für extrem schnelles Ethernet entwickelt wurde.

SHA1 Secure-Hash-Algorithm Version 1 (SHA1) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.

SHDSL Symmetrical High-bit-rate Digital Subscriber Line. Siehe DSL.

Shell Die Shell ist eine Eingabeschnittstelle (z. B. Kommandozeile oder

grafische Benutzerschnittstelle) zwischen Computer und Benutzer.

Shorthold Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.

SIF Bei einer Stateful Inspection Firewall (SIF) wird die Weiterleitung eines Datenpakets nicht nur durch Quell- und Zieladressen oder Port bestimmt, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung.

SIP Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das Protokoll wird für IP-Telefonie (VoIP) verwendet.

SIP-Provider Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.

SMTP Das Simple Mail Transfer Protocol (SMTP) wird zum Austausch von E-Mails eingesetzt.

SNMP Mithilfe des Simple Network Management Protocol (SNMP) werden verschiedene Netzwerkkomponenten (z. B. Router, Server, usw.) von einem zentralen System aus konfiguriert, kontrolliert und überwacht. Die änderbaren Einstellungen der Netzwerkkomponenten sind dabei in einer Datenbank gespeichert – der Management Information Base (MIB). SNMP verwendet UDP. Die Netzwerkkomponente empfängt dabei Anfragen (Requests) auf Port 161, während das verwaltende System Bestätigungsmeldungen (TRAPs) auf Port 162 entgegennimmt.

SNTP Das Simple Network Time Protocol (SNTP) wird zur Zeitübertragung und Synchronisation zwischen Server und Client eingesetzt.

Softkey Als Softkey bezeichnet man eine Taste, deren Funktion von der zugehörigen Bildschirmanzeige bestimmt wird.

Spatial Streams Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der Übertragungsrate.

SPD Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die Security-Policy-Datenbank führt die Formen des Datenverkehrs auf, die gesichert werden sollen. Da-

zu werden Faktoren wie Quell- und Zieladresse des Datenpakets verwendet.

Splitter Mithilfe einer Breitbandanschlusseinheit (BBAE), umgangssprachlich Splitter, werden Signale, die über eine Teilnehmeranschlussleitung eintreffen, in Daten- und Telefonleitungen aufgeteilt.

SRTP Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die mithilfe von AES verschlüsselte Variante des Real-Time Transport Protocol (RTP).

SSH Secure Shell (SSH) ist ein Netzwerkprotokoll mit dem man eine verschlüsselte Verbindung zur Shell eines Geräts herstellen kann.

SSID Der Service Set Identifier (SSID) definiert ein Funknetzwerk, das auf IEEE 802.11 basiert. Der SSID ist der Netzwerkname des Wireless LAN. Alle Access Points und Clients, die zum gleichen Netzwerk gehören, verwenden denselben SSID. Die SSID-Zeichenfolge kann bis zu 32 Zeichen lang sein und wird allen Paketen unverschlüsselt vorangestellt. Mithilfe der SSID ANY kontaktiert ein Client alle erreichbaren Access Points. Dem Anwender werden daraufhin alle verfügbaren WLANs angezeigt und er kann das passende Netz auswählen. Wenn ein Access Point für verschiedene Netze verwendet wird, erhält jedes Funknetzwerk eine eigene MSSID (Multi Service Set Identifier).

SSL Secure Sockets Layer (SSL) ist ein Protokoll zur Datenverschlüsselung. Seit Version 3.1 wird die neue Bezeichnung Transport Layer Security (TLS) verwendet. SSL wird hauptsächlich für HTTPS verwendet, um die Datenübertragung zwischen Web-Server und Web-Browser zu verschlüsseln.

STAC Mithilfe von STAC wird die übertragene Datenmenge verringert (Datenkompression).

Standardroute Die Standardroute (Default Route) wird verwendet, falls keine andere passende Route vorhanden ist.

Standardrouter Siehe Default Gateway.

Standleitung Eine Standleitung (Leased Line) ist eine permanente Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz.

Statische IP-Adresse Im Gegensatz zu einer dynamischen IP-Adresse wird die statische IP-Adresse fest vom Anwender zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-

Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.

STUN-Server Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Ein STUN-Server ermöglicht VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Netzwerk.

Subadressierung Neben der ISDN-Telefonnummer kann eine Subadresse beim Verbindungsaufbau übertragen werden. Diese Subadresse überträgt eine beliebige Zusatzinformation. Diese kann genutzt werden, um z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt anzusprechen oder bestimmte Programme auf einem PC aufzurufen.

Subnetz Ein Teilnetz eines IP-Netzes wird als Subnetz bezeichnet. Ein Teilnetz wird wie ein normales Netzwerk über IP-Adresse und (Sub-)Netzmaske (IPv4) bzw. Präfixlänge (IPv6) definiert. Beispiel: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 mögliche IP-Adressen) ist ein Subnetz von 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 mögliche IP-Adressen).

Switch Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerksegmente miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells berieben werden. Das dem Switch vergleichbare Gerät der Bitübertragungsschicht wird als Hub bezeichnet.

SWYX SwyxWare ist eine softwarebasierte Kommunikationslösung für VoIP.

Syslog Das Syslog-Protokoll wird zur Übermittlung von Status-Meldungen in einem IP-Netzwerk verwendet. Verschiedene Netzwerkkomponenten können somit von einem zentralen System aus überwacht werden. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP-Port 514 gesendet.

Systemtelefon Ein Systemtelefon ist mit mehreren Funktions- und Sondertasten ausgestattet und kann die Leistungsmerkmale einer Telefonanlage nutzen.

T.38 T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.

TA Siehe Terminaladapter.

TACACS+ Das Terminal Access Controller Access Control System Plus (TACACS+) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern. Der TACACS+-Server authentifiziert den Client mittels der Überprüfung von z. B. Benutzername und Kennwort. Im Gegensatz zum UDP-basierten RADIUS-Protokoll verwendet TACACS+ TCP auf Port 49 und überträgt die gesamte Kommunikation verschlüsselt.

TAE Siehe Netzabschluss. Man unterscheidet zwischen F-codierten Steckverbindern für Telefone und N-codierten Steckverbindern für Faxgeräte, Modems und Anrufbeantworter.

TAPI Telephony Applications Programming Interface (TAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch CAPI.

TCP Beim Transmission Control Protocol (TCP) handelt es sich um ein verbindungsorientiertes Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungsorientierten Protokoll wird vor der Übertragung eine logische Verbindung aufgebaut und aufrechterhalten. Dies ermöglicht eine zuverlässige Übertragung der Daten. Allerdings werden ständig Kontrollinformationen neben dem eigentlichen Datenpaketen übertragen. Dies führt zu einem Anstieg des übertragenen Datenvolumens. Siehe auch UDP.

TCP-ACK-Paket Ein ACK-Signal (Acknowledgement = Bestätigung) wird bei einer Datenübertragung verwendet, um den Erhalt oder die Verarbeitung von Daten oder Befehlen zu bestätigen. TCP verwendet ACK-Signale zur Kommunikation.

TE Der Endgeräteanschluss (Terminal Equipment, TE) bezeichnet einen Anschluss bzw. eine Betriebsart. Der TE-Anschluss ist der Anschluss eines Endgeräts. Im TE-Betrieb wird das Gateway am internen S0 der Telefonanlage angeschlossen und stellt damit ein ISDN-Endgerät dar. Siehe auch NT.

TEI Der Terminal Endpoint Identifier (TEI) ist gemäß ISDN-Protokoll DSS1 eine Kennung zur Identifizierung der Endgeräte.

Telefax Siehe Fax.

Telefonnummer des Angerufenen anzei- Mithilfe von Connected Line Identification Presentation (COLP) wird die Telefonnummer des Angerufenen (B-Telefonnummer) zum An-

gen (COLP / COLR)	rufer übertragen. Mithilfe von Connected Line Identification Restriction (COLR) wird die Übertragung der Telefonnummer des Angerufenen zum Anrufer unterdrückt.
Telefonnummer des Anrufers anzeigen (CLIP / CLIR)	Mithilfe von Calling Line Identification Presentation (CLIP) wird die Telefonnummer des Anrufers (A-Telefonnummer) zum Angerufenen übertragen. CLIP off Hook übermittelt die Telefonnummer des anklopfenden Anrufers. Mithilfe von Calling Line Identification Restriction (CLIR) wird die Übertragung der Telefonnummer des Anrufers zum Angerufenen unterdrückt.
Telefonnummer unterdrücken	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR) und Telefonnummer des Angerufenen anzeigen (COLP / COLR).
Telnet	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
Terminaladapter	Mithilfe eines Terminaladapters (TA) können Endgeräte an eine Schnittstelle angeschlossen werden, an der sie nicht direkt betrieben werden können, z. B. analoge Endgeräte an einem ISDN-Anschluss.
TFE	Eine Türfreisprecheinrichtung (TFE) ist an Eingängen montiert und ein Teil eines Türsprechsystems, z. B. einer Telefonanlage.
TFTP	Das Trivial File Transfer Protocol (TFTP) regelt die Übertragung von Dateien. Im Vergleich zu FTP fehlen eine Möglichkeit zur Dateianzeige, eine Rechtevergabe und eine Benutzerauthentifizierung.
Tiger 192	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Time Service	Mithilfe des Time Protocol (time) wird Datum und Uhrzeit synchronisiert. Das Protokoll verwendet den Port 37 über TCP und UDP.
TK-Anlage	TK-Anlage ist eine andere Bezeichnung für eine Telefonanlage.
TLS	Siehe SSL.
Tonwahl	Siehe Mehrfrequenzwahlverfahren.
TOS	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
Traceroute	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpa-

	kete bis zum abgefragten Ziel-Host vermittelt werden.
Trigger	Unter Trigger versteht man einen Auslöseimpuls.
Triple DES	Siehe DES.
Trunk	Ein Trunk sind gebündelte Anschlüsse bzw. Übertragungskanäle. Siehe auch Bündel.
TTL	Die Time to live (TTL) ist die konfigurierte Gültigkeitsdauer eines Datenpakets. Beim Internet Protocol (IP) legt die TTL fest, wie viele Hops ein Datenpaket passieren darf. Der Maximalwert beträgt 255 Hops. Mit jedem Hop wird die TTL um 1 reduziert. Falls ein Datenpaket nach Ablauf seiner TTL noch nicht sein Ziel erreicht hat, wird es verworfen.
Twofish	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128,192 oder 256 Bit.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) ist eine DSL-Variante. Sie wurde als ANSI T1.413 entwickelt und als G.992.2 standardisiert. U-ADSL erlaubt die parallele Nutzung verschiedener Kommunikationstechniken, z. B. ISDN und POTS, und benötigt keinen Splitter.
Überprüfung der Rückroute	Falls bei einer Schnittstelle "Überprüfung der Rückroute" (Back Route Verify) aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden.
UDP	Beim User Datagram Protocol (UDP) handelt es sich um ein verbindungsloses Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungslosen Protokoll ist keine Kontrolle für die Auslieferung des Pakets integriert. Die Kontrolle muss in der Anwendungsschicht erfolgen. Im Gegenzug ist UDP schneller als verbindungsorientierte Protokolle.
ULA	Unique Local Addresses (ULA) sind IPv6-Adressen, die nicht geroutet werden. Sie können in privaten Netzen (z. B. einem LAN) verwendet werden. ULAs beginnen mit dem Präfix fd.
UMTS	Das Universal Mobile Telecommunications System (UMTS), auch als 3G bezeichnet, ist ein Mobilfunkstandard mit einer spezifizierten max. Datenübertragungsrate von 384 kbit/s bzw. 21 Mbit/s in Verbindung mit HSPA+.

Unicast Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertagen.

UP0 Der UP0-Anschluss ist eine Schnittstelle beim ISDN-Basisanschluss und verbindet genau ein ISDN-Endgerät mit dem NTBA. Der Anschluss wird über eine Zweidraht-Verkabelung realisiert und bietet eine höhere Reichweite als der S0-Bus.

UPnP Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.

Upstream Das Gateway leitet die Daten des eigenen Netzwerks weiter.

URL Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: http://www.example.org/index.htp (Web-Seite im Internet)

UUS Bei User to User Signalling (USS) können Textnachrichten mit anderen Teilnehmern ausgetauscht werden.

V.110 V.110 beschreibt ein Verfahren zur Anpassung von Bitströmen mit 0,6, 1,2, 2,4, 2,8, 7,2, 9,6, 12, 14,4, 19,2 und 38,4 kbit/s in den ISDN-Bitstrom von 64 kbit/s.

VDSL Very High Speed Digital Subscriber Line. Siehe DSL.

VID Siehe VLAN.

VLAN Ein Netzwerk kann in eines oder mehrere logische Teilnetze – sogenannte Virtual-Local-Area-Networks (VLAN) – aufgespalten werden, indem die Netzwerkkomponenten das Datenpaket eines definieren Teilnetzes nicht mehr in andere Teilnetze weiterleiten. Jedem VLAN wird eine eindeutige Nummer zugeordnet. Diese Nummer wird VLAN ID (VID) genannt und den Datenpaketen im VLAN-Tag zugeordnet.

Voice Mail Box Eine Voice Mail Box ist der persönliche Anrufbeantworter eines Benutzers in einem Voice Mail System.

Voice Mail System Ein Voice Mail System ermöglicht das Speichern, Abrufen und Weiterleiten von Sprachmitteilungen ähnlich wie ein Anrufbeantworter, jedoch mit weitaus mehr Optionen.

VoIP Voice over IP (VoIP), auch IP-Telefonie genannt, bezeichnet die Übertragung von Sprache über ein IP-Netzwerk. Der Auf- und Abbau der Telefonverbindung erfolgt dabei über Signalisierungsproto-

kolle, wie z. B. SIP.

VPN Mithilfe eines virtuellen privaten Netzwerks (VPN) werden private Datenpakete durch ein öffentliches Netzwerk transportiert. Die Informationen werden dabei durch Einkapselung in neue Protokolle von den öffentlich zugänglichen Daten getrennt, um sie an den vorgesehenen Empfänger zu leiten. Man spricht in diesem Zusammenhang auch von einem Tunnel, der zwischen den privaten Netzen der beiden Verbindungsteilnehmer aufgebaut wird. VPN-Protokolle sind IPSec, PPTP, L2TP und GRE.

VSS Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.

Wahlberechtigung Siehe Amtsberechtigung.

Wahlkontrolle Siehe Black / White List.

Wahlregeln Mithilfe der Wahlregeln können Anrufe abhängig von der gewählten Rufnummer (Zone) über festgelegte Provider bzw. Bündel geleitet werden.

Wählverbindung Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.

Wahlvorbereitung Die Wahlvorbereitung beschreibt die Eingabe der Telefonnummer vor dem Einleiten des Gesprächs, z. B. durch Abheben des Hörers.

Walled Garden Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.

WAN Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausgedehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.

Wartemusik Siehe Music On Hold.

WDS Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.

Web-Server Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.

Wechselsprechen Wechselsprechen ist ein Leistungsmerkmal. Mithilfe der Wechselsprechfunktion wird ein Anruf automatisch angenommen und Lauthören eingeschaltet. Hebt der angerufene Teilnehmer den Hörer ab,

	wird eine normale Sprechverbindung hergestellt.
WEP	Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.
WINS	Der Windows Internet Name Service (WINS) ist eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft. Wie DNS dient WINS der zentralen Namensauflösung. Siehe auch DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.
WMM	Wi-Fi Multimedia (WMM) priorisiert die Datenpakete unterschiedlicher Anwendungen und verbessert damit die Übertragung von Sprach-, Musik- und Videodaten in WLAN-Netzwerken. Dazu stellt WMM Quality-of-Service-Merkmale (QoS) für IEEE 802.11-basierte Netzwerke bereit.
WPA	Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.
WPA - Enterprise	WPA - Enterprise bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmer durch das Extensible Authentication Protocol (EAP). Nach erfolgreicher Authentisierung übermittelt der Server dem Client und dem Access Point einen gemeinsamen Schlüssel für die Datenübertragung im WLAN.
WPA - PSK	WPA - PSK bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmern über Preshared Keys. Dabei nutzen Access Point und Client die gleiche Zeichenfolge für die Schlüsselberechnung im WLAN. Diese Zeichenfolge muss von den Anwendern konfiguriert werden.
WPA 2	Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.
X.25	X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.
X.31	Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.
X.500	Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.
X.509	Der X.509-Standard beschreibt die Erstellung der Zertifikate für eine

	Public-Key-Infrastruktur (PKI).
X.75	X.75 ist eine standardisierte Protokollfamilie für ISDN-Netzwerke mit einer Übertragungsrate von 64 kbit/s.
XAuth	Mithilfe von XAUTH (Extended Authentication) wird IKE um weitere Authentifizierungsmechanismen ergänzt. Nach einer erfolgreichen IKE-Phase-1-Authentifizierung kann der Benutzer noch einmal separat identifiziert werden. Die Identifizierung erfolgt über Benutzername und Passwort, PAP, CHAP oder Hardware-basierte Systeme.
Zeitschlitz	Ein Zeitschlitz ist ein fest zugeordneter Zeitabschnitt innerhalb eines Übertragungsrahmens und entspricht meist einem Übertragungskanal.
Zertifikat	Ein Zertifikat identifiziert eine Person, eine Institution, ein Gerät oder eine Anwendung. Ein Public-Key-Zertifikat ist ein digitales Zertifikat und stellt eine Verbindung zwischen der Identität und einem öffentlichen Schlüssel her. Zertifikate mit öffentlichem Schlüsseln werden von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt. Nicht mehr vertrauenswürdige Zertifikate können über Zertifikatsperrlisten (Certificate Revocation List, CRL) deaktiviert werden.
Zone	Unter einer Zone versteht man eine Rufnummer oder mehrere Rufnummern, die mit der gleichen Sequenz beginnen.

Index

B

E

F

K

N

O

P

Q

R

S

T

U

V

W

X

Z