

Benutzerhandbuch RXL-Serie und bintec PSU XL

Referenz

Copyright© Version 5.9, 2012 Teldat GmbH

Rechtlicher Hinweis

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von Teldat-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.teldat.de .

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Teldat 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 Teldat-Gateways finden Sie unter www.teldat.de .

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

Marken

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

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

Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Teldat GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Teldat GmbH nicht gestattet.

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter www.teldat.de .

Wie Sie Teldat GmbH erreichen

Teldat 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.de

Inhaltsverzeichnis

Kapitel 1	Einleitung	1
Kapitel 2	Zum Handbuch	3
Kapitel 3	Inbetriebnahme	6
3.1	Aufstellen und Anschließen: bintec RXL12x00	6
3.1.1	bintec PSU XL	8
3.2	Reinigen.	9
3.3	Support Information	9
Kapitel 4	Grundkonfiguration	10
4.1	Voreinstellungen	10
4.1.1	Vorkonfigurierte Daten	10
4.2	System-Voraussetzungen	10
4.3	Vorbereitung	11
4.3.1	Daten sammeln	11
4.3.2	PC einrichten	13
4.3.3	Systempasswort ändern	15
4.4	Internetverbindung einrichten.	15
4.4.1	Internetverbindung über UMTS/LTE.	16
4.4.2	Konfiguration prüfen	16
4.5	Softwareaktualisierung	17
Kapitel 5	Reset	18
Kapitel 6	Technische Daten	19

6.1	Lieferumfang	19
6.2	Allgemeine Produktmerkmale	19
6.3	LEDs	22
6.4	Anschlüsse	23
6.5	Pin-Belegungen	24
6.5.1	Serielle Schnittstelle	25
6.5.2	USB-Console-Schnittstelle	25
6.5.3	USB-Schnittstelle	26
6.5.4	Ethernet-Schnittstellen	26
6.5.5	ISDN-BRI-Schnittstelle	27
6.5.6	XLR-Einbaubuchse am bintec RXL12x00	28
6.5.7	XLR-Einbaubuchsen am bintec PSU XL	29
6.6	WEEE-Information	30
Kapitel 7	Zugang und Konfiguration	31
7.1	Zugangsmöglichkeiten	31
7.1.1	Zugang über LAN	31
7.1.2	Zugang über die serielle Schnittstelle	34
7.1.3	Zugang über ISDN	36
7.2	Anmelden	37
7.2.1	Benutzernamen und Passwörter im Auslieferungszustand	37
7.2.2	Anmelden zur Konfiguration	38
7.3	Konfigurationsmöglichkeiten	39
7.3.1	GUI (Graphical User Interface)	39
7.3.2	SNMP Shell	56
7.4	BOOTmonitor	56
Kapitel 8	Assistenten	58

Kapitel 9	Systemverwaltung	59
9.1	Status	59
9.2	Globale Einstellungen	62
9.2.1	System	62
9.2.2	Passwörter	65
9.2.3	Datum und Uhrzeit	67
9.2.4	Systemlizenzen	71
9.3	Schnittstellenmodus / Bridge-Gruppen	74
9.3.1	Schnittstellen.	75
9.4	Administrativer Zugriff	77
9.4.1	Zugriff	77
9.4.2	SSH	78
9.4.3	SNMP.	82
9.5	Remote Authentifizierung	83
9.5.1	RADIUS	83
9.5.2	TACACS+	89
9.5.3	Optionen	92
9.6	Zertifikate	93
9.6.1	Zertifikatsliste	94
9.6.2	CRLs	104
9.6.3	Zertifikatsserver	105
Kapitel 10	Physikalische Schnittstellen	107
10.1	Ethernet-Ports	107
10.1.1	Portkonfiguration	108
10.2	ISDN-Ports	111
10.2.1	ISDN-Konfiguration	111
10.2.2	MSN-Konfiguration	114

10.3	UMTS/LTE.	118
10.3.1	UMTS/LTE.	118
Kapitel 11	LAN	125
11.1	IP-Konfiguration	125
11.1.1	Schnittstellen	125
11.2	VLAN	137
11.2.1	VLANs	138
11.2.2	Portkonfiguration	139
11.2.3	Verwaltung	140
Kapitel 12	Wireless LAN Controller	141
12.1	Wizard	141
12.1.1	Grundeinstellungen	142
12.1.2	Funkmodulprofil	143
12.1.3	Drahtlosnetzwerk	143
12.1.4	Automatische Installation starten	145
12.2	Controller-Konfiguration	147
12.2.1	Allgemein	148
12.3	Slave-AP-Konfiguration	150
12.3.1	Slave Access Points	150
12.3.2	Funkmodulprofile	155
12.3.3	Drahtlosnetzwerke (VSS)	162
12.4	Monitoring	167
12.4.1	Aktive Clients	167
12.4.2	Drahtlosnetzwerke (VSS)	168
12.4.3	Benachbarte APs	168
12.4.4	Rogue APs	169
12.5	Wartung	170

12.5.1	Firmware-Wartung	170
Kapitel 13	Netzwerk	173
13.1	Routen	173
13.1.1	IPv4-Routen	173
13.1.2	IPv6-Routen	179
13.1.3	Optionen	181
13.2	IPv6-Präfixe	183
13.2.1	IPv6-Präfixe	183
13.3	NAT.	187
13.3.1	NAT-Schnittstellen	187
13.3.2	NAT-Konfiguration	188
13.4	Lastverteilung	194
13.4.1	Lastverteilungsgruppen	194
13.4.2	Special Session Handling	199
13.5	QoS	203
13.5.1	QoS-Filter	203
13.5.2	QoS-Klassifizierung	207
13.5.3	QoS-Schnittstellen/Richtlinien	210
13.6	Zugriffsregeln	218
13.6.1	Zugriffsfiler	219
13.6.2	Regelketten	223
13.6.3	Schnittstellenzuweisung	225
13.7	Drop-In	227
13.7.1	Drop-In-Gruppen	227
Kapitel 14	Routing-Protokolle	230
14.1	RIP	230
14.1.1	RIP-Schnittstellen.	230

14.1.2	RIP-Filter	233
14.1.3	RIP-Optionen	235
14.2	OSPF	238
14.2.1	Bereiche	239
14.2.2	Schnittstellen	241
14.2.3	Globale Einstellungen	244
Kapitel 15	Multicast.	247
15.1	Allgemein	249
15.1.1	Allgemein	249
15.2	IGMP	249
15.2.1	IGMP	250
15.2.2	Optionen	253
15.3	Weiterleiten	254
15.3.1	Weiterleiten	254
15.4	PIM	255
15.4.1	PIM-Schnittstellen	256
15.4.2	PIM-Rendezvous-Punkte	259
15.4.3	PIM-Optionen	261
Kapitel 16	WAN.	263
16.1	Internet + Einwählen	263
16.1.1	PPPoE	266
16.1.2	PPTP	273
16.1.3	ISDN	278
16.1.4	UMTS/LTE.	287
16.1.5	IP Pools	292
16.2	IPv6-Tunnel	293
16.2.1	IPv6-Tunnel	293

16.3	Standleitung	296
16.3.1	Schnittstellen	297
16.4	Real Time Jitter Control	300
16.4.1	Regulierte Schnittstellen	301
Kapitel 17	VPN	303
17.1	IPSec	303
17.1.1	IPSec-Peers	305
17.1.2	Phase-1-Profilе	321
17.1.3	Phase-2-Profilе	329
17.1.4	XAUTH-Profilе	335
17.1.5	IP Pools	337
17.1.6	Optionen	338
17.2	L2TP	342
17.2.1	Tunnelprofile	342
17.2.2	Benutzer	346
17.2.3	Optionen	353
17.3	PPTP	353
17.3.1	PPTP-Tunnel	354
17.3.2	Optionen	362
17.3.3	IP Pools	363
17.4	GRE	364
17.4.1	GRE-Tunnel	364
Kapitel 18	Firewall	367
18.1	Richtlinien	369
18.1.1	IPv4-Filterregeln	369
18.1.2	IPv6-Filterregeln	372
18.1.3	QoS	375
18.1.4	Optionen	376

18.2	Schnittstellen	378
18.2.1	IPv4-Gruppen	378
18.2.2	IPv6-Gruppen	379
18.3	Adressen	380
18.3.1	Adressliste	380
18.3.2	Gruppen	382
18.4	Dienste	383
18.4.1	Diensteliste	383
18.4.2	Gruppen	385
Kapitel 19	VoIP	388
19.1	SIP	388
19.1.1	Optionen	388
Kapitel 20	Lokale Dienste	390
20.1	DNS	390
20.1.1	Globale Einstellungen	392
20.1.2	DNS-Server	394
20.1.3	Statische Hosts	396
20.1.4	Domänenweiterleitung	398
20.1.5	Cache	400
20.1.6	Statistik	401
20.2	HTTPS	402
20.2.1	HTTPS-Server	402
20.3	DynDNS-Client	403
20.3.1	DynDNS-Aktualisierung	403
20.3.2	DynDNS-Provider	405
20.4	DHCP-Server	407
20.4.1	DHCP Pool	407

20.4.2	IP/MAC-Bindung	410
20.4.3	DHCP-Relay-Einstellungen	412
20.5	CAPI-Server	412
20.5.1	Benutzer	413
20.5.2	Optionen	414
20.6	Scheduling.	415
20.6.1	Auslöser.	415
20.6.2	Aktionen	421
20.6.3	Optionen	432
20.7	Überwachung	433
20.7.1	Hosts	433
20.7.2	Schnittstellen.	436
20.7.3	Ping-Generator.	437
20.8	ISDN-Diebstahlsicherung	439
20.8.1	Optionen	439
20.9	UPnP	441
20.9.1	Schnittstellen.	442
20.9.2	Allgemein	443
20.10	Hotspot-Gateway	444
20.10.1	Hotspot-Gateway	446
20.10.2	Optionen	450
20.11	BRRP	450
20.11.1	Virtuelle Router	452
20.11.2	VR-Synchronisation	457
20.11.3	Optionen	459
Kapitel 21	Wartung	461
21.1	Diagnose	461
21.1.1	Ping-Test	461
21.1.2	DNS-Test	462

21.1.3	Traceroute-Test	463
21.2	Software & Konfiguration	463
21.2.1	Optionen	464
21.3	Neustart	469
21.3.1	Systemneustart.	469
Kapitel 22	Externe Berichterstellung.	470
22.1	Systemprotokoll	470
22.1.1	Syslog-Server	470
22.2	IP-Accounting	473
22.2.1	Schnittstellen.	473
22.2.2	Optionen	474
22.3	Benachrichtigungsdienst	475
22.3.1	Benachrichtigungsempfänger	475
22.3.2	Benachrichtigungseinstellungen	478
22.4	SNMP.	480
22.4.1	SNMP-Trap-Optionen	480
22.4.2	SNMP-Trap-Hosts	481
Kapitel 23	Monitoring.	483
23.1	Internes Protokoll.	483
23.1.1	Systemmeldungen	483
23.2	IPSec	484
23.2.1	IPSec-Tunnel	485
23.2.2	IPSec-Statistiken	487
23.3	ISDN/Modem	488
23.3.1	Aktuelle Anrufe	489
23.3.2	Anrufliste	489
23.4	Schnittstellen.	490

23.4.1	Statistik	490
23.5	Bridges	493
23.5.1	br<x>	493
23.6	Hotspot-Gateway	493
23.6.1	Hotspot-Gateway	493
23.7	QoS	494
23.7.1	QoS	494
23.8	OSPF	495
23.8.1	Status	495
23.8.2	Statistik	497
23.9	PIM	499
23.9.1	Allgemeine Statusangaben	499
23.9.2	Nicht-schnittstellen-spezifischer Status	500
23.9.3	Schnittstellenspezifische Zustände	503
	Glossar	507
	Index	553

Kapitel 1 Einleitung

bintec RXL12x00 ist ein Ethernet-basiertes System, das alle aktuellen Anforderungen des Marktes an ein leistungsfähiges und flexibles VPN-Gateway erfüllt.

bintec PSU XL dient als redundante Stromversorgung für ein oder zwei angeschlossene **bintec RXL12x00**. Es erkennt interne Stromversorgungsfehler angeschlossener Geräte automatisch und schaltet auf die alternative Stromzufuhr um.

Sicherheitshinweise

Was Sie im Umgang mit Ihrem **bintec** Gateway beachten müssen, erfahren Sie in den Sicherheitshinweisen, die Sie am Ende der gedruckten Anleitung finden.

Installation

Wie Sie Ihr Gerät anschließen, erfahren Sie in [Aufstellen und Anschließen: bintec RXL12x00](#) auf Seite 6. Dieses Kapitel sagt Ihnen auch, welche Vorbereitungen zur Konfiguration nötig sind.

Konfiguration

Konfigurationsgrundlagen erfahren Sie im Kapitel [Grundkonfiguration](#) auf Seite 10. Dort zeigen wir Ihnen, wie Sie Ihr Gerät von einem Windows-PC aus in Betrieb nehmen und weitere nützliche Hilfsprogramme installieren.

Passwort

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



Hinweis

Benutzername: *admin*

Passwort: *admin*



Hinweis

Denken Sie daran, das Passwort sofort zu ändern, wenn Sie sich das erste Mal auf Ihrem Gerät einloggen. Alle **bintec**-Geräte werden mit gleichem Passwort ausgeliefert. Sie sind daher erst gegen einen unautorisierten Zugriff geschützt, wenn Sie das Passwort ändern. Die Vorgehensweise bei der Änderung von Passwörtern ist im Kapitel [Systempasswort ändern](#) auf Seite 15 beschrieben.

Workshops

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

Dime Manager

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

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

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

Kapitel 2 Zum Handbuch

Dieses Dokument ist gültig für **bintec**-Geräte mit einer System-Software ab Software-Version 9.1.2.

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

Benutzerhandbuch - Referenz

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

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

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

Symbolübersicht

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

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

Auszeichnungselemente

Auszeichnung	Verwendung
•	Kennzeichnet Listen.
Menü -> Untermenü Datei -> Öffnen	Kennzeichnet Menüs und Untermenüs im GUI und in der Windows-Oberfläche.
nicht-proportional (Courier), z. B. <code>ping</code> <code>192.168.0.254</code>	Kennzeichnet Kommandos, die Sie wie dargestellt eingeben müssen.
fett, z. B. Windows-Startmenü	Kennzeichnet Tasten, Tastenkombinationen und Windows-Begriffe.
fett, z. B. Lizenzschlüssel	Kennzeichnet Felder im GUI .
kursiv, z. B. <i>keiner</i>	Kennzeichnet Werte, die Sie eintragen bzw. die eingestellt werden können.
Online: blau und kursiv, z. B. www.teldat.de	Kennzeichnet Hyperlinks.

Kapitel 3 Inbetriebnahme



Achtung

Vor Installation und Inbetriebnahme Ihres Geräts lesen Sie bitte aufmerksam die Sicherheitshinweise. Diese finden Sie am Ende der gedruckten Anleitung.

3.1 Aufstellen und Anschließen: bintec RXL12x00



Hinweis

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



Achtung

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



Hinweis

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

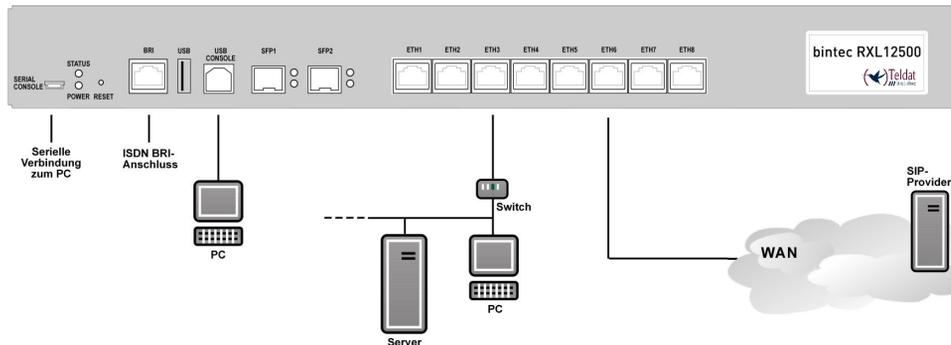


Abb. 2: Anschlussmöglichkeiten **bintec RXL12x00**

Gehen Sie beim Aufstellen und Anschließen in der folgenden Reihenfolge vor (siehe Anschlusspläne für die einzelnen Geräte im Kapitel *Technische Daten* auf Seite 19):

- (1) Befestigen Sie die mitgelieferten Gummifüßchen an den markierten Flächen an der Unterseite des Geräts.
- (2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage oder installieren Sie Ihr Gerät mit Hilfe der mitgelieferten Winkel in einem 19-Zoll-Schrank.
- (3) LAN
Zur Standardkonfiguration Ihres Geräts über Ethernet verbinden Sie den ersten Switch-Port (**ETH1**) Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.
- (4) Netzanschluss
Schließen Sie das Gerät an eine Steckdose an. Der Netzanschluss befindet sich auf der Geräterückseite.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- ISDN-BRI

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

- Weitere LANs und WAN

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

- Serielle Verbindung

Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs mit einer der seriellen Schnittstellen des Geräts (**USB Console** oder **Serial Conso-**

le). Beide Konsolenanschlüsse sind im Auslieferungszustand auf eine Geschwindigkeit von 115200 Baud eingestellt. Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

Das Gerät ist nun für die Konfiguration mit dem **GUI** vorbereitet. Im Kapitel *Grundkonfiguration* auf Seite 10 finden Sie ausführliche Schritt-für-Schritt-Anleitungen zu den grundlegenden Funktionen Ihres Geräts.

3.1.1 bintec PSU XL



Warnung

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

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

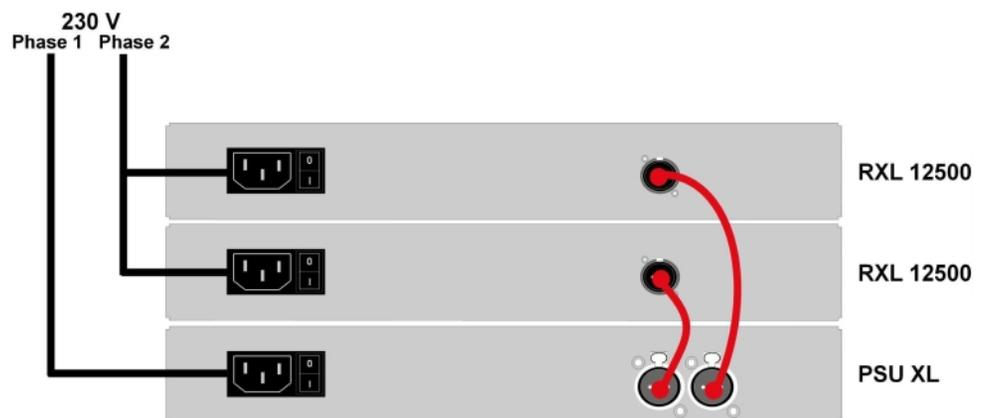


Abb. 3: Anschlussmöglichkeit **bintec PSU XL** an **bintec RXL12x00**

Siehe auch die Belegung der XLR-Einbaubuchsen *XLR-Einbaubuchse am bintec RXL12x00* auf Seite 28 und *XLR-Einbaubuchsen am bintec PSU XL* auf Seite 29.

3.2 Reinigen

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



Achtung

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

3.3 Support Information

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

Email hotline@teldat.de

Internationale Supportkoordinati-
on Telefon: +49 911 9673 1550

Fax: +49 911 9673 1599

Endkunden-Hotline 0900 1 38 65 93 (1,10 €/min aus dem deutschen Festnetz)

Ausführliche Informationen zu unseren Support Leistungen erhalten Sie unter www.teldat.de.

Kapitel 4 Grundkonfiguration

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

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

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

4.1 Voreinstellungen

4.1.1 Vorkonfigurierte Daten

Ihr Gerät wird mit einer vordefinierten IP-Konfiguration ausgeliefert:

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

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

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



Hinweis

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

Die Vorgehensweise bei der Änderung von Passwörtern finden Sie unter [Systempasswort ändern](#) auf Seite 15.

4.2 System-Voraussetzungen

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

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

- Betriebssystem Microsoft Windows ab Windows XP
- Internet Explorer 8 oder 9, Mozilla Firefox ab Version 3.
- Installierte Netzwerkkarte (Ethernet)
- DVD-Laufwerk
- Installiertes TCP/IP-Protokoll (siehe [PC einrichten](#) auf Seite 13)

4.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

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

Darüber hinaus können Sie ...

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

4.3.1 Daten sammeln

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

Gegebenenfalls können Sie die Beispielwerte übernehmen.

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

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

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

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

Administrator.

Grundkonfiguration

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

Basisinformationen

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

Internetzugang über ADSL

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

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

Daten für den Internetzugang über ADSL

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

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

Zusätzliche Informationen für T-Online

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



Hinweis

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

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

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

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

Ihr Benutzername könnte dann so aussehen:

00012345678906112345678#0001 @t-online.d

Daten für den Internetzugang über UMTS/LTE

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

4.3.2 PC einrichten

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

- Stellen Sie sicher, dass das TCP/IP-Protokoll auf dem PC installiert ist.
- Weisen Sie Ihrem PC eine feste IP-Adresse zu.

TCP/IP-Protokoll prüfen

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

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

- (2) Klicken Sie auf **LAN-Verbindung**.
- (3) Klicken Sie im Statusfenster auf **Eigenschaften**.
- (4) Suchen Sie in der Liste der Netzwerkkomponenten den Eintrag **Internetprotokoll (TCP/IP)**.

TCP/IP-Protokoll installieren

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

- (1) Klicken Sie im Statusfenster der **LAN-Verbindung** zunächst auf **Eigenschaften**, dann auf **Installieren**.
- (2) Wählen Sie den Eintrag **Protokoll**.
- (3) Klicken Sie auf **Hinzufügen**.
- (4) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **OK**.
- (5) Folgen Sie den Anweisungen am Bildschirm und starten Sie zum Schluss den Rechner neu.

PC IP-Adresse zuweisen

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

- (1) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
- (2) Wählen Sie **Folgende IP-Adresse verwenden** und geben Sie eine geeignete IP-Adresse ein.

Gateway IP-Adresse im PC eintragen

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

- (1) Geben Sie in **Internetprotokoll (TCP/IP) -> Eigenschaften** unter **Standardgateway** die IP-Adresse Ihres Gateways ein.
- (2) Tragen Sie unter **Folgende DNS-Serveradressen verwenden** die IP-Adresse Ihres Geräts ein.
- (3) Klicken Sie auf **OK**.
- (4) Schließen Sie das Statusfenster mit **OK**.

Der Rechner verfügt nun über eine IP-Konfiguration.



Hinweis

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

4.3.3 Systempasswort ändern

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

Gehen Sie dazu vor wie folgt:

- (a) Gehen Sie in das Menü **Systemverwaltung** -> **Globale Einstellungen** -> **Passwörter**.
- (b) Geben Sie für **Systemadministrator-Passwort** ein neues Passwort ein.
- (c) Geben Sie das neue Passwort noch einmal unter **Systemadministrator-Passwort bestätigen** ein.
- (d) Klicken Sie auf **OK**.
- (e) Speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

Beachten Sie folgende Regeln zum Passwortgebrauch:

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

4.4 Internetverbindung einrichten

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

4.4.1 Internetverbindung über UMTS/LTE

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

- (1) Gehen Sie im in das Menü **Assistenten->Internetzugang**.
- (2) Legen Sie mit **Neu** einen neuen Eintrag an und wählen Sie als **Verbindungstyp** *UMTS/LTE*.
- (3) Folgen Sie den Schritten, die der Assistent vorgibt. Der Assistent verfügt über eine eigene Online-Hilfe, die Ihnen ggf. notwendige Informationen vermittelt.
- (4) Nachdem Sie den Assistenten beendet haben, speichern Sie die Konfiguration mit dem Button **Konfiguration speichern** oberhalb der Menünavigation.

4.4.2 Konfiguration prüfen

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

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

- (1) Testen Sie die Verbindung zum Gerät. Klicken Sie im Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihrer Anlage ein (z. B. `192.168.0.254`). Es erscheint ein Fenster mit dem Hinweis "Antwort von...".
- (2) Testen Sie den Internetzugang, indem Sie im Internet Browser www.teldat.de eingeben. Auf den Internet-Seiten der Teldat GmbH finden Sie Neuigkeiten, Updates und weiterführende Dokumentation.



Hinweis

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

4.5 Softwareaktualisierung

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

Gehen Sie folgendermaßen vor:

- (1) Gehen Sie in das Menü **Wartung->Software & Konfiguration**.
- (2) Wählen Sie unter **Aktion** *Systemsoftware aktualisieren* und unter **Quelle** *Aktuelle Software vom Teldat-Server*
- (3) Bestätigen Sie mit **Los**.

Optionen

Aktuell Installierte Software	
BOSS	V.9.1 Rev.2 IPSec from 2011/06/10 00:00:00
Systemlogik	0.0
Optionen zu Software und Konfiguration	
Aktion	Systemsoftware aktualisieren
Quelle	Aktuelle Software vom Teldat-Server

Los

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



Achtung

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

Kapitel 5 Reset

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

Manueller Reset des Gerätes

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

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

Kapitel 6 Technische Daten

In diesem Kapitel sind die Hardware-Eigenschaften von **bintec RXL12x00** und **bintec PSU XL** zusammengefasst.

6.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

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

6.2 Allgemeine Produktmerkmale

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

Allgemeine Produktmerkmale bintec RXL12x00 , bintec PSU XL

Eigenschaft	bintec RXL12x00	bintec PSU XL
Maße und Gewicht:		
Gerätemaße ohne Kabel (B x H x T)	19" Gehäuse (482,6 mm x 220 mm x 45 mm, mit Winkeln)	19" Gehäuse (482,6 mm x 220 mm x 45 mm, mit Winkeln)
Gewicht	ca. 2,7 kg	ca. 2,6 kg

Eigenschaft	bintec RXL12x00	bintec PSU XL
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 4 kg	ca. 3 kg
Speicher	1 GB RAM, 128 MB Flash-ROM	-
Flash Card Slot	unterstützt SD-Flash-Karten bis zu 32 GB (SD 2.0)	-
LEDs	24 (1x Power, 1x Status, 1x2 BRI, 8x2 Ethernet, 2x2 SFP-Funktion)	2 x Power (Power 1 und Power 2)
Leistungsaufnahme Gerät	Leerlauf 15 Watt, Last 30 Watt, max. 40 Watt	max. 2x 40 Watt, typ. 2x 15 Watt
Spannungsversorgung	1) Kaltgeräteanschluss Voltage Range 85 ~ 264 V AC Frequency Range 47 ~ 63 Hz Efficiency (Typ.) 79 % 2) 12V-XLR-Anschluss (männlich) zum Anschluss an bintec PSU XL	1) 1 x Kaltgeräteanschluss Voltage Range 85 ~ 264 V AC Frequency Range 47 ~ 63 Hz Efficiency (Typ.) 79 %
Umweltanforderungen:		
Lagertemperatur	-25 °C bis +70 °C	-25 °C bis +70 °C
Betriebstemperatur	0 °C bis +40 °C	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:		
Ethernet IEEE 802.3 LAN (8-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	-

Eigenschaft	bintec RXL12x00	bintec PSU XL
ISDN-BRI	Euro-ISDN (Mehrgeräte- und Anlagenanschluss, für In-Haus-Verkabelung) Nur TE-Modus	-
SFP LAN Port	SFP Slot für gängige optische 10/100/1000 Mbit/s Ethernet SFP Module, nicht hotswap-fähig	-
Console/RS232	Baudraten: 1200 - 115200 Baud, Standard: 115200 Baud	-
USB Console (Type B)	Baudraten: 1200 - 115200 Baud, Standard: 115200 Baud	-
USB (Type A)	Buchse zum Anschluss eines UMTS-Sticks.	-
Vorhandene Buchsen:		
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse	-
USB Console	Standard USB-Type-B-Buchse	-
USB	Standard USB-Type-A-Buchse	-
Ethernet-Schnittstellen	RJ45-Buchse	-
ISDN-BRI-Schnittstelle	RJ45-Buchse	-
Spannungsversorgung	1) 1x Kaltgeräteanschluss zur primären Stromversorgung 2) 1 x XLR-Buchse (Eingang) zur redundanten Stromversorgung, 12V DC	1) 1x Kaltgeräteanschluss zur primären Stromversorgung 2) 2 x XLR-Buchse (Ausgang) zur redundanten Stromversorgung, 12V DC
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
Mitgelieferte Software	Dime Manager auf DVD	-
Mitgelieferte Dokumentation	Kurzanleitung und Sicherheitshinweise	Kurzanleitung und Sicherheitshinweise

Eigenschaft	bintec RXL12x00	bintec PSU XL
	Benutzerhandbuch bintec Dime Manager auf DVD	
Online-Dokumentation	Benutzerhandbuch Workshops Release Notes, falls erforderlich	-

6.3 LEDs

Die LEDs geben Aufschluss über Aktivitäten und Zustände des Geräts.

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

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



Abb. 4: Anordnung der LEDs

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

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

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
POWER	grün	an	Stromversorgung ist angeschlossen.
		aus	Keine Stromversorgung.
STATUS	grün	an	Nach dem Einschalten: Das Gerät wird gestartet. Während des Betriebs: Es ist ein Fehler aufgetreten.

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

6.4 Anschlüsse

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



Abb. 5: Netzanschluss und die XLR-Buchse (**bintec RXL12x00**)



Abb. 6: Netzanschluss und die XLR-Buchsen (**bintec PSU XL**)

Alle anderen Anschlüsse befinden sich auf der Vorderseite des Geräts.

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

Die Anschlüsse sind folgendermaßen angeordnet:

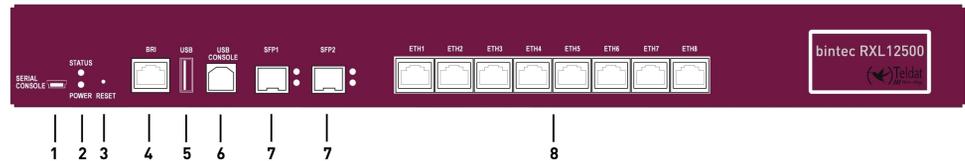


Abb. 7: **bintec RXL12x00** Vorderseite

bintec RXL12x00 Vorderseite

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

6.5 Pin-Belegungen

6.5.1 Serielle Schnittstelle

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

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

1 5



Abb. 8: 5-polige Mini-USB-Buchse

Die Pin-Belegung ist wie folgt:

Pin-Belegung der Mini-USB-Buchse

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

Sie benötigen einen Seriell-USB-Treiber für den Baustein CP210x. Diesen können Sie von www.teldat.de herunterladen.

6.5.2 USB-Console-Schnittstelle

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

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

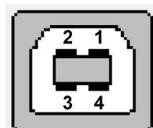


Abb. 9: USB-Type-B-Buchse

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



Hinweis

Sie benötigen einen Seriell-USB-Treiber für den Baustein CP210x. Diesen können Sie von www.teldat.de herunterladen.

6.5.3 USB-Schnittstelle

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

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



Abb. 10: USB-Type-A-Buchse

Die Pin-Belegung ist wie folgt:

Pin-Belegung der USB-Type-A-Buchse

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

6.5.4 Ethernet-Schnittstellen

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

Der 8-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Der Anschluss erfolgt über RJ45-Buchsen.

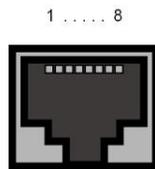


Abb. 11: Ethernet-10/100/1000 Base-T-Schnittstelle (RJ45-Buchse)

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 -

6.5.5 ISDN-BRI-Schnittstelle

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

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

Der Anschluss erfolgt über eine RJ45-Buchse:

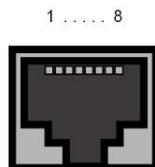


Abb. 12: ISDN-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss im TE-Modus

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

6.5.6 XLR-Einbaubuchse am bintec RXL12x00

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



Abb. 13: XLR-Einbaubuchse

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

Dreipolige XLR-Buchse (männlich)

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

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

6.5.7 XLR-Einbaubuchsen am bintec PSU XL

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



Abb. 14: XLR-Einbaubuchse

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

Dreipolige XLR-Buchse (weiblich)

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

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

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 tjänat ut ska kasseras och lämnas till de förutsedda sortergårdarna och skiljas från normalt hushållsavfall.



Tegnet på apparatet som viser en avfallcontainer med et kryss 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 κοντέινερ 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.



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



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



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



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

Kapitel 7 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

7.1 Zugangsmöglichkeiten

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

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

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

7.1.1 Zugang über LAN

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



Achtung

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

7.1.1.1 HTTP/HTTPS

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

- `http://192.168.0.254`
- oder
- `https://192.168.0.254`

7.1.1.2 Telnet

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

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

Gehen Sie folgendermaßen vor:

Windows

- (1) Klicken Sie im Windows-Startmenü auf **Ausführen...**
- (2) Geben Sie `telnet <IP-Adresse Ihres Geräts>` ein.
- (3) Klicken Sie auf **OK**.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (4) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 38.

Unix

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

- (1) Geben Sie `telnet <IP-Adresse Ihres Geräts>` in ein Terminal ein.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (2) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 38.

7.1.1.3 SSH

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

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

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

Schlüssel zur Verschlüsselung

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

- (1) Loggen Sie sich auf eine der bereits verfügbaren Arten auf Ihrem Gerät ein (z. B. über Telnet - zum Login siehe [Anmelden](#) auf Seite 37).
- (2) Am Eingabe-Prompt geben Sie `update -i` ein. Sie befinden sich auf der Flash Management Shell.
- (3) Rufen Sie eine Liste aller auf dem Gerät gespeicherten Dateien auf: `ls -al`.

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

```
Flash-Sh > ls -al

Flags Version Length Date Name ...
Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860
Vrw-pl--f 0.0 350 2004/09/07 10:44:14 sshd_host_rsa_key.pub
Vrw-pl--f 0.0 1011 2004/09/07 10:44:12 sshd_host_rsa_key
Vrw-pl--f 0.0.01 730 2004/09/07 10:42:17 sshd_host_dsa_key.pub
Vrw-pl--f 0.0.01 796 2004/09/07 10:42:16 sshd_host_dsa_key

Flash-Sh >
```



Hinweis

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

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

- (1) Verlassen Sie die Flash Management Shell mit `exit`.
- (2) Rufen Sie das **GUI** auf und melden Sie sich an Ihrem Gerät an (siehe [Das GUI aufrufen](#) auf Seite 41).
- (3) Stellen Sie sicher, dass als Sprache *Deutsch* gewählt ist.
- (4) Kontrollieren Sie den Schlüsselstatus im Menü **Systemverwaltung->Administrativer Zugriff->SSH**. Wenn beide Schlüssel verfügbar sind, sehen Sie in den beiden Feldern **RSA-Schlüsselstatus** und **DSA-Schlüsselstatus** den Wert *Generiert*.
- (5) Wenn Sie in einem der beiden Felder oder in beiden Feldern den Wert *Nicht generiert* sehen, so müssen Sie den entsprechenden Schlüssel erzeugen lassen. Um die Schlüssel vom Gerät erzeugen zu lassen, klicken Sie auf **Generieren**.
Das Gerät erzeugt den entsprechenden Schlüssel und speichert ihn im FlashROM.

Generiert zeigt die erfolgreiche Generierung an.

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

Login über SSH

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

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

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

UNIX

- (1) Geben Sie `ssh <IP-Adresse des Geräts>` in einem Terminal ein.
Das Login-Prompt-Fenster wird angezeigt, sie befinden sich auf der SNMP Shell des Geräts.
- (2) Fahren Sie mit [Anmelden](#) auf Seite 37 fort.

Windows

- (1) Wie eine SSH-Verbindung aufgebaut wird, hängt stark von der verwendeten Software ab. Beachten Sie die Dokumentation des von Ihnen verwendeten Programms.
Sobald Sie sich mit dem Gerät verbunden haben, wird das Login-Prompt-Fenster angezeigt. Sie befinden sich auf der SNMP Shell des Geräts.
- (2) Fahren Sie mit [Anmelden](#) auf Seite 37 fort.



Hinweis

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

7.1.2 Zugang über die serielle Schnittstelle

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

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

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

Windows

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

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

- (1) Klicken Sie im Windows-Startmenü auf **Programme -> Zubehör -> Kommunikation -> HyperTerminal -> Gerät an COM1** (bzw. **Gerät an COM2**, wenn Sie die COM2-Schnittstelle des Rechners benutzen), um HyperTerminal zu starten.
- (2) Drücken Sie die **Eingabetaste** (evtl. mehrmals), wenn sich das HyperTerminal-Fenster geöffnet hat.

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

Überprüfen

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

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

- (1) Klicken Sie auf **Datei -> Eigenschaften**.
- (2) Klicken Sie im Register **Verbinden mit** auf **Konfigurieren**
Folgende Einstellungen sind erforderlich:
 - Bits pro Sekunde: *9600*
 - Datenbits: *8*
 - Parität: *Keiner*
 - Stopbits: *1*
 - Flusssteuerung: *Keiner*
- (3) Tragen Sie die Werte ein und klicken Sie auf **OK**.
- (4) Stellen Sie im Register **Einstellungen** ein:
 - Emulation: *VT100*
- (5) Klicken Sie auf **OK**.

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

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

Unix

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

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

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

7.1.3 Zugang über ISDN

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

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



Hinweis

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

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

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

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

- (1) Schließen Sie Ihr Gerät an das ISDN an.
- (2) Loggen Sie sich wie gewohnt als Administrator auf dem Gerät im Remote-LAN ein.
- (3) Geben Sie in der SNMP-Shell `isdnlogin <Rufnummer des ISDN-Anschlusses Ihres Geräts> ein`, z. B. `isdnlogin 1234`.
- (4) Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.

Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 38.

7.2 Anmelden

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

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

7.2.1 Benutzernamen und Passwörter im Auslieferungszustand

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

Benutzernamen und Passwörter im Auslieferungszustand

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

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

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

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



Achtung

Alle **bintec**-Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter nicht geändert werden. Die Vorgehensweise bei der Änderung von Passwörtern ist unter *Passwörter* auf Seite 65 beschrieben.

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

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

7.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in *Zugangsmöglichkeiten* auf Seite 31 beschrieben.

GUI(Graphical User Interface)

So loggen Sie sich über die HTML-Oberfläche ein:

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

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

SNMP-Shell

So loggen Sie sich auf der SNMP-Shell ein:

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

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

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

7.3 Konfigurationsmöglichkeiten

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

Sie haben folgende Möglichkeiten, Ihr Gerät zu konfigurieren:

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



Hinweis

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

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

Verbindungs- und Konfigurationsarten

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

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



Hinweis

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

7.3.1 GUI (Graphical User Interface)

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

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

Es ist in Ihr Gerät integriert und steht in Englisch zur Verfügung. Weitere Sprachen können, falls erwünscht, im Download-Bereich [Software & Konfiguration](#) auf Seite 463 auf www.teldat.de heruntergeladen und auf dem Gerät installiert werden. Gehen Sie hierzu vor wie in [Optionen](#) auf Seite 464 beschrieben.

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

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

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

Automatisches Aktualisierungsintervall <input type="text" value="300"/> Sekunden Übernehmen		
! Warnung: Systempasswort nicht geändert!		
Systeminformationen		
Uptime	10 Tage(e) 22 Stunde(n) 42 Minute(n)	
Systemdatum	Donnerstag, 13 Apr 2000, 05:21:41	
Seriennummer	SR6AAA009400008	
BOSS-Version	V.9.1 Rev. 2 IPSec from 2012/03/23 00:00:00	
Letzte gespeicherte Konfiguration	Samstag, 26 Feb 2000, 03:52:50	
Ressourceninformationen		
CPU-Nutzung	0%	
Arbeitsspeichernutzung	23.1/63.9 MByte (36%)	
ISDN Verwendung Extern	0 / 2 B-Kanäle	
Aktive Sitzungen (SIF, RTP, etc...)	3	
Aktive IPSec-Tunnel	0 / 2	
Physikalische Schnittstellen		
Schnittstelle	Verbindungsinformation	Link
en1-0	192.168.0.254 / 255.255.255.0	
en1-4	Nicht konfiguriert / Nicht konfiguriert	
WLAN1	Access-Point / Verwendeter Kanal - / 0 Clients / FW: 2.0.0.0	
bri-0	Nicht konfiguriert	
ADSL	0	kbit/s Downstream
	0	kbit/s Upstream
WAN-Schnittstellen		
Beschreibung	Verbindungsinformation	Link
PPPoE1		
Branch_Peer-1		
Branch_Peer-2		

Abb. 16: **GUI** Startseite

7.3.1.1 Das GUI aufrufen

- (1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind (siehe [Aufstellen und Anschließen: bintec RXL12x00](#) auf Seite 6).
- (2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe [PC einrichten](#) auf Seite 13).
- (3) Öffnen Sie einen Webbrowser.
- (4) Geben Sie `http://192.168.0.254` in das Adressfeld des Webbrowsers ein.
- (5) Geben Sie in das Feld **User** `admin` und in das Feld **Password** ein und klicken Sie auf **LOGIN**.

Sie befinden sich nun im Statusmenü des **GUI** Ihres Geräts (siehe [Status](#) auf Seite 59).

7.3.1.2 Bedienelemente

GUI Fenster

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

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

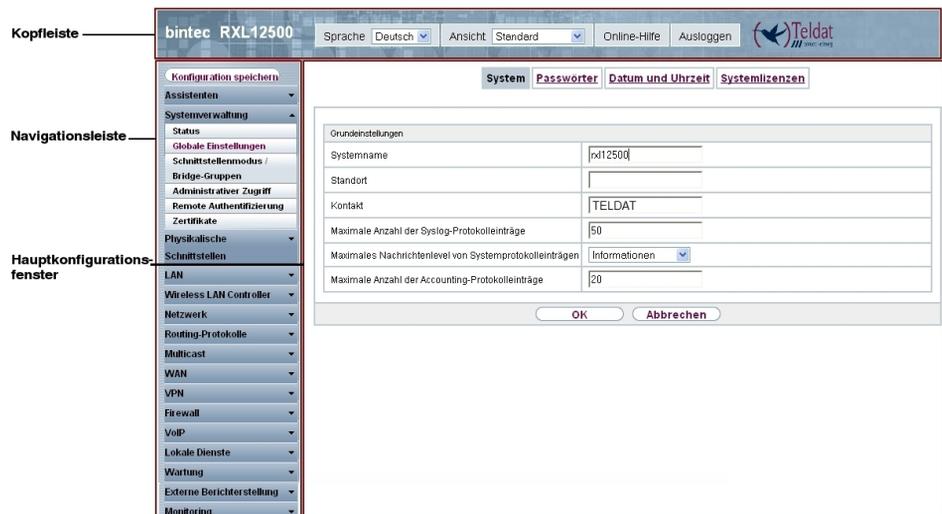


Abb. 17: Bereiche des GUI

Kopfleiste



Abb. 18: GUI Kopfleiste

GUI Kopfleiste

Menü	Funktion
Sprache <input type="text" value="Deutsch"/>	Sprachauswahl: Wählen Sie in dem Dropdown-Menü die gewünschte Sprache aus, in der das GUI angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen Deutsch und Englisch.
Ansicht <input type="text" value="Standard"/>	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: <ul style="list-style-type: none"> • Konfiguration speichern, vorherige Boot-Konfiguration sichern, dann verlassen. • Konfiguration speichern, dann verlassen. • Ohne zu speichern verlassen.

Navigationsleiste



Abb. 19: Konfiguration speichern Schaltfläche



Abb. 20: Menüs

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

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

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

Sie haben folgende zwei Wahlmöglichkeiten:

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

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

Die Navigationsleiste enthält weiterhin die Hauptkonfigurationsmenüs und deren Untermenüs.

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

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

Statusseite

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

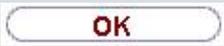
Hauptkonfigurationsfenster

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

Konfigurationselemente

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

GUI Schaltflächen

Schaltfläche	Funktion
	Aktualisiert die Ansicht.
	Wenn Sie einen neu konfigurierten Listeneintrag nicht sichern wollen, machen Sie diesen und die evtl. getätigten Einstellungen durch Abbrechen rückgängig.
	Bestätigt die Einstellungen eines neuen Eintrags und die Parameteränderungen in einer Liste.

Schaltfläche	Funktion
	Startet die konfigurierte Aktion sofort.
	Ruft das Untermenü zum Anlegen eines neuen Eintrags auf.
	Fügt einen Eintrag zu einer internen Liste hinzu.

GUI Schaltflächen für spezielle Funktionen

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

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

GUI Symbole

Symbol	Funktion
	Löscht den entsprechenden Listeneintrag.
	Zeigt das Menü zur Änderung der Einstellungen eines Eintrags an.
	Zeigt die Details eines Eintrags an.
	Verschiebt einen Eintrag. Es öffnet sich eine Combobox, in der Sie auswählen können, vor/hinter welchen Listeneintrag der ausgewählte Eintrag verschoben werden soll.
	Legt einen weiteren Listeneintrag vorher an und öffnet das Konfigurationsmenü.
	Setzt den Status des Eintrags auf <i>Inaktiv</i> .
	Setzt den Status des Eintrags auf <i>Aktiv</i> .
	Kennzeichnet den Status "Ruhend" einer Schnittstelle oder einer Verbindung.

Symbol	Funktion
	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-Bandskan aus.
	Zeigt die nächste Seite einer Liste an.
	Zeigt die vorherige Seite einer Liste an.

In der Listenansicht haben Sie folgende Bedienfunktionen zur Auswahl:

GUI Listenoptionen

Menü	Funktion
Aktualisierungsintervall	<p>Hier können Sie das Intervall einstellen, in dem die Ansicht aktualisiert werden soll.</p> <p>Geben Sie dazu einen Zeitraum in Sekunden in das Eingabefeld ein und bestätigen Sie mit Übernehmen.</p>
Filter	<p>Sie haben die Möglichkeit, die Einträge einer Liste nach bestimmten Kriterien filtern und entsprechend anzeigen zu lassen.</p> <p>Sie können die Anzahl der pro Seite angezeigten Einträge bestimmen, indem Sie in Ansicht x pro Seite die gewünschte Zahl eingeben.</p> <p>Mit den Tasten  und  blättern Sie eine Seite vor bzw. eine Seite zurück.</p> <p>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.</p>

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

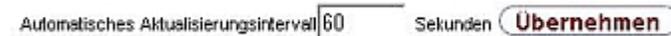


Abb. 21: Konfiguration des Aktualisierungsintervalls



Abb. 22: Liste filtern

Struktur der GUI Konfigurationsmenüs

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

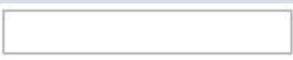
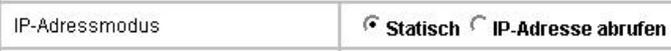
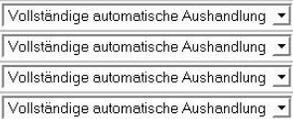
GUI Menüstruktur

Menü	Funktion
Basis-Konfigurationsmenü/Liste	Bei Auswahl eines Menüs der Navigationsleiste wird zunächst das Menü mit den Basisparametern angezeigt. Bei einem Untermenü mit mehreren Seiten wird jeweils das Menü mit den Basisparametern der ersten Seite angezeigt. Das Menü enthält entweder eine Liste aller konfigurierten Einträge oder die Grundeinstellungen für die jeweilige Funktion.
Untermenü 	Die Schaltfläche Neu ist in jedem Menü vorhanden, in dem eine Liste aller konfigurierten Einträgen angezeigt wird. Klicken Sie diese Schaltfläche, um das Konfigurationsmenü für das Anlegen eines neuen Listeneintrags aufzurufen.
Untermenü 	Klicken Sie auf diese Schaltfläche, um den bestehenden Listeneintrag zu bearbeiten. Sie gelangen in das Konfigurationsmenü.
Menü Erweiterte Einstellungen	Klicken Sie auf diesen Reiter, um erweiterte Konfigurationsoptionen anzuzeigen.

Für die Konfiguration stehen folgende Optionen zur Verfügung:

GUI Konfigurationselemente

Menü	Funktion
Eingabefelder	z. B. leeres Textfeld

Menü	Funktion
	 <p>Textfeld mit verdeckter Eingabe</p>  <p>Geben Sie entsprechende Daten ein.</p>
Radiobuttons	<p>z. B.</p>  <p>Wählen Sie die entsprechende Option aus.</p>
Checkboxes	<p>z. B. Aktivieren durch Auswahl der Checkbox</p>  <p>Auswahl verschiedener möglicher Optionen</p> 
Dropdown-Menüs	<p>z. B.</p>  <p>Klicken Sie auf den Pfeil, um die Liste zu öffnen. Wählen Sie die gewünschte Option mit der Maus.</p>
Interne Listen	<p>z. B.</p>  <p>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.</p>

Darstellung von Optionen, die nicht zur Verfügung stehen

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



Wichtig

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

Warnsymbole

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

Achten Sie besonders auf folgenden Hinweis:

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

7.3.1.3 GUI Menüs

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



Hinweis

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

Das **GUI** enthält folgende Menüs:

Assistenten

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

Menü	Funktion
	te, um Ihr Lokales Netzwerk (LAN) an das Internet anzuschließen.
VPN	In diesem Menü werden Sie durch alle Einstellungen geführt, die notwendig sind um Ihre LAN-LAN Verbindung als Virtual Private Network (VPN) einzurichten.
VoIP PBX im LAN	Der Assistent wird z. B. für bestimmte Telefonanlagen im LAN wie z. B. hybird benötigt, um die SIP-Kompatibilität zu gewährleisten. Dazu erfolgt die Kommunikation nach außen über eine einzige IP-Adresse, NAT wird als full-cone NAT realisiert.

Systemverwaltung

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

Physikalische Schnittstellen

Menü	Funktion
Ethernet-Ports	In diesem Menü konfigurieren Sie die Ethernet-Schnittstellen Ihres Geräts. Hier wählen Sie z. B. die Geschwindigkeit und die Art der Schnittstelle aus.
ISDN-Ports	In diesem Menü konfigurieren Sie die ISDN-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluss Ihr Gerät angeschlossen ist.
UMTS/LTE	In diesem Menü konfigurieren Sie die CardBus-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, dass UMTS aktiviert wird.

LAN

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

Wireless LAN Controller

Menü	Funktion
Wizard	Der Wizard hilft Ihnen beim Einrichten einer WLAN-Infrastruktur.
Controller-Konfiguration	In diesem Menü nehmen Sie grundlegende Wireless-LAN-Controller-Einstellungen vor.
Slave-AP-Konfiguration	In diesem Menü konfigurieren Sie die Slave Access Points.
Monitoring	In diesem Menü können Sie aktive und benachbarte Clients überwachen.
Wartung	In diesem Menü können Sie die Software Ihrer Access Points aktualisieren sowie Konfigurationen sichern.

Netzwerk

Menü	Funktion
Routen	In diesem Menü tragen Sie weitere Routen ein.

Menü	Funktion
IPv6-Präfixe	In diesem Menü konfigurieren Sie die IPv6-Präfixe.
NAT	In diesem Menü konfigurieren Sie die NAT-Firewall (NAT, Network Address Translation).
Lastverteilung	In diesem Menü konfigurieren Sie applikationsgesteuertes Bandbreitenmanagement.
QoS	In diesem Menü konfigurieren Sie alle Einstellungen zu "Quality of Service".
Zugriffsregeln	In diesem Menü werden Zugriffe auf Daten und Funktionen eingegrenzt.
Drop-In	In diesem Menü können Sie Schnittstellen logisch voneinander trennen ohne das gemeinsame Netz aufzugeben.

Routing-Protokolle

Menü	Funktion
RIP	In diesem Menü konfigurieren Sie die dynamische Aktualisierung der Routing-Tabelle mittels RIP.
OSPF	In diesem Menü werden alle globalen und Schnittstellen-spezifischen OSPF-Einstellungen vorgenommen.

Multicast

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

WAN

Menü	Funktion
Internet + Einwählen	In diesem Menü definieren Sie Internetverbindungen für die verschiedenen Verbindungsprotokolle oder Einwahlverbindungen ein.
IPv6-Tunnel	In diesem Menü definieren Sie Tunnelmechanismen, um IPv6-Datenpakete über ein IPv4-Netzwerk zu transportieren.
Standleitung	In diesem Menü werden die permanenten Verbindungen zweier Kommunikationspartner angezeigt.
Real Time Jitter Control	In diesem Menü können Sie die Upload Geschwindigkeit festlegen.

VPN

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

Firewall

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

VoIP

Menü	Funktion
SIP	In diesem Menü konfigurieren Sie einen Netzübergang zwischen unterschiedlichen Telekommunikationsnetzen.

Lokale Dienste

Menü	Funktion
DNS	In diesem Menü konfigurieren Sie die Namensauflösung.
HTTPS	In diesem Menü konfigurieren sie Port und Zertifikat für eine Konfigurationssitzung über HTTPS.
DynDNS-Client	In diesem Menü konfigurieren Sie die dynamische Namensauflösung.
DHCP-Server	In diesem Menü konfigurieren Sie Ihr Gerät als DHCP-Server.
CAPI-Server	In diesem Menü konfigurieren Sie Ihr Gerät als CAPI-Server.
Scheduling	In diesem Menü konfigurieren Sie zeitabhängige Standardaktionen Ihres Geräts.
Überwachung	In diesem Menü konfigurieren Sie die Überwachung von Schnittstellen oder von Hosts im Netzwerk.
ISDN-Diebstahlsicherung	In diesem Menü können Sie die Funktion ISDN-Diebstahlsicherung schnittstellenabhängig konfigurieren.
UPnP	In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.
Hotspot-Gateway	In diesem Menü konfigurieren Sie das bintec Hotspot-Gateway .
BRRP	In diesem Menü können Sie eine redundante Netzwerkumgebung konfigurieren.

Wartung

Menü	Funktion
Diagnose	In diesem Menü können Sie die Erreichbarkeit von Hosts, DNS

Menü	Funktion
	Servern oder Routen testen.
Software & Konfiguration	In diesem Menü verwalten Sie die Konfigurationsdateien Ihres Geräts. Sie speichern sie z. B. lokal auf Ihrem Gerät oder aber auf Ihrem Rechner ab. Sie können außerdem eine Aktualisierung der Systemsoftware initiieren.
Neustart	In diesem Menü können Sie den Neustart des Geräts initiieren.

Externe Berichterstellung

Menü	Funktion
Systemprotokoll	In diesem Menü konfigurieren Sie den Host, zu dem die intern auf dem Gerät protokollierten Daten zur Speicherung und Weiterverarbeitung weitergeleitet werden sollen.
IP-Accounting	In diesem Menü legen Sie fest, für welche Schnittstellen Accounting-Meldungen generiert werden sollen.
Benachrichtigungsdienst	In diesem Menü werden dem Administrator je nach Konfiguration Emails gesendet, sobald relevante Syslog Meldungen auftreten.
SNMP	In diesem Menü konfigurieren Sie, ob das Gerät auf externe SNMP-Zugriffe lauschen und SNMP Traps senden soll.

Monitoring

Menü	Funktion
Internes Protokoll	In diesem Menü werden die Systemmeldungen angezeigt.
IPSec	In diesem Menü werden die aktuell aktiven IPSec-Verbindungen und Verbindungsstatistiken angezeigt.
ISDN/Modem	In diesem Menü werden die ISDN-Verbindungen angezeigt.
Schnittstelle	In diesem Menü werden Verbindungsstatistiken und der Status aller Schnittstellen angezeigt.
Bridges	In diesem Menü können Sie die aktuellen Werte der konfigurier-

Menü	Funktion
	ten Bridges einsehen.
Hotspot-Gateway	In diesem Menü wird eine Liste aller bintec Hotspot Benutzer angezeigt.
QoS	In diesem Menü werden Statistiken für alle Schnittstellen angezeigt, für die QoS konfiguriert wurde.
OSPF	In diesem Menü wird der Status und Statistiken für alle Schnittstellen angezeigt, für die OSPF konfiguriert wurde.
PIM	In diesem Menü wird der Status alle Schnittstellen angezeigt, für die PIM konfiguriert wurde.

7.3.2 SNMP Shell

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

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

7.4 BOOTmonitor

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

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

- (1) Boot System (Neustart des Systems):
Das Gerät lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.
- (2) Software Update via TFTP (Softwareaktualisierung über TFTP):
Das Gerät führt ein Software-Update über einen TFTP-Server aus.
- (3) Software Update via XMODEM (Softwareaktualisierung über XMODEM):
Das Gerät führt ein Software-Update über eine serielle Schnittstelle mit XMODEM aus.
- (4) Delete configuration (Konfiguration löschen):
Das Gerät wird in den Auslieferungszustand zurückversetzt. Alle Konfigurationsda-

teien werden gelöscht, die BOOTmonitor-Einstellungen werden auf die Standardwerte gesetzt.

- (5) Default BOOTmonitor Parameters (Standardeinstellungen des BOOTmonitors):
Sie können die Standard-Einstellungen des BOOTmonitors des Geräts verändern, z. B. die Baudrate für serielle Verbindungen.
- (6) Show System Information (Systeminformationen anzeigen):
Zeigt nützliche Informationen des Geräts, wie z. B. Seriennummer, MAC-Adresse und Software-Versionen.

Der BOOTmonitor wird wie folgt gestartet.

Beim Hochfahren durchläuft das Gerät verschiedene Funktionszustände:

- Start-Modus
- BOOTmonitor-Modus
- Normaler Betriebsmodus

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

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

```
RXL1250 Bootmonitor V.7.9 Rev.1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by Teldat GmbH
```

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

```
Your Choice> _
```

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



Hinweis

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

Kapitel 8 Assistenten

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

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

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

Kapitel 9 Systemverwaltung

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

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

9.1 Status

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

Sie erhalten einen Überblick über folgende Daten:

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

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



Achtung

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

Automatisches Aktualisierungsintervall <input type="text" value="300"/> Sekunden <input type="button" value="Übernehmen"/>		
! Warnung: Systempasswort nicht geändert!		
Systeminformationen		
Uptime	10 Tage) 22 Stunde(n) 42 Minute(n)	
Systemdatum	Donnerstag, 13 Apr 2000, 05:21:41	
Seriennummer	SR6AAA009400008	
BOSS-Version	V.9.1 Rev. 2 IPSec from 2012/03/23 00:00:00	
Letzte gespeicherte Konfiguration	Samstag, 26 Feb 2000, 03:52:50	
Ressourceninformationen		
CPU-Nutzung	0%	
Arbeitsspeichernutzung	23.163.9 MByte (36%)	
ISDN Verwendung Extern	0 / 2 B-Kanäle	
Aktive Sitzungen (SIF, RTP, etc...)	3	
Aktive IPSec-Tunnel	0 / 2	
Physikalische Schnittstellen		
Schnittstelle	Verbindungsinformation	Link
en1-0	192.168.0.254 / 255.255.255.0	
en1-4	Nicht konfiguriert / Nicht konfiguriert	
WLAN1	Access-Point / Verwendeter Kanal - / 0 Clients / FW: 2.0.0.0	
bri-0	Nicht konfiguriert	
ADSL	0	kbit/s Downstream
	0	kbit/s Upstream
WAN-Schnittstellen		
Beschreibung	Verbindungsinformation	Link
PPPoE1		
Branch_Peer-1		
Branch_Peer-2		

Abb. 24: Systemverwaltung ->Status

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

Felder im Menü Systeminformationen

Feld	Wert
Uptime	Zeigt die Zeit an, die vergangen ist, seit das Gerät neu gestartet wurde.
Systemdatum	Zeigt das aktuelle Systemdatum und die Systemuhrzeit an.
Seriennummer	Zeigt die Geräte-Seriennummer an.
BOSS-Version	Zeigt die aktuell geladene Version der Systemsoftware an.
Back-up der Konfiguration auf SD Karte	Zeigt an, ob ein Back-up der Konfiguration auf der SD-Karte verfügbar ist oder nicht.
Letzte gespeicherte Konfiguration	Zeigt Tag, Datum und Uhrzeit der letzten Konfigurationsspeicherung (Boot-Konfiguration im Flash) an.

Felder im Menü Ressourceninformationen

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

Felder im Menü Physikalische Schnittstellen

Feld	Wert
Schnittstelle - Verbindungsinformation - Status	<p>Hier sind alle physikalischen Schnittstellen aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle angeschlossen bzw. aktiv ist.</p> <p>Schnittstellendetails für Ethernet-Schnittstellen:</p> <ul style="list-style-type: none"> • IPv4-Adresse / IPv6-Adresse • Netzmaske / Präfixlänge • Nicht konfiguriert <p>Schnittstellendetails für ISDN-Schnittstellen:</p> <ul style="list-style-type: none"> • Konfiguriert • Nicht konfiguriert <p>Schnittstellendetails für xDSL-Schnittstellen:</p> <ul style="list-style-type: none"> • Leitungsgeschwindigkeit Downstream/Upstream

Felder im Menü WAN-Schnittstellen

Feld	Wert
Beschreibung - Verbindungsinformation - Status	Hier sind alle WAN-Schnittstellen und IPv6-Tunnel aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle aktiv ist.

9.2 Globale Einstellungen

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

9.2.1 System

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

System		Passwörter	Datum und Uhrzeit	Timer	Systemlizenzen
Grundeinstellungen					
Systemname	hybird				
Standort					
Kontakt	TELDAT				
Maximale Anzahl der Syslog-Protokolleinträge	50				
Maximales Nachrichtenlevel von Systemprotokolleinträgen	Informationen <input type="button" value="v"/>				
Maximale Anzahl der Accounting-Protokolleinträge	20				
Systemeinstellungen					
Signalisierung der Übergabe	<input checked="" type="radio"/> Mit Freiton <input type="radio"/> Mit Wartemusik (Music On Hold, MoH)				
Übergabe auf besetzten Teilnehmer	<input type="checkbox"/> Aktiviert				
Abwurf auf Rufnummer	Kein Abwurf - Besetztton <input type="button" value="v"/>				
Externe Verbindungen zusammenschalten	<input type="checkbox"/> Aktiviert				
Ländereinstellungen					
Ländereinstellung	Deutschland <input type="button" value="v"/>				
Displaysprache	Deutsch <input type="button" value="v"/>				
Internationaler Präfix / Länderkennzahl	00 / <input type="text"/>				
Nationaler Präfix/Ortsnetzkenzahl	0 / <input type="text"/>				
Erweiterte Einstellungen					
Abrechnungseinstellungen					
Tarifeinheitenfaktor	0,00				
Währung					
Gebühreninformationen (SO/Upn-Erweiterung)	<input type="radio"/> Keypad <input type="radio"/> Funktional <input checked="" type="radio"/> Beide				
Tagmodus					
Globaler Abwurf	Variante1 <input type="button" value="v"/>				
Nachtbetrieb					
Team-Signalisierung	Variante1 <input type="button" value="v"/>				
TFE-Signalisierung	Variante1 <input type="button" value="v"/>				
Abwurf auf Ansage	Variante1 <input type="button" value="v"/>				
Individueller Teilnehmer Abwurf	Variante1 <input type="button" value="v"/>				
Globaler Abwurf	Variante1 <input type="button" value="v"/>				
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

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

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

Felder im Menü Basisparameter

Feld	Wert
Systemname	Geben Sie den Systemnamen Ihres Geräts ein. Dieser wird

Feld	Wert
	<p>auch als PPP-Host-Name benutzt.</p> <p>Möglich ist eine Zeichenkette mit maximal 255 Zeichen.</p> <p>Als Standardwert ist der Gerätetyp voreingestellt.</p>
Standort	<p>Geben Sie an, wo sich Ihr Gerät befindet.</p>
Kontakt	<p>Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden.</p> <p>Möglich ist eine Zeichenkette mit maximal 255 Zeichen.</p> <p>Standardwert ist <i>TEL DAT</i>.</p>
Maximale Anzahl der Syslog-Protokolleinträge	<p>Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000</i>.</p> <p>Standardwert ist <i>50</i>. Sie können die gespeicherten Meldungen in Monitoring->Internes Protokoll anzeigen lassen.</p>
Maximales Nachrichtenlevel von Systemprotokolleinträgen	<p>Wählen Sie die Priorität der Systemmeldungen aus, ab der protokolliert werden soll.</p> <p>Nur Systemmeldungen mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass bei der Priorität <i>Debug</i> sämtliche erzeugten Meldungen aufgezeichnet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i>: Es werden nur Meldungen mit der Priorität Notfall aufgezeichnet. • <i>Alarm</i>: Es werden Meldungen mit der Priorität Notfall und Alarm aufgezeichnet. • <i>Kritisch</i>: Es werden Meldungen mit der Priorität Notfall, Alarm und Kritisch aufgezeichnet. • <i>Fehler</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch und Fehler aufgezeichnet. • <i>Warnung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler und Warnung aufgezeichnet.

Feld	Wert
	<ul style="list-style-type: none"> • <i>Benachrichtigung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung und Benachrichtigung aufgezeichnet. • <i>Informationen</i> (Standardwert): Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung, Benachrichtigung und Informationen aufgezeichnet. • <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.
Maximale Anzahl der Accounting-Protokolleinträge	<p>Geben Sie die maximale Anzahl an Einträgen an, die für Login-Vorgänge auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind 0 bis 1000 .</p> <p>Standardwert ist 20 .</p>
Manuelle IP-Adresse des WLAN-Controller	<p>Geben Sie die IP-Adresse des WLAN-Controllers an.</p> <p>Der Wert kann nur verändert werden, wenn die WLAN-Controller-Funktion aktiviert ist.</p>

9.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

System **Passwörter** Datum und Uhrzeit Timer Systemlizenzen

Systempasswort	
Systemadministrator-Passwort	••••••
Systemadministrator-Passwort bestätigen	••••••
Konfiguration per Telefon (vierstellige PIN, numerisch)	
PIN1	••••
Fernzugang Telefonie (sechsstellige PIN)	
Fernzugang (z. B. Follow me, Raumüberwachung)	<input type="checkbox"/> Aktiviert
SNMP-Communities	
SNMP Read Community	••••••
SNMP Write Community	••••••
Globale Passwortoptionen	
Passwörter und Schlüssel als Klartext anzeigen	Anzeigen

OK Abbrechen

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



Hinweis

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

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

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

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

Felder im Menü Systempasswort

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

Felder im Menü SNMP-Communities

Feld	Wert
SNMP Read Community	Geben Sie das Passwort für den Benutzernamen <code>read</code> ein.
SNMP Write Community	Geben Sie das Passwort für den Benutzernamen <code>write</code> 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 <i>Anzeigen</i> wird die Funktion aktiviert. Standardmäßig ist die Funktion nicht aktiv. Wenn Sie die Funktion aktivieren, werden alle Passwörter und

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

9.2.3 Datum und Uhrzeit

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

System Passwörter **Datum und Uhrzeit** Timer Systemlizenzen

Grundeinstellungen							
Zeitzone	Europe/Berlin ▼						
Aktuelle Ortszeit	Montag, 12 Nov 2012, 13:46:00						
Manuelle Zeiteinstellung							
Datum einstellen	<table style="width: 100%; border: none;"> <tr> <td style="width: 33%; border: none;">Tag</td> <td style="width: 33%; border: none;">Monat</td> <td style="width: 33%; border: none;">Jahr</td> </tr> <tr> <td style="border: 1px solid #ccc;"> </td> <td style="border: 1px solid #ccc;"> </td> <td style="border: 1px solid #ccc;"> </td> </tr> </table>	Tag	Monat	Jahr			
Tag	Monat	Jahr					
Zeit einstellen	<table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;">Stunde</td> <td style="width: 50%; border: none;">Minute</td> </tr> <tr> <td style="border: 1px solid #ccc;"> </td> <td style="border: 1px solid #ccc;"> </td> </tr> </table>	Stunde	Minute				
Stunde	Minute						
Automatische Zeiteinstellung (Zeitprotokoll)							
ISDN-Zeitserver	<input type="checkbox"/> Aktiviert						
Erster Zeitserver	SNTP ▼						
Zweiter Zeitserver	SNTP ▼						
Dritter Zeitserver	SNTP ▼						
Zeitaktualisierungsintervall	1440 Minute(n)						
Zeitaktualisierungsrichtlinie	Normal ▼						
System als Zeitserver	<input type="checkbox"/> Aktiviert						
OK Abbrechen							

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

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

ISDN/Manuell

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

Wenn für die **Zeitzone** der korrekt Standort des Geräts (Land/Stadt) eingestellt ist, erfolgt die Umschaltung der Uhrzeit von Sommer- auf Winterzeit (und zurück) automatisch. Die Umschaltung erfolgt unabhängig von der Zeit der Vermittlungsstelle oder von einem ntp-Server. Die Sommerzeit beginnt am letzten Sonntag im März durch die Umschaltung von 2 Uhr auf 3 Uhr. Die in der fehlenden Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt. Die Winterzeit beginnt am letzten Sonntag im Oktober durch die Umschaltung von 3 Uhr auf 2 Uhr. Die in der zusätzlichen Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt.

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

Zeitserver

Sie können die Systemzeit auch automatisch über verschiedene Zeitserver beziehen. Um sicherzustellen, dass das Gerät die gewünschte aktuelle Zeit verwendet, sollten Sie einen oder mehrere Zeitserver konfigurieren. Die Umschaltung der auf diese Weise bezogenen Uhrzeit von Sommer- auf Winterzeit (und zurück) muss manuell durchgeführt werden, indem der Wert im Feld **Zeitzone** mit einer Option UTC+ oder UTC- entsprechend angepasst wird.



Hinweis

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

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

Felder im Menü 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. <i>Europe/Berlin</i> .
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	<p>Geben Sie ein neues Datum ein.</p> <p>Format:</p> <ul style="list-style-type: none"> • Tag: dd • Monat: mm • Jahr: yyyy
Zeit einstellen	<p>Geben Sie eine neue Uhrzeit ein.</p> <p>Format:</p> <ul style="list-style-type: none"> • Stunde: hh • Minute: mm

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	<p>Legen Sie fest, ob die Systemzeit über ISDN aktualisiert werden soll.</p> <p>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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erster Zeitserver	<p>Geben Sie den ersten Zeitserver an, entweder mit Domännennamen oder IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst

Feld	Beschreibung
	<p>über UDP-Port 37.</p> <ul style="list-style-type: none"> • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage verwendet.
Zweiter Zeitserver	<p>Geben Sie den zweiten Zeitserver an, entweder mit Domänennamen oder mit IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitervers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Dritter Zeitserver	<p>Geben Sie den dritten Zeitserver an, entweder mit Domänennamen oder mit IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitervers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Deaktiviert</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	<p>Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird.</p>

Feld	Beschreibung
	Der Standardwert ist <i>1440</i> .
Zeitaktualisierungsrichtlinie	<p>Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Normal</i> (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen. • <i>Aggressiv</i>: Zehn Minuten lang wird versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • <i>Endlos</i>: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver zuerst nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. <p>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 <i>Endlos</i>.</p>
System als Zeitserver	<p>Wählen Sie aus, ob der interne Zeitserver verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Zeitanfragen eines Clients werden mit der aktuellen Systemzeit beantwortet. Diese wird als GMT ohne Offset angegeben.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Zeitanfragen eines Clients werden nicht beantwortet.</p>

9.2.4 Systemlizenzen

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

Es sind generell folgende Lizenztypen zu unterscheiden:

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

- kostenpflichtige Zusatzlizenzen

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

Lizenzdaten eintragen

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

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

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

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

Mögliche Werte für Status

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

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



Hinweis

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

9.2.4.1 Bearbeiten oder Neu

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

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

Freischalten von Zusatzlizenzen

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

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

Felder im Menü Grundeinstellungen

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



Hinweis

Wenn als Status *Nicht OK* angezeigt wird:

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

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

Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

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

- (2) Betätigen Sie das -Symbol in der Zeile, in der die zu löschende Lizenz steht.
- (3) Bestätigen Sie mit **OK**.

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

9.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

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

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

Konventionen für die Port-/Schnittstellennamen

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 Ethernet
- (b) Nummer der Bridge-Gruppe

Beispiel: *br0* (erste Bridge-Gruppe)

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)

9.3.1 Schnittstellen

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

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

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

Schnittstellen

#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe		
1	en1-0	Routing-Modus		
2	en1-4	Routing-Modus		

Konfigurationsschnittstelle Eine auswählen ▾

Hinzufügen
OK
Abbrechen

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

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

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschreibung	Zeigt den Namen der Schnittstelle an.

Feld	Beschreibung
Modus / Bridge-Gruppe	Wählen Sie aus, ob Sie die Schnittstelle im <i>Routing-Modus</i> betreiben möchten oder ordnen die Schnittstelle einer bestehenden (<i>br0, br1</i> usw.) oder neuen Bridge-Gruppe (<i>Neue Bridge-Gruppe</i>) zu. Bei Auswahl von <i>Neue Bridge-Gruppe</i> wird nach Anklicken des OK -Buttons automatisch eine neue Bridge-Gruppe erzeugt.
Konfigurationsschnittstelle	<p>Wählen Sie aus, über welche Schnittstelle die Konfiguration durchgeführt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Eine auswählen</i> (Standardwert): Einstellung im Auslieferungszustand. Die richtige Konfigurationsschnittstelle muss aus den anderen Optionen ausgewählt werden. • <i>Nicht beachten</i>: Keine Schnittstelle wird als Konfigurationsschnittstelle definiert. • <i><Schnittstellename></i>: Legen Sie die Schnittstelle fest, die zur Konfiguration benutzt wird. Wenn diese Schnittstelle Mitglied einer Bridge-Gruppe ist, übernimmt sie deren IP-Adresse, wenn sie aus der Bridge-Gruppe herausgenommen wird.

9.3.1.1 Hinzufügen

Wählen Sie die Schaltfläche **Neu**, um den Modus von weiteren Schnittstellen zu bearbeiten.

Schnittstellen

Schnittstelle
Eine auswählen ▾

OK
Abbrechen

Abb. 30: **Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen->Hinzufügen**

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

Felder im Menü Hinzufügen

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

9.4 Administrativer Zugriff

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

9.4.1 Zugriff

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

Zugriff SSH SNMP

! Der administrative Zugang ist zur Zeit nicht eingeschränkt. Die angezeigte Konfiguration wurde noch nicht aktiviert.

Schnittstelle	Telnet	SSH	HTTP	HTTPS	Ping	SNMP	ISDN-Login
en1-0	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
en1-4	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
mpsisdn	<input type="checkbox"/>	<input checked="" type="checkbox"/>					

Service Login (ISDN Web-Access) **Aktiviert**

Service Call Ticket (SSH Web-Access) **Aktiviert**

Hinzufügen OK Abbrechen

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

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

Weiterhin können Sie Ihr Gerät für Wartungsarbeiten durch den Teldat-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 Teldat-Kundenservice!

9.4.1.1 Hinzufügen

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

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

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

Felder im Menü Zugriff

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

9.4.2 SSH

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

Zugriff SSH SNMP

SSH-Parameter (Secure Shell)	
SSH-Dienst aktiv	<input checked="" type="checkbox"/> Aktiviert
Komprimierung	<input type="checkbox"/> Aktiviert
TCP-Keepalives	<input checked="" type="checkbox"/> Aktiviert
Protokollierungslevel	Informationen ▾
Authentifizierungs- und Verschlüsselungsparameter	
Verschlüsselungsalgorithmen	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256
Hashing-Algorithmen	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD 160
Schlüsselstatus	
RSA-Schlüsselstatus	Generiert
DSA-Schlüsselstatus	Generiert

OK Abbrechen

Abb. 33: **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.teldat.de.

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 <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Feld	Wert
Komprimierung	<p>Wählen Sie aus, ob Datenkompression verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-Keepalives	<p>Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierungslevel	<p>Wählen Sie den Syslog-Level für die vom SSH-Daemon generierten Syslog-Messages aus.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Informationen</i> (Standardwert): Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet. • <i>Fatal</i>: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet. • <i>Fehler</i>: Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet. • <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.

Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

Feld	Wert
Verschlüsselungsalgorithmen	<p>Wählen Sie die Algorithmen, die für die Verschlüsselung der SSH-Verbindung verwendet werden sollen.</p> <p>Mögliche Optionen:</p> <ul style="list-style-type: none"> • <i>3DES</i> • <i>Blowfish</i> • <i>AES-128</i> • <i>AES-256</i> <p>Standardmäßig sind <i>3DES</i>, <i>Blowfish</i> und <i>AES-128</i> aktiv.</p>
Hashing-Algorithmen	<p>Wählen Sie die Algorithmen, die zur Message-Authentisierung der SSH-Verbindung verwendet werden sollen.</p>

Feld	Wert
	<p>Mögliche Optionen:</p> <ul style="list-style-type: none"> • <i>MD5</i> • <i>SHA-1</i> • <i>RipeMD 160</i> <p>Standardmäßig sind <i>MD5</i>, <i>SHA-1</i> und <i>RipeMD 160</i> aktiv.</p>

Felder im Menü Schlüsselstatus

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

Feld	Wert
	platz im FlashROM.

9.4.3 SNMP

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

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

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

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

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

Zugriff SSH SNMP

Grundeinstellungen	
SNMP-Version	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> v3
SNMP-Listen-UDP-Port	161

OK Abbrechen

Abb. 34: 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:

Feld	Wert
	<ul style="list-style-type: none"> • <i>v1</i>: SNMP-Version 1 • <i>v2c</i>: Community-Based SNMP-Version 2 • <i>v3</i>: SNMP-Version 3 <p>Standardmäßig sind <i>v1</i>, <i>v2c</i> und <i>v3</i> aktiv.</p> <p>Ist keine Option ausgewählt, ist die Funktion nicht aktiv.</p>
SNMP-Listen-UDP-Port	<p>Zeigt den UDP-Port (<i>161</i>) an, an dem das Gerät SNMP-Requests annimmt.</p> <p>Der Wert kann nicht verändert werden.</p>



Tipp

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

9.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

9.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS-Pakete

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

Pakettypen

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

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

9.5.1.1 Bearbeiten oder Neu

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

RADIUS TACACS+ Optionen

Basisparameter	
Authentifizierungstyp	PPP-Authentifizierung ▼
Server-IP-Adresse	<input type="text"/>
RADIUS-Passwort	<input type="password"/>
Standard-Benutzerpasswort	<input type="password"/>
Priorität	0 ▼
Eintrag aktiv	<input checked="" type="checkbox"/> Aktiviert
Gruppenbeschreibung	Default Group 0 ▼
Erweiterte Einstellungen	
Richtlinie	Verbindlich ▼
UDP-Port	<input type="text" value="1812"/>
Server Timeout	<input type="text" value="1000"/> Millisekunden
Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
Wiederholungen	<input type="text" value="1"/>
RADIUS-Dialout:	<input type="checkbox"/> Aktiviert Neulade-Intervall <input type="text" value="0"/> Sekunden
OK Abbrechen	

Abb. 35: **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:

Feld	Wert
	<ul style="list-style-type: none"> • <i>PPP-Authentifizierung</i> (Standardwert): Der RADIUS-Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. • <i>Accounting</i>: Der RADIUS-Server wird zur Erfassung statistischer Verbindungsdaten verwendet. • <i>Login-Authentifizierung</i>: Der RADIUS-Server wird verwendet, um den Zugang zur SNMP Shell Ihres Geräts zu kontrollieren. • <i>IPSec-Authentifizierung</i>: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln. • <i>XAUTH</i>: Der RADIUS-Server wird verwendet, um IPSec-Peers über XAuth zu authentisieren.
Betreibermodus	<p>Nur für Authentifizierungstyp = <i>Accounting</i>.</p> <p>Wählen Sie in Hotspot-Anwendungen den Modus aus, der vom Anbieter definiert ist.</p> <p>In Standardanwendungen belassen Sie den Wert bei <i>Standard</i>.</p> <p>Mögliche Werte für Hotspot-Anwendungen:</p> <ul style="list-style-type: none"> • <i>France Telecom</i>: Für Hotspot-Anwendungen der France Telecom. • <i>bintec HotSpot Server</i>: Für bintec Hotspot-Anwendungen.
Server-IP-Adresse	Geben Sie die IP-Adresse des RADIUS-Servers ein.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein.
Standard-Benutzerpasswort	Einige RADIUS-Server benötigen für jede RADIUS-Anfrage ein Benutzerpasswort. Geben Sie daher das Passwort hier ein, das Ihr Gerät als Standard-Benutzerpasswort in der Anfrage für die Dialout-Routen an den RADIUS-Server mitsendet.
Priorität	Wenn mehrere RADIUS-Server-Einträge angelegt wurden, wird der Server mit der obersten Priorität als erstes verwendet. Wenn dieser Server nicht antwortet, wird der Server mit der nächstniedrigeren Priorität verwendet usw.

Feld	Wert
	<p>Mögliche Werte von 0 (höchste Priorität) bis 7 (niedrigste Priorität).</p> <p>Standardwert ist 0 .</p> <p>Siehe auch Richtlinie in den erweiterten Einstellungen.</p>
Eintrag aktiv	<p>Wählen Sie aus, ob der in diesem Eintrag konfigurierte RADIUS-Server verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Gruppenbeschreibung	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neu</i> (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein. • <i>Default Group 0</i>: Wählen Sie diesen Eintrag für spezielle Anwendungen, wie z. B. Hotspot-Server-Konfiguration, aus. • <i><Gruppenname></i>: 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	<p>Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Verbindlich</i> (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. • <i>Nicht verbindlich</i>: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS-Server wird angefragt, bis Ihr Gerät eine Antwort von einem als autoritativ konfigurierten Server erhält.

Feld	Wert
UDP-Port	<p>Geben Sie den zu verwendenden UDP-Port für RADIUS-Daten ein.</p> <p>Gemäß RFC 2138 sind die Standard-Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Gebührenerfassung (1646 in älteren RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist.</p> <p>Standardwert ist <i>1812</i>.</p>
Server Timeout	<p>Geben Sie die maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden ein.</p> <p>Nach Ablauf dieser Zeit wird die Anfrage gemäß Wiederholungen wiederholt bzw. der nächste konfigurierte RADIUS-Server angefragt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>50</i> und <i>50000</i>.</p> <p>Standardwert ist <i>1000</i> (1 Sekunde).</p>
Erreichbarkeitsprüfung	<p>Wählen Sie eine Überprüfung der Erreichbarkeit eines RADIUS-Servers im Status <i>Inaktiv</i>.</p> <p>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 Status wieder auf <i>aktiv</i> gesetzt. Wenn der RADIUS-Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit <i>inaktiv</i> ist.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Wiederholungen	<p>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 <i>inaktiv</i> gesetzt. bei Erreichbarkeitsprüfung = <i>Aktiviert</i> versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird Status wieder auf <i>aktiv</i> zurückgesetzt.</p>

Feld	Wert
	<p>Mögliche Werte sind ganze Zahlen zwischen 0 und 10 .</p> <p>Standardwert ist 1 . Um zu verhindern, dass Status auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf 0 .</p>
RADIUS-Dialout	<p>Nur für Authentifizierungstyp = <i>PPP-Authentifizierung</i> und <i>IPSec-Authentifizierung</i>.</p> <p>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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiv ist, können Sie folgende Option eingeben:</p> <ul style="list-style-type: none"> • <i>Neulade-Intervall</i>: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. <p>Standardmäßig ist hier 0 eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>

9.5.2 TACACS+

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

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

Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:

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

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

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

9.5.2.1 Bearbeiten oder Neu

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

RADIUS TACACS+ Optionen

Basisparameter	
Authentifizierungstyp	Login-Authentifizierung
Server-IP-Adresse	
TACACS+-Passwort	••••••••
Priorität	0
Eintrag aktiv	<input checked="" type="checkbox"/> Aktiviert

Erweiterte Einstellungen	
Richtlinie	Nicht verbindlich
TCP-Port	49
Timeout	3 Sekunden
Blockzeit	60 Sekunden
Verschlüsselung	<input checked="" type="checkbox"/> Aktiviert

OK Abbrechen

Abb. 36: 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: <ul style="list-style-type: none"> <i>Login-Authentifizierung</i>: Hier können Sie festlegen, ob der aktuelle TACACS+-Server für die Login-Authentifizierung zu Ihrem Gerät benutzt werden soll.
Server-IP-Adresse	Geben Sie die IP-Adresse des TACACS+-Servers ein, der für eine Login-Authentifizierung abgefragt werden soll.
TACACS+-Passwort	Geben Sie das Passwort ein, welches benutzt werden soll, um den Datenaustausch zwischen dem TACACS+-Server und dem

Feld	Beschreibung
	Netzzugangsserver (Ihrem Gerät) zu authentifizieren und (falls zutreffend) zu verschlüsseln. Die maximale Länge des Eintrags ist 32 Zeichen.
Priorität	<p>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 = <i>Nicht verbindlich</i>), wird der Eintrag mit der nächstniedrigeren Priorität genutzt.</p> <p>Verfügbare Werte sind 0 bis 9, der Standardwert ist 0.</p>
Eintrag aktiv	<p>Wählen Sie aus, ob dieser Server für die Login-Authentifizierung verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Richtlinie	<p>Wählen Sie die Interpretation der TACACS+-Antwort aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht verbindlich</i> (Standardwert): Die TACACS+-Server werden gemäß ihrer Priorität (siehe Priorität) abgefragt, bis eine positive Antwort oder von einem autoritativen Server eine negative Antwort empfangen wurde. • <i>Verbindlich</i>: Eine negative Antwort auf eine Anfrage wird akzeptiert, d. h. es wird kein weiterer TACACS+-Server abgefragt. <p>Die Geräte-interne Benutzerverwaltung wird durch TACACS+ nicht ausgeschaltet. Sie wird geprüft, nachdem alle TACACS+-Server abgefragt wurden.</p>
TCP-Port	Zeigt den für das TACACS+-Protokoll verwendeten Standard-TCP-Port (49) an. Der Wert kann nicht verändert werden.
Timeout	Geben Sie die Zeit in Sekunden ein, die der NAS auf eine Ant-

Feld	Beschreibung
	<p>wort von TACACS+ warten soll.</p> <p>Falls während der Wartezeit keine Antwort empfangen wird, wird der nächste konfigurierte TACACS+-Server abgefragt (nur für Richtlinie = <i>Nicht verbindlich</i>) und der aktuelle Server in einen <i>blockiert</i>-Status versetzt.</p> <p>Mögliche Werte sind 1 bis 60, der Standardwert ist 3.</p>
Blockzeit	<p>Geben Sie die Zeit in Sekunden ein, die der aktuelle Server in einem blockierten Status verbleiben soll.</p> <p>Nach Ende der Blockierung wird der Server in den Status versetzt, der im Feld Eintrag aktiv angegeben ist.</p> <p>Mögliche Werte sind 0 bis 3600, der Standardwert ist 60. Der Wert 0 bedeutet, dass der Server nie in einen <i>blockiert</i>-Status versetzt wird und somit keine weiteren Server angefragt werden.</p>
Verschlüsselung	<p>Wählen Sie aus, ob der Datenaustausch zwischen dem TACACS+-Server und dem NAS mit MD5 verschlüsselt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>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.</p>

9.5.3 Optionen

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

Abb. 37: 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	<p>Standardmäßig wird folgende Reihenfolge bei der Authentisierung für eingehende Verbindungen unter Berücksichtigung von RADIUS angewendet: zunächst CLID, danach PPP und daraufhin PPP mit RADIUS.</p> <p>Optionen:</p> <ul style="list-style-type: none"> • <i>Inband</i> : 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. • <i>Outband (CLID)</i> : Nur Outband-RADIUS-Anfragen (d. h. Anfragen zur Rufnummernidentifizierung) werden zum RADIUS-Server geschickt (CLID = Calling Line Identification). <p>Standardmäßig ist <i>Inband</i> aktiviert.</p>

9.6 Zertifikate

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

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

ist, wird ein Nachweis, ein sogenanntes digitales Zertifikat benötigt.

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

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

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

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

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

9.6.1 Zertifikatsliste

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

9.6.1.1 Bearbeiten

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

Zertifikatsliste CRLs Zertifikatsserver

Parameter bearbeiten	
Beschreibung	<input type="text" value="xp.pfx"/>
Zertifikat ist ein CA-Zertifikat	<input checked="" type="checkbox"/> Wahr
Überprüfung anhand einer Zertifikatsperrliste (CRL)	<input type="radio"/> Deaktiviert
	<input type="radio"/> Immer
	<input checked="" type="radio"/> Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist
	<input type="radio"/> Einstellungen des übergeordneten Zertifikates benutzen
Vertrauenswürdigkeit des Zertifikats erzwingen	<input checked="" type="checkbox"/> Wahr
Details anzeigen	
<pre> Certificate = SerialNumber = 11 SubjectName = &lt;CN=r1200_aw, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE&gt; IssuerName = &lt;CN=linuxCA, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE&gt; Validity = NotBefore = 2006 Sep 15th, 07:07:49 GMT NotAfter = 2008 Sep 14th, 07:07:49 GMT PublicKeyInfo = Algorithm name (X.509) : rsaEncryption Modulus n (1024 bits) : 1657430007353061929971175628985365836058592284552111716307381855989730994 4241959750497426343375890536490502929548450998243448632595011570952551767 7011616656908963216398179133323977323187771274664312501085550617414306630 0411834850766905090689578661769721208181141085359073369329733126120426693 320106097890434357773 Exponent e (17 bits) : 65537 Extensions = Available = key usage, basic constraints KeyUsage = DigitalSignature NonRepudiation KeyEncipherment BasicConstraints = cA = FALSE </pre>	
MD5-Fingerabdruck	F0:41:44:3F:6A:62:DD:12:97:2C:67:21:F7:59:80:3E
SHA1-Fingerabdruck	98:5B:D6:3E:4A:9B:95:8B:FE:FF:C2:27:CF:24:42:A7:17:6F:8C:54
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

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

Felder im Menü

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.
Zertifikat ist ein CA-Zertifikat	Markieren Sie das Zertifikat als Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA).

Feld	Beschreibung
	<p>Zertifikate, die von dieser CA ausgestellt wurden, werden bei der Authentifizierung akzeptiert.</p> <p>Mit <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>Überprüfung anhand einer Zertifikatsperrliste (CRL)</p>	<p>Nur für Zertifikat ist ein CA-Zertifikat = Wahr</p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i>: keine Überprüfung von CRLs. • <i>Immer</i>: CRLs werden grundsätzlich überprüft. • <i>Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist (Standardwert)</i>: Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden. • <i>Einstellungen des übergeordneten Zertifikates benutzen</i>: 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.
<p>Vertrauenswürdigkeit des Zertifikats erzwingen</p>	<p>Legen Sie fest, dass dieses Zertifikat ohne weitere Überprüfung bei der Authentifizierung als Benutzerzertifikat akzeptiert werden soll.</p> <p>Mit <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>



Achtung

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

9.6.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

Zertifikatsliste CRLs Zertifikatsserver

Zertifikatsanforderung	
Zertifikatsanforderungsbeschreibung	<input type="text"/>
Modus	<input checked="" type="radio"/> Manuell <input type="radio"/> SCEP
Privaten Schlüssel generieren	RSA <input type="text"/> 1024 <input type="text"/> Bits
Subjektname	
Benutzerdefiniert	<input type="checkbox"/> Aktiviert
Allgemeiner Name	<input type="text"/>
E-Mail	<input type="text"/>
Organisationseinheit	<input type="text"/>
Organisation	<input type="text"/>
Ort	<input type="text"/>
Staat/Provinz	<input type="text"/>
Land	<input type="text"/>
Erweiterte Einstellungen	
Subjekt-Alternativnamen	
#1	Keiner <input type="text"/>
#2	Keiner <input type="text"/>
#3	Keiner <input type="text"/>
Optionen	
Autospeichermodus	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 39: 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	<p>Wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Manuell</i> (Standardwert): Ihr Gerät erzeugt für den Schlüssel eine PKCS#10-Datei, die direkt im Browser hochgeladen oder

Feld	Beschreibung
	<p>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.</p> <ul style="list-style-type: none"> • <i>SCEP</i>: Der Schlüssel wird mittels des Simple Certificate Enrollment Protocols bei einer CA beantragt.
Privaten Schlüssel generieren	<p>Nur für Modus = <i>Manuell</i></p> <p>Wählen Sie einen Algorithmus für die Schlüsselerstellung aus.</p> <p>Zur Verfügung stehen <i>RSA</i> (Standardwert) und <i>DSA</i>.</p> <p>Wählen Sie weiterhin die Länge des zu erzeugenden Schlüssels aus.</p> <p>Mögliche Werte: <i>512, 768, 1024, 1536, 2048, 4096</i>.</p> <p>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.</p>
SCEP-URL	<p>Nur für Modus = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B. <code>http://scep.teldat.de:8080/scep/scep.dll</code></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
CA-Zertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Wählen Sie das CA-Zertifikat aus.</p> <ul style="list-style-type: none"> • <i>-- Download --</i>: Geben Sie in CA-Name den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator. <p>Falls keine CA-Zertifikate zur Verfügung stehen, wird Ihr Gerät zuerst das CA-Zertifikat der betroffenen CA herunterladen.</p>

Feld	Beschreibung
	<p>Es fährt dann mit dem Registrierungsprozess fort, sofern keine wesentlichen Parameter mehr fehlen. In diesem Fall kehrt es in das Menü Zertifikatsanforderung generieren zurück.</p> <p>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.</p> <ul style="list-style-type: none"> • <Name eines vorhandenen Zertifikats>: Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, wählen Sie diese manuell aus.
RA-Signierungszertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Nur für CA-Zertifikat nicht = <i>-- Download --</i></p> <p>Wählen Sie ein Zertifikat für die Signierung der SCEP Kommunikation aus.</p> <p>Standardwert ist <i>-- CA-Zertifikat verwenden --</i>, d. h. es wird das CA-Zertifikat verwendet.</p>
RA-Verschlüsselungszertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Nur wenn RA-Signierungszertifikat nicht = <i>-- CA-Zertifikat verwenden --</i></p> <p>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.</p> <p>Standardwert ist <i>-- RA-Signierungszertifikat verwenden --</i>, d. h. es wird dasselbe Zertifikat wie zur Signierung verwendet.</p>
Passwort	<p>Nur für Modus = <i>SCEP</i></p> <p>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.</p>

Felder im Menü Subjektname

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

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: <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird kein zusätzlicher Name eingegeben. • <i>IP</i>: Es wird eine IP-Adresse eingetragen. • <i>DNS</i>: Es wird ein DNS-Name eingetragen. • <i>E-Mail</i>: Es wird eine E-Mail-Adresse eingetragen. • <i>URI</i>: Es wird ein Uniform Resource Identifier eingetragen. • <i>DN</i>: Es wird ein Distinguished Name (DN) eingetragen. • <i>RID</i>: 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 <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

9.6.1.3 Importieren

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

The screenshot shows a dialog box titled 'Importieren' with the following fields and controls:

- Externer Dateiname:** A text input field with a 'Durchsuchen...' button to its right.
- Lokale Zertifikatsbeschreibung:** A text input field.
- Dateikodierung:** A dropdown menu currently showing 'Auto'.
- Passwort:** A text input field.
- Buttons:** 'OK' and 'Abbrechen' buttons at the bottom.

Abb. 40: 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, sodass Ihr Gerät das Zertifikat dekodieren kann. Mögliche Werte: <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Aktiviert die automatische Kodierererkennung. Falls der Zertifikat-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung. • <i>Base64</i> • <i>Binär</i>
Passwort	Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort.

Feld	Beschreibung
	Tragen Sie das Passwort hier ein.

9.6.2 CRLs

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

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

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

9.6.2.1 Importieren

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

Zertifikatsliste CRLs Zertifikatsserver

CRL-Import

Externer Dateiname	<input type="text"/>	<input type="button" value="Durchsuchen..."/>
Lokale Zertifikatsbeschreibung	<input type="text"/>	
Dateikodierung	Auto <input type="button" value="v"/>	
Passwort	<input type="text"/>	

Abb. 41: **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: <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Aktiviert die automatische Kodierererkennung. Falls der CRL-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung. • <i>Base64</i> • <i>Binär</i>
Passwort	Geben Sie das zum Importieren zu verwendende Passwort ein.

9.6.3 Zertifikatsserver

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

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

9.6.3.1 Neu

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

The screenshot shows a configuration window for 'Zertifikatsserver'. At the top, there are three tabs: 'Zertifikatsliste', 'CRLs', and 'Zertifikatsserver'. The 'Zertifikatsserver' tab is selected. Below the tabs is a section titled 'Basisparameter' containing three input fields: 'Beschreibung' (empty), 'LDAP-URL-Pfad' (containing 'ldap://'), and 'OK' and 'Abbrechen' buttons at the bottom.

Abb. 42: **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 10 Physikalische Schnittstellen

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

10.1 Ethernet-Ports

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

Die Ethernet-Ports **ETH1** bis **ETH8** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle *en1-0* ist zugewiesen und mit **IP-Adresse** *192.168.0.254* und **Netzmaske** *255.255.255.0* vorkonfiguriert.

Die Ports **ETH9** und **ETH10** (mit Anschlussmöglichkeit zweier SFP-Moduls) sind der logischen Ethernet-Schnittstelle *en1-4* zugewiesen und nicht vorkonfiguriert.



Hinweis

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

ETH1 - ETH8

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.

ETH9 und ETH10 (mit Anschlussmöglichkeit zweier SFP-Moduls)

Standardmäßig ist den Ports **ETH9 und ETH10** die logische Ethernet-Schnittstelle *en1-4* zugewiesen. Die Konfigurationsoptionen sind identisch mit denen der Ports **ETH1 - ETH8**.



Hinweis

Wenn Sie den **ETH**-Port mit einem SFP-Modul betreiben wollen, muss dieses vor dem Systemstart gesteckt sein!

Im laufenden Betrieb ist in diesem Fall kein Wechsel auf den Betrieb des **ETH**-Port ohne SFP-Modul möglich. Soll der **ETH**-Port nach Einsatz eines SFP-Moduls verwendet werden, muss das Gerät neu gestartet werden.

Die wechselnde Nutzung des **ETH**-Ports im laufenden Betrieb ohne vorherigen Einsatz mit SFP-Modul ist jedoch möglich.

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

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

VLANs für Routing-Schnittstellen

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

10.1.1 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 Ge-

samtbandbreite 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.

Portkonfiguration

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

Switch-Konfiguration

Switch-Port	Ethernet-Schnittstellenauswahl	Konfigurierte Geschwindigkeit/konfigurierter Modus	Aktuelle Geschwindigkeit / Aktueller Modus	Flusskontrolle
1	en1-0	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert
2	en1-0	Vollständige automatische Aushandlung	100 Mbit/s / Full Duplex	Deaktiviert
3	en1-0	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert
4	en1-0	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert
5	en1-4	Vollständige automatische Aushandlung	Inaktiv	Deaktiviert

OK Abbrechen

Abb. 43: 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 die Schnittstellen <i>en1-0</i> bis <i>en1-9</i> . In der Grundeinstellung ist Switch Port 1-4 die Schnittstelle <i>en1-0</i> , Switch Port 5-10 die Schnittstelle <i>en1-5</i> zugeordnet.
Konfigurierte Geschwindigkeit/konfigurierter Modus	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll. Mögliche Werte: • <i>Vollständige automatische Aushandlung</i> (Standardwert)

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Auto 1000 Mbit/s only</i> • <i>Auto 100 Mbit/s only</i> • <i>Auto 10 Mbit/s only</i> • <i>Auto 100 Mbit/s / Full Duplex</i> • <i>Auto 100 Mbit/s / Half Duplex</i> • <i>Auto 10 Mbit/s / Full Duplex</i> • <i>Auto 10 Mbit/s / Half Duplex</i> • <i>Fest 1000 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Half Duplex</i> • <i>Fest 10 Mbit/s / Full Duplex</i> • <i>Fest 10 Mbit/s / Half Duplex</i> • <i>Keiner</i> : Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	<p>Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>1000 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Half Duplex</i> • <i>10 Mbit/s / Full Duplex</i> • <i>10 Mbit/s / Half Duplex</i> • <i>Inaktiv</i>
Flusskontrolle	<p>Wählen Sie aus, ob auf der entsprechenden Schnittstelle eine Flusskontrolle vorgenommen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i> (Standardwert): Es wird keine Flusskontrolle vorgenommen. • <i>Aktiviert</i>: Es wird eine Flusskontrolle durchgeführt. • <i>Auto</i>: Es wird eine automatische Flusskontrolle durchgeführt.

10.2 ISDN-Ports

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

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

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

10.2.1 ISDN-Konfiguration



Hinweis

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

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

10.2.1.1 Bearbeiten mit

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

ISDN-BRI-Schnittstelle

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

ISDN-Konfiguration MSN-Konfiguration

Basisparameter	
Portname	bri-0 (TE)
Automatische Konfiguration beim Start	<input checked="" type="checkbox"/> Aktiviert
Ergebnis der automatischen Konfiguration	Port-Verwendung: Nicht verwendet , ISDN-Konfigurationstyp: Punkt-zu-Mehrpunkt
Port-Verwendung	Nicht verwendet ▼
ISDN-Konfigurationstyp	<input checked="" type="radio"/> Punkt-zu-Mehrpunkt <input type="radio"/> Punkt-zu-Punkt
Erweiterte Einstellungen	
X.31 (X.25 im D-Kanal)	<input type="checkbox"/> Aktiviert
OK Abbrechen	

Abb. 44: Physikalische Schnittstellen->ISDN-Ports->ISDN-Konfiguration->

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

Felder im Menü Basisparameter

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Automatische Konfiguration beim Start	Wählen Sie aus, ob der ISDN Switch Typ (D-Kanalerkennung für Wählverbindungen) automatisch erkannt werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Ergebnis der automatischen Konfiguration	Zeigt den Status der ISDN-Autokonfiguration an. Die automatische D-Kanal-Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter Port-Verwendung manuell ausgewählt ist. Das Feld kann nicht editiert werden. Anzeigt wird das Ergebnis der automatischen Konfiguration für die Port-Verwendung und den ISDN-Konfigurationstyp . Mögliche Werte: <ul style="list-style-type: none"> • Alle möglichen Werte für die Port-Verwendung und den ISDN-Konfigurationstyp. • <i>Wird ausgeführt</i>: Erkennung läuft noch.

Feld	Beschreibung
Port-Verwendung	<p>Nur wenn Automatische Konfiguration beim Start deaktiviert ist.</p> <p>Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht verwendet</i>: Der ISDN-Anschluss wird nicht genutzt. • <i>Dialup (Euro-ISDN)</i> • <i>Standleitung</i>
ISDN-Konfigurationstyp	<p>Nur wenn Automatische Konfiguration beim Start deaktiviert ist und für Port-Verwendung = <i>Dialup (Euro-ISDN)</i></p> <p>Wählen Sie die ISDN-Anschlussart aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Punkt-zu-Mehrpunkt</i> (Standardwert): Mehrgeräteeanschluss. • <i>Punkt-zu-Punkt</i>: Anlagenanschluss.
ISDN-Switch-Typ	<p>Nur für Port-Verwendung = <i>Standleitung</i></p> <p>Wählen Sie das ISDN-Protokoll, das Ihnen Ihr Provider zur Verfügung stellt:</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standleitung B1 64S</i>: Festverbindung über B-Kanal 1 (64 kbit/s) • <i>Standleitung B1+B2 64S2</i>: Festverbindung über beide B-Kanäle (128 kbit/s) • <i>Standleitung D+B1+B2 TS02</i>: Festverbindung über D-Kanal und beide B-Kanäle (144 kbit/s) • <i>Standleitung B1+B2 Unterschiedliche Endpunkte</i>: Festverbindung zu zwei verschiedenen Endpunkten. • <i>Standleitung B1+D TS01</i>: Festverbindung über B-Kanal 1 und D-Kanal (80 kbit/s) • <i>Standleitung B2+D TS01</i>: Festverbindung über B-Kanal 2 und D-Kanal (80 kbit/s) • <i>Standleitung B2 64S</i>: Festverbindung über B-Kanal 2 (64

Feld	Beschreibung
	kbit/s)

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
X.31 (X.25 im D-Kanal)	<p>Wählen Sie aus, ob Sie X.31 (X.25 im D-Kanal) z. B. für CAPI-Applikationen nutzen wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
X.31 TEI-Wert	<p>Nur wenn X.31 (X.25 im D-Kanal) aktiviert ist.</p> <p>Bei ISDN-Autokonfiguration wird der X.31-TEI automatisch erkannt. Hat die Autokonfiguration den TEI nicht erkannt, können Sie hier manuell den Wert eingeben, der von der Vermittlungsstelle zugewiesen wurde.</p> <p>Mögliche Werte sind <i>0</i> bis <i>63</i>.</p> <p>Standardwert ist <i>-1</i> (für automatische Erkennung).</p>
X.31 TEI-Dienst	<p>Nur für X.31 (X.25 im D-Kanal) = aktiviert</p> <p>Wählen Sie den Dienst, für den Sie den X.31-TEI nutzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>CAPI</i> • <i>CAPI-Standard</i> • <i>Packet Switch</i> (Standardwert) <p><i>CAPI</i> und <i>CAPI-Standard</i> dienen zur Nutzung des X.31-TEI für CAPI-Applikationen. Bei <i>CAPI</i> wird der in der CAPI-Applikation eingestellte TEI-Wert benutzt, bei <i>CAPI-Standard</i> wird der Wert der CAPI-Applikation ignoriert und immer der hier eingestellte Standardwert benutzt.</p> <p><i>Packet Switch</i> stellen Sie ein, wenn Sie den X.31-TEI für das X.25-Gerät nutzen möchten.</p>

10.2.2 MSN-Konfiguration

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

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

Das Gerät unterstützt die Dienste:

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

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



Hinweis

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

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

10.2.2.1 Neu

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

Abb. 45: **Physikalische Schnittstellen->ISDN-Ports->MSN-Konfiguration->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
ISDN-Port	Wählen Sie den ISDN-Port aus, für den die MSN konfiguriert werden soll.
Dienst	Wählen Sie den Dienst aus, dem ein Ruf auf die untenstehende MSN zugewiesen werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>ISDN-Login</i> (Standardwert): Ermöglicht Einloggen mit

Feld	Beschreibung
	<p><i>ISDN-Login.</i></p> <ul style="list-style-type: none"> • <i>PPP (Routing):</i> Standardeinstellung für PPP-Routing. Enthält die automatische Erkennung der unten genannten PPP-Verbindungen außer <i>PPP DOVB</i>. • <i>IPSec:</i> Ermöglicht die Festlegung einer Rufnummer für IP-Sec-Callback. • <i>Andere (PPP):</i> Weitere Dienste können ausgewählt werden: <i>PPP 64k</i> (Ermöglicht 64 kBit/s PPP-Datenverbindungen), <i>PPP 56k</i> (Ermöglicht 56 kBit/s PPP-Datenverbindungen), <i>PPP V.110 (9600) PPP V.110 (14400)</i>, <i>PPP V.110 (19200)</i>, <i>PPP V.110 (38400)</i> (Ermöglicht PPP-Verbindungen mit V.110 und mit Bit-Raten von 9600 Bit/s, 14400 Bit/s, 19200 Bit/s, 38400 Bit/s), <i>PPP V.120</i> (Ermöglicht eingehende PPP-Verbindungen mit V.120).
MSN	<p>Geben Sie die Rufnummer ein, die zur Überprüfung der Called Party Number verwendet wird, wobei zur Rufannahme eine Übereinstimmung einzelner Ziffern im Eintrag unter Berücksichtigung der Konfiguration in MSN-Erkennung genügt.</p>
MSN-Erkennung	<p>Wählen Sie den Modus aus, mit dem Ihr Gerät den Ziffernvergleich von MSN mit der "Called Party Number" des eingehenden Rufes durchführt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Rechts nach Links</i> (Standardwert) • <i>Links nach Rechts (DDI):</i> Immer auswählen, wenn Ihr Gerät mit einem Point-to-Point-Anschluss (Anlagenanschluss) verbunden ist.
Dienstmerkmal	<p>Wählen Sie die Art des eingehenden Rufes (Diensterkennung) aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Daten + Sprache</i> (Standardwert): Sowohl Daten- als auch Sprachruf. • <i>Daten:</i> Datenruf • <i>Sprache:</i> Sprachruf (Modem, Sprache, analoges Fax)

10.3 UMTS/LTE

10.3.1 UMTS/LTE

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

Eine Liste der unterstützten UMTS/LTE-USB-Sticks finden Sie unter www.teldat.de im Bereich **Produkte**.



Hinweis

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



Hinweis

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

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

10.3.1.1 Bearbeiten

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



Hinweis

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

UMTS/LTE

Grundeinstellungen	
UMTS/LTE-Status	<input checked="" type="checkbox"/> Aktiviert
Modem-Status	Aktiv
Aktuelles Netzwerk	LTE
Mobilfunk-Anbieter	Telekom.de
Netzwerkqualität	 -77 dBm
Bevorzugter Netzwerktyp	Automatisch 
Eingehender Diensttyp	<input checked="" type="radio"/> Deaktiviert <input type="radio"/> ISDN-Login <input type="radio"/> PPP-Einwahl <input type="radio"/> IPsec
SIM-Karte verwendet PIN	••••••••
Fallback-Nummer	
APN (Access Point Name)	internet.telekom

Abb. 46: Physikalische Schnittstellen->UMTS/LTE->UMTS/LTE-> 

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
UMTS/LTE-Status	<p>Wählen Sie aus, ob das gewählte UMTS/LTE-Modem aktiviert werden soll oder nicht.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Modem-Status	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Zeigt den Status des UMTS/LTE-Modems an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> • <i>Inaktiv</i> • <i>Init</i> • <i>Gerufen</i> • <i>Rufend</i> • <i>Verbinden</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>SIM Einlegen erforderlich</i> • <i>PIN Eingabe erforderlich</i> • <i>Fehler</i> • <i>Nicht verbunden</i>
Aktuelles Netzwerk	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Zeigt das aktuelle Netzwerk an, z. B. GSM oder UMTS.</p>
Mobilfunk-Anbieter	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Wird nur angezeigt, wenn sich das Modem im Zustand "up" befindet.</p> <p>Zeigt den aktuell verbundenen Mobilfunk-Anbieter an.</p>
Netzwerkqualität	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Zeigt die aktuelle Qualität der UMTS/LTE-Verbindung an. Der Wert kann nicht verändert werden.</p>
Bevorzugter Netzwerktyp	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Wählen Sie aus, welcher Netzwerktyp bevorzugt verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Für die Verbindung wird automatisch GPRS, UMTS oder LTE gewählt, je nachdem welcher Netzwerktyp örtlich zur Verfügung steht. • <i>Nur GPRS</i>: Nur GPRS wird verwendet, sollte GPRS nicht verfügbar sein, kommt keine Verbindung zustande. • <i>Nur UMTS</i>: Nur UMTS wird verwendet, sollte UMTS nicht verfügbar sein, kommt keine Verbindung zustande. • <i>Bevorzugt GPRS</i>: Es wird bevorzugt GPRS verwendet, sollte GPRS nicht verfügbar sein, wird UMTS verwendet. • <i>Bevorzugt UMTS</i>: Es wird bevorzugt UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet. • <i>Nur LTE</i>: Nur LTE wird verwendet, sollte LTE nicht verfügbar sein, kommt keine Verbindung zustande • <i>LTE preferred (Priorität 4G/3G/2G)</i>: Es wird bevor-

Feld	Beschreibung
	<p>zugt LTE verwendet, sollte LTE nicht verfügbar sein, wird UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet</p> <ul style="list-style-type: none"> • <i>LTE/UMTS (Priorität 4G/3G)</i>: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird UMTS verwendet. • <i>LTE/GPRS (Priorität 4G/2G)</i>: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet. • <i>LTE/GPRS/UMTS (Priorität 4G/2G/3G)</i>: LTE wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird UMTS verwendet. • <i>UMTS/LTE (Priorität 3G/4G)</i>: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird LTE verwendet. • <i>UMTS/GPRS (Priorität 3G/2G)</i>: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird GPRS verwendet. • <i>UMTS/LTE/GPRS (Priorität 3G/4G/2G)</i>: UMTS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von UMTS wird LTE verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet.. • <i>GPRS/LTE (Priorität 2G/4G)</i>: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird LTE verwendet. • <i>GPRS/UMTS (Priorität 2G/3G)</i>: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird UMTS verwendet. • <i>GPRS/LTE/UMTS (Priorität 2G/4G/3G)</i>: GPRS wird verwendet, bei nicht ausreichender Signalstärke und Signalqualität von GPRS wird LTE verwendet, bei nicht ausreichender Signalstärke und Signalqualität von LTE wird UMTS verwendet.

Feld	Beschreibung
	<div data-bbox="544 206 1315 691" style="border: 1px solid #ccc; padding: 10px;">  <p>Hinweis</p> <p>Ein eingehender Datenruf (PPP-Einwahl oder ISDN-Login über V.110) kann in der Regel nur über GSM aufgebaut werden. Für UMTS/LTE ist ein Aufbau nur möglich, wenn der Provider diese Funktionalität auf Antrag freigeschaltet hat.</p> <p>Wenn sich ein Modem im Zustand "up" befindet und Bevorzugter Netzwerktyp nicht <i>Nur UMTS</i> ist, registriert sich das Modem normalerweise im GSM-Netz, damit eingehende Daten-Rufe signalisiert werden können. Wird danach eine Verbindung zum Internet hergestellt, wird in das UMTS-Netz umgeschaltet, sofern UMTS aktuell verfügbar ist.</p> </div>
Eingehender Dienstyp	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Wählen Sie aus, welchem Subsystem des Gateways ein über das Modem eingehender Ruf zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i>: Es erfolgt keine Rufannahme (Standardwert für LTE-Verbindungen). • <i>ISDN-Login</i>: Der Ruf wird dem ISDN-Login-Subsystem zugewiesen (Standardwert für UMTS-Verbindungen). • <i>PPP-Einwahl</i>: Der Ruf wird dem PPP-Subsystem zugewiesen. • <i>IPSec</i>: Der Ruf erfolgt über IPSec. <p>Beachten Sie für die Einstellung Eingehender Dienstyp <i>IP-Sec</i> Folgendes:</p> <p>IPSec-Callback wird dazu verwendet, einen IPSec-Peer zu veranlassen, eine Internetverbindung aufzubauen, um so einen IPSec-Tunnel über das Internet zu ermöglichen. Mit Hilfe eines direkten Anrufs über das UMTS/LTE-Mobilfunknetz kann dem Peer signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den Anruf über Mobilfunk veranlasst, eine Verbindung aufzubauen.</p>

Feld	Beschreibung
	<p>Im Menü VPN->IPSec->IPSec-Peers->->Erweiterte Einstellungen können Sie unter Eigene IP-Adresse per ISDN/GSM übertragen zudem auswählen, ob die IP-Adresse zum IPSec-Tunnelaufbau in dem Callback-UMTS/LTE-Ruf mitgesendet werden soll. Dieses verkürzt und erleichtert unter Umständen den Tunnelaufbau.</p>
PUK	<p>Wird nur angezeigt, wenn das Gerät dreimal vergeblich versucht hat, eine Verbindung aufzubauen, z. B. wenn die PIN der SIM-Karte (siehe das Feld SIM-Karte verwendet PIN) dreimal falsch eingegeben wurde.</p> <p>Geben Sie den PUK (Personal Unblocking Key) Ihrer SIM-Karte ein, um die SIM-Karte zu entsperren.</p>
SIM-Karte verwendet PIN	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Geben Sie die PIN Ihrer UMTS/LTE-Modemkarte ein.</p>
	<p> Hinweis</p> <p>Die Eingabe einer falschen PIN unterbindet die Kommunikation bis der Eintrag korrigiert wird.</p>
	<p> Hinweis</p> <p>Wenn das Gerät dreimal vergeblich versucht hat eine Verbindung aufzubauen, z. B. weil dreimal die falsche PIN eingegeben wurde, so müssen Sie zum Entsperren der SIM-Karte den PUK eingeben.</p>
Fallback-Nummer	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Tragen Sie die Rufnummer für die Funktion GSM Fallback ein.</p> <p>Wenn ein Sprachruf auf diese Nummer eingeht, wird eine ggf. aktive Verbindung sofort getrennt und der Betriebsmodus des Modems auf GSM zurückgesetzt, in welchem das Modem so lange bleibt, bis wieder ein Datenruf (PPP, ISDN-Login, IPSec-Callback) erfolgt. Ist für die WAN-Verbindung der Flatrate-Mo-</p>

Feld	Beschreibung
	<p>dus aktiviert (Option Immer aktiv aktiviert in WAN->Internet + Einwählen->UMTS/LTE->) , führt dies zu sofortigem Verbindungswiederaufbau.</p> <div data-bbox="542 367 1316 555" style="border: 1px solid gray; padding: 5px;"> <p> Hinweis</p> <p>Beachten Sie, dass die SIM-Karte diese Funktion unterstützen muss und nicht alle Mobilfunk-Anbieter Sprachrufe auf Daten-SIM-Karten weiterleiten.</p> </div>
<p>APN (Access Point Name)</p>	<p>Nur für UMTS/LTE-Status = Aktiviert</p> <p>Wenn GPRS/UMTS/LTE benutzt werden soll, müssen Sie hier den sogenannten Access Point Name eintragen, den Sie von Ihrem Provider erhalten haben. Maximal können 80 Zeichen eingegeben werden.</p> <p>Wird hier nichts oder ein falscher APN angegeben, so funktioniert eine konfigurierte GPRS/UMTS/LTE-Verbindung nicht.</p>

Kapitel 11 LAN

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

11.1 IP-Konfiguration

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

11.1.1 Schnittstellen

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

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

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

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

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

Beispiel Teilnetze

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

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

Durch Anklicken der -Schaltfläche gelangen Sie auf eine Seite mit weiterführenden Informationen zu den konfigurierten IP-Adressen der Schnittstelle.

11.1.1.1 Bearbeiten oder Neu

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

Schnittstellen

(VLAN-ID2)					
Basisparameter					
Basierend auf Ethernet-Schnittstelle	Eine auswählen <input type="button" value="v"/>				
Schnittstellenmodus	<input type="radio"/> Untagged <input checked="" type="radio"/> Tagged (VLAN)				
VLAN-ID	<input type="text" value="2"/>				
MAC-Adresse	<input type="text" value="00:a0:f9"/> <input checked="" type="checkbox"/> Voreingestellte verwenden				
Grundlegende IPv4-Parameter					
Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> DHCP				
IP-Adresse / Netzmaske	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;"><input type="text" value="IP-Adresse"/></td> <td style="width: 40%;"><input type="text" value="Netzmaske"/></td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	<input type="text" value="IP-Adresse"/>	<input type="text" value="Netzmaske"/>	<input type="button" value="Hinzufügen"/>	
<input type="text" value="IP-Adresse"/>	<input type="text" value="Netzmaske"/>				
<input type="button" value="Hinzufügen"/>					
Grundlegende IPv6-Parameter					
IPv6	<input checked="" type="checkbox"/> Aktiviert				
Sicherheitsrichtlinie	<input type="radio"/> Unsicher <input checked="" type="radio"/> Sicher				
Zusätzliche IPv6-Adresskonfiguration	<input type="checkbox"/> Aktiviert				
IPv6-Modus	<input type="radio"/> Client <input checked="" type="radio"/> Router				
Rolle bei der Präfixdelegation	<input type="radio"/> Upstream <input checked="" type="radio"/> Downstream				
Router Advertisement übertragen	<input checked="" type="checkbox"/> Aktiviert				
IPv6-Präfix/Länge	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;"><input type="text" value="Upstream-Schnittstelle"/></td> <td style="width: 40%;"><input type="text" value="IPv6-Präfix/Länge"/></td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	<input type="text" value="Upstream-Schnittstelle"/>	<input type="text" value="IPv6-Präfix/Länge"/>	<input type="button" value="Hinzufügen"/>	
<input type="text" value="Upstream-Schnittstelle"/>	<input type="text" value="IPv6-Präfix/Länge"/>				
<input type="button" value="Hinzufügen"/>					
Standardrouter	<input checked="" type="checkbox"/> Aktiviert				

Abb. 47: LAN->IP-Konfiguration->Schnittstellen->Neu

Erweiterte Einstellungen	
Erweiterte IPv4-Einstellungen	
DHCP-MAC-Adresse	<input type="text"/> <input checked="" type="checkbox"/> Voreingestellte verwenden
DHCP-Hostname	<input type="text"/>
DHCP Broadcast Flag	<input checked="" type="checkbox"/> Aktiviert
Proxy ARP	<input type="checkbox"/> Aktiviert
TCP-MSS-Clamping	<input type="checkbox"/> Aktiviert
Erweiterte IPv6-Einstellungen	
Router-Gültigkeitsdauer	<input type="text" value="600"/>
Router-Präferenz	<input type="radio"/> Hoch <input checked="" type="radio"/> Mittel <input type="radio"/> Niedrig
DHCP-Modus	<input type="checkbox"/> Andere - DNS-Server, SIP-Server
	<input type="checkbox"/> Verwaltet - IPv6-Adressverwaltung
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 48: LAN->IP-Konfiguration->Schnittstellen->Neu->Erweiterte Einstellungen

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

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	<p>Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird.</p> <p>Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.</p>
Schnittstellenmodus	<p>Nur bei physikalischen Schnittstellen im Routing-Modus.</p> <p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Tagged (VLAN)</i> (Standardwert): Diese Option gilt nur für Routing-Schnittstellen. <p>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.</p> <ul style="list-style-type: none"> <i>Untagged</i>: Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet.
VLAN-ID	Nur für Schnittstellenmodus = <i>Tagged (VLAN)</i>

Feld	Beschreibung
	<p>Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben.</p> <p>Mögliche Werte sind <i>1</i> (Standardwert) bis <i>4094</i>.</p>
MAC-Adresse	<p>Geben Sie die mit der Schnittstelle verbundene MAC-Adresse ein. Wählen Sie <i>Voreingestellte verwenden</i>, um die vorgegebene Hardware-Adresse zu verwenden.</p> <p>Sie können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde.</p>

Felder im Menü Grundlegende IPv4-Parameter

Feld	Beschreibung
Adressmodus	<p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse / Netzmaske zugewiesen. • <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse / Netzmaske	<p>Nur für Adressmodus = <i>Statisch</i></p> <p>Fügen Sie mit Hinzufügen einen neuen Adresseintrag hinzu und geben Sie die IP-Adresse und die entsprechende Netzmaske der Schnittstelle ein.</p>

Felder im Menü Grundlegende IPv6-Parameter

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob diese Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Sicherheitsrichtlinie	Nur für IPv6 = <i>Aktiviert</i>

Feld	Beschreibung
	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Sicher</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Unsicher</i>: Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 367 konfigurieren.</p>
<p>Zusätzliche IPv6-Adresskonfiguration</p>	<p>Nur für IPv6 = Aktiviert</p> <p>Wählen Sie, ob Sie die automatische IP-Adress-Aushandlung von Unique-Local-Adressen (ULA) und globalen Adressen deaktivieren und die IPv6-Adresse dieser Schnittstelle manuell festsetzen möchten. Link-Local-Adressen werden weiterhin automatisch gebildet.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>IPv6-Adresse</p>	<p>Nur für IPv6 = Aktiviert und Zusätzliche IPv6-Adresskonfiguration = Aktiviert</p> <p>Geben Sie die IPv6-Adresse der Schnittstelle ein. Die entsprechende Länge ist mit einem Wert von 64 fest vorgegeben.</p> <p>Mit Hinzufügen können Sie weitere Adresseinträge hinzufügen.</p>
<p>IPv6-Modus</p>	<p>Nur für IPv6 = Aktiviert</p> <p>Wählen Sie die Funktion, die von der Schnittstelle übernommen wird.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Router</i> (Standardwert): Die Schnittstelle verbindet verschiedene Netze miteinander. • <i>Client</i>: Die Schnittstelle bindet das Teilnetz an ein übergeordnetes Netzwerk an.
Rolle bei der Präfixdelegation	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Router</p> <p>Wählen Sie das Verfahren zur Zuteilung des Präfix.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Downstream</i> (Standardwert): Die Schnittstelle weist das Präfix zu. • <i>Upstream</i>: Der Schnittstelle wird das Präfix zugewiesen oder es wird fest eingestellt.
Router Advertisement übertragen	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router und Prefix Delegation Role = Downstream</p> <p>Wählen Sie, ob Router-Advertisements über die Schnittstelle gesendet werden. Mithilfe der Router-Advertisements wird die Default Router List sowie die Prefix List erstellt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Präfixmodus	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router und Rolle bei der Präfixdelegation = Upstream</p> <p>Wählen Sie, wie das Präfix festgesetzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Präfix beziehen</i> (Standardwert): Der Schnittstelle wird das Präfix zugewiesen. • <i>statisch</i>: Das Präfix der Schnittstelle wird manuell festgesetzt.
IPv6-Präfix/Länge	<p>Für IPv6 = Aktiviert, IPv6-Modus = Router und Rolle bei der Präfixdelegation = Downstream</p> <p>Mithilfe von Hinzufügen legen Sie ein neues IPv6-Präfix an. Dieses können Sie in einem sich neu öffnenden Fenster konfi-</p>

Feld	Beschreibung
	<p>gurieren.</p> <p>Für IPv6 = <i>Aktiviert</i>, IPv6-Modus = <i>Router</i>, Rolle bei der Präfixdelegation = <i>Upstream</i> und Präfixmodus = <i>statisch</i></p> <p>Geben Sie für die Schnittstelle das IPv6-Präfix und die entsprechende Länge sowie optional die IPv6-Adresse des verwendeten Gateways an.</p> <p>Mit Hinzufügen können Sie weitere Präfix-Einträge hinzufügen.</p>
Standardrouter	<p>Nur für IPv6 = <i>Aktiviert</i>, IPv6-Modus = <i>Router</i>, Rolle bei der Präfixdelegation = <i>Downstream</i> und Router Advertisement übertragen = <i>Aktiviert</i></p> <p>Wählen Sie, ob das Gerät als Standardrouter verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Im Feld **IPv6-Präfix/Länge** fügen Sie IPv6-Präfixe hinzu und konfigurieren diese. Sie können auch Präfixe löschen.

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

Schnittstellen

(VLAN-ID2)

Basisparameter

Basierend auf Ethernet-Schnittstelle

Schnittstelle

VLAN-ID

MAC-Adresse

Grundlegende

Adressmodus

IP-Adresse

Grundlegende

IPv6

Sicherheit

Zusätzliche

IPv6-Modus

Rolle bei der

Router-Adve

IPv6-Präfix

Standardrouter Aktiviert

Erweitert

Erweiterte IPv6-Einstellungen

On Link Flag **Wahr**

Autonomous Flag **Wahr**

Bevorzugte Gültigkeitsdauer **Sekunden**

Gültigkeitsdauer **Sekunden**

Erweiterte Einstellungen

Abb. 49: LAN->IP-Konfiguration->Schnittstellen->Hinzufügen

Felder im Menü Basisparameter

Feld	Beschreibung
Upstream-Schnittstelle	<p>Wählen Sie eine IPv6-Schnittstelle aus, welcher ein Präfix zugewiesen werden soll.</p> <p>Für Unique Local Addresses (ULAs) gibt es oft keine Upstream-Schnittstelle, zu der Pakete transportiert werden können. In diesem Fall können Sie die Einstellung <i>Keine</i> verwenden.</p>
Upstream-Präfixe	<p>Für Upstream-Schnittstelle = <code><IPv6-Schnittstelle></code></p> <p>Wählen Sie ein konfiguriertes Präfix aus.</p> <p>Präfixe können Sie bei der Konfiguration einer Schnittstelle im Menü LAN->IP-Konfiguration->Schnittstellen erzeugen, falls Sie unter Rolle bei der Präfixdelegation <i>Upstream</i> auswählen.</p>

Feld	Beschreibung
	<p>len.</p> <p>Andernfalls können Sie Präfixe im Menü Netzwerk->IPv6-Präfixe->IPv6-Präfixe anlegen.</p> <p>Für Upstream-Schnittstelle = <i>Keine</i></p> <p>Geben Sie ein ULA-Präfix (ULA: Unique Local Addresses) ein.</p>
Automatische Subnetzerstellung	<p>Dieser Menüpunkt wird nur angezeigt, falls die Präfixlänge des Upstream-Präfix kleiner als /64 ist.</p> <p>Wählen Sie, ob Sie die automatische Subnetz-Aushandlung aktivieren möchten.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Subnetz	<p>Für Automatische Subnetzerstellung = <i>Aktiviert</i></p> <p>Das automatisch generierte Subnetz wird angezeigt.</p> <p>Für Automatische Subnetzerstellung nicht <i>Aktiviert</i></p> <p>Geben Sie ein Subnetz ein.</p>
Präfix	<p>Nur für Automatische Subnetzerstellung = <i>Aktiviert</i></p> <p>Das automatisch generierte Präfix wird angezeigt.</p>

Das Menü **Erweitert** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
On Link Flag	<p>Wählen Sie, ob das On-Link Flag (L-Flag) gesetzt werden soll. Dadurch fügt der Host das Präfix der Präfixliste hinzu.</p> <p>Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Autonomous Flag	<p>Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll. Dadurch nutzt der Host das Präfix und die 64-Bit-Interface-ID, um daraus seine Adresse abzulei-</p>

Feld	Beschreibung
	<p>ten.</p> <p>Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Bevorzugte Gültigkeitsdauer	<p>Geben Sie eine Zeitspanne in Sekunden an. In diesem Intervall wird das Präfix einem anderen vorgezogen, dessen Bevorzugte Gültigkeitsdauer bereits abgelaufen ist.</p> <p>Der Standardwert ist <i>604800</i> Sekunden.</p>
Gültigkeitsdauer	<p>Geben Sie eine Zeitspanne in Sekunden an, für die das Präfix gültig ist.</p> <p>Der Standardwert ist <i>2592000</i> Sekunden.</p>

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

Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
DHCP-MAC-Adresse	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Ist Voreingestellte verwenden aktiviert (Standardeinstellung) wird die Hardware-MAC-Adresse der Ethernet-Schnittstelle verwendet. Bei physikalischen Schnittstellen ist die aktuelle MAC-Adresse standardmäßig eingetragen.</p> <p>Wenn Sie Voreingestellte verwenden deaktivieren, geben Sie eine MAC-Adresse für die virtuelle Schnittstelle ein, z. B. <i>00:e1:f9:06:bf:03</i>.</p> <p>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.</p>
DHCP-Hostname	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Geben Sie den Hostnamen ein, der vom Provider gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.</p>
DHCP Broadcast Flag	<p>Nur für Adressmodus = <i>DHCP</i></p>

Feld	Beschreibung
	<p>Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für definierte Gegenstellen beantworten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-MSS-Clamping	<p>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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Bei Aktivierung ist im Eingabefeld der Standardwert <i>1350</i> eingetragen.</p>

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
Router-Gültigkeitsdauer	<p>Nur für IPv6 = <i>Aktiviert</i>, IPv6-Modus = <i>Router</i>, Router Advertisement übertragen = <i>Aktiviert</i> und Standardrouter = <i>Aktiviert</i></p> <p>Geben Sie eine Zeitspanne in Sekunden an. Für dieses Intervall verbleibt der Router in der Default Router List.</p> <p>Der Standardwert ist <i>600</i> Sekunden. Der Maximalwert ist <i>65520</i> Sekunden. Ein Wert von <i>0</i> besagt, dass der Router kein Standardrouter ist und nicht in die Default Router List eingetragen werden soll.</p>

Feld	Beschreibung
Router-Präferenz	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router, Router Advertisement übertragen = Aktiviert und Standardrouter = Aktiviert</p> <p>Wählen Sie die Präferenz Ihres Routers für die Wahl des Standardrouters. Dies ist in Fällen nützlich, in denen ein Knoten Advertisements von mehreren Routern erhält oder in Back-Up-Szenarien.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hoch</i> • <i>Mittel</i> (Standardwert) • <i>Niedrig</i>
DHCP-Modus	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus.</p> <div data-bbox="544 912 1315 1035" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> Hinweis</p> <p>Der Router muss nicht als DHCP-Server eingerichtet sein.</p> </div> <p>Mit Auswahl von <i>Andere - DNS-Server, SIP-Server</i> werden nicht-adressbezogene Informationen, wie z. B. DNS, VoIP, usw. durchgeleitet.</p> <p>Mit Auswahl von <i>Verwaltet - IPv6-Adressverwaltung</i> werden Informationen zur IPv6-Adresse weitergeleitet. Die IPv6-Adresse des Client wird dabei über DHCP bereitgestellt und nicht automatisch ausgehandelt.</p> <p>Standardmäßig sind alle Funktionen nicht aktiv.</p>

11.2 VLAN

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

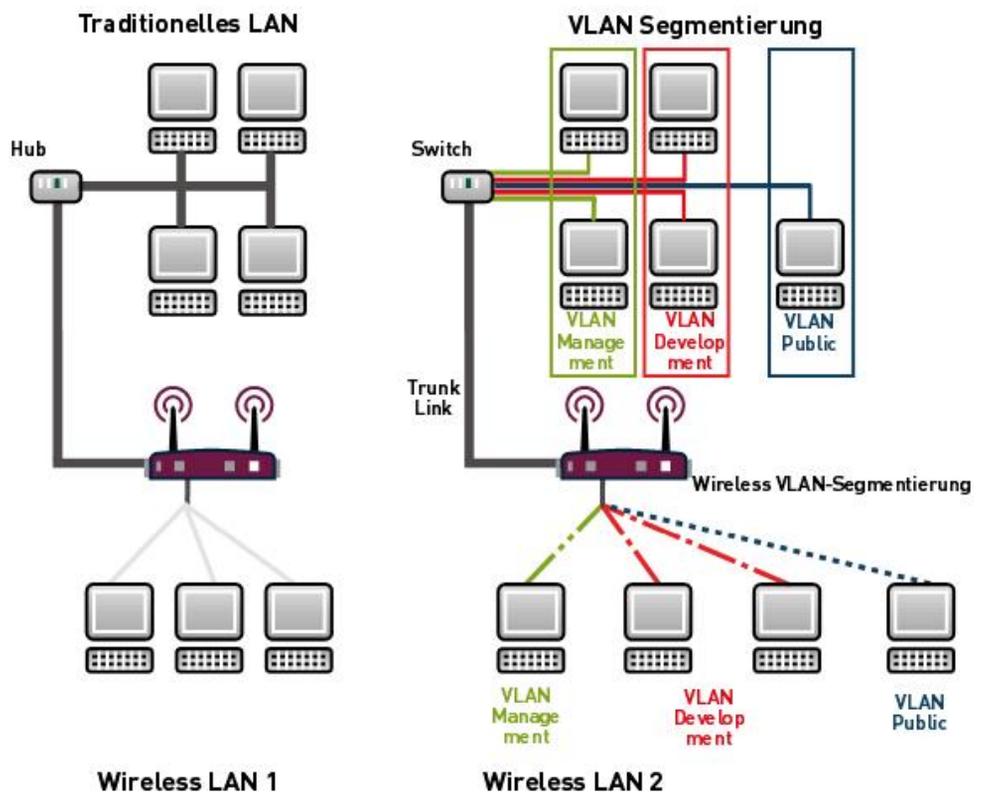


Abb. 50: VLAN-Segmentierung

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**.

11.2.1 VLANs

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

11.2.1.1 Bearbeiten oder Neu

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

VLANs Portkonfiguration Verwaltung

VLAN konfigurieren							
VLAN Identifier	1						
VLAN-Name	Management						
VLAN-Mitglieder	<table border="1"> <tr> <td>Schnittstelle</td> <td>Ausgehende Regel</td> <td>Löschen</td> </tr> <tr> <td>en1-0</td> <td>Untagged</td> <td></td> </tr> </table>	Schnittstelle	Ausgehende Regel	Löschen	en1-0	Untagged	
Schnittstelle	Ausgehende Regel	Löschen					
en1-0	Untagged						
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

Abb. 51: 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

Feld	Beschreibung
	ist eine Zeichenkette mit bis zu 32 Zeichen.
VLAN-Mitglieder	<p>Wählen Sie die Ports aus, die zu diesem VLAN gehören sollen. Über die Schaltfläche Hinzufügen können Sie weitere Mitglieder hinzufügen.</p> <p>Wählen Sie weiterhin zu jedem Eintrag aus, ob die Frames, die von diesem Port übertragen werden, <i>Tagged</i> (also mit VLAN-Information) oder <i>Untagged</i> (also ohne VLAN-Information) übertragen werden sollen.</p>

11.2.2 Portkonfiguration

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

VLANs Portkonfiguration Verwaltung			
Ansicht	20	pro Seite	<< >> Filtern in Keiner gleich Los
Schnittstelle	PVID	Frames ohne Tag verwerfen	Nicht-Mitglieder verwerfen
en1-0	1 - Management	<input type="checkbox"/>	<input type="checkbox"/>
Seite: 1, Objekte: 1 - 1			
		OK	Abbrechen

Abb. 52: 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	<p>Weisen Sie dem ausgewählten Port die gewünschte PVID (Port VLAN Identifier) zu.</p> <p>Wenn ein Paket ohne VLAN-Tag diesen Port erreicht, wird es mit dieser PVID versehen.</p>
Frames ohne Tag verwerfen	Wenn die Option aktiviert ist, werden ungetaggte Frames verworfen. Ist die Option deaktiviert, werden ungetaggte Frames

Feld	Beschreibung
	mit der in diesem Menü definierten PVID getaggt.
Nicht-Mitglieder verwerfen	Wenn die Option aktiviert ist, werden alle getaggten Frames verworfen, die mit einer VLAN-ID getaggt sind, in der der ausgewählte Port nicht Mitglied ist.

11.2.3 Verwaltung

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

Abb. 53: 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 <i>Aktiviert</i> 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 12 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 **bintec 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 **bintec 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.

12.1 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.

12.1.1 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 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.

12.1.2 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.

12.1.3 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.

12.1.3.1 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.

12.1.4 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 zuzuordnen 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.

12.2 Controller-Konfiguration

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

12.2.1 Allgemein

Allgemein

Grundeinstellungen	
Region	Germany ▼
Schnittstelle	LAN_EN1-0 ▼
DHCP-Server	DHCP-Server mit aktivierter CAPWAP Option (138): <input checked="" type="radio"/> Extern oder statisch <input type="radio"/> Intern
Slave-AP-Standort	<input checked="" type="radio"/> Lokal (LAN) <input type="radio"/> Entfernt (WAN)
Slave-AP-LED-Modus	Status ▼

OK
Abbrechen

Abb. 54: 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	<p>Wählen Sie das Land, in welchem der Wireless LAN Controller betrieben werden soll.</p> <p>Mögliche Werte sind alle auf dem Wirelessmodul des Geräts vorkonfigurierten Länder.</p> <p>Der Bereich der verwendbaren Kanäle variiert je nach Länder-einstellung.</p> <p>Standardwert ist <i>Germany</i>.</p>
Schnittstelle	<p>Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.</p>
DHCP-Server	<p>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.</p>

Feld	Beschreibung
	<p>Hinweis: Stellen Sie bei Nutzung eines externen DHCP-Servers sicher, dass CAPWAP Option 138 aktiv ist.</p> <p>Wenn Sie z. B. ein bintec 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 <i>CAPWAP Controller</i> und tragen Sie im Feld Wert die IP-Adresse des WLAN Controllers ein.</p> <p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Extern oder statisch</i> (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. • <i>Intern</i>: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.
IP-Adressbereich	<p>Nur für DHCP-Server = <i>Intern</i></p> <p>Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein. Diese IP-Adressen und Ihr Gerät müssen aus demselben Netz stammen.</p>
Slave-AP-Standort	<p>Wählen Sie aus, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal (LAN)</i> (Standardwert) • <i>Entfernt (WAN)</i> <p>Die Einstellung <i>Entfernt (WAN)</i> ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die</p>

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 <i>Entfernt (WAN)</i> seine Konfiguration bis die Verbindung wieder hergestellt ist. Danach bootet er und anschließend synchronisieren sich Controller und AP erneut.
Slave-AP-LED-Modus	<p>Diese Funktion ist nur für die Access-Points bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n verfügbar.</p> <p>Wählen Sie das Leuchtverhalten der Slave-AP-LEDs.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Status</i> (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde. • <i>Blinkend</i>: Die LEDs zeigen ihr Standardverhalten. • <i>Aus</i>: Alle LEDs sind deaktiviert.

12.3 Slave-AP-Konfiguration

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

12.3.1 Slave Access Points

Slave Access Points Funkmodulprofile Drahtlosnetzwerke (VSS)

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

Ansicht pro Seite Filtern in gleich

Standort	Name	IP-Adresse	LAN-MAC-Adresse	Kanal	Kanalsuche	Status	Aktion
		192.168.0.254	00:01:cd:06:76:fa			🔴 Gefunden	📄

Seite: 1, Objekte: 1 - 1

Abb. 55: 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**).

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.

12.3.1.1 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.

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

Access-Point-Einstellungen					
Gerät	WI2040n				
Standort	<input type="text"/>				
Name	WI2040n				
Beschreibung	<input type="text"/>				
CAPWAP-Verschlüsselung	<input checked="" type="checkbox"/> Aktiviert				
Funkmodul1					
Betriebsmodus	<input checked="" type="radio"/> Ein <input type="radio"/> Aus				
Aktives Funkmodulprofil	Eine auswählen ▾				
Kanal	Kein Profil ausgewählt!				
Verwendeter Kanal	0				
Sendeleistung	Max. ▾				
Zugewiesene Drahtlosnetzwerke (VSS)	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Profil</td> <td style="width: 50%;">MAC-Adresse</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	Profil	MAC-Adresse	<input type="button" value="Hinzufügen"/>	
Profil	MAC-Adresse				
<input type="button" value="Hinzufügen"/>					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 56: 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
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Sie können die Verschlüsselung aufheben, um die Kommunikation zu Debug-Zwecken einzusehen.</p>

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
Betriebsmodus	<p>Zeigt, in welchem Modus das Funkmodul betrieben werden soll. Sie können den Modus ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ein</i> (Standardwert): Das Funkmodul dient als Access Point in Ihrem Netzwerk. • <i>Aus</i> : Das Funkmodul ist nicht aktiv.
Aktives Funkmodulprofil	<p>Zeigt das aktuell gewählte Funkmodulprofil. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere Funkmodulprofile angelegt sind.</p>
Kanal	<p>Zeigt den zugewiesenen Kanal. Sie können einen anderen Kanal wählen.</p> <p>Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.</p> <p>Access Point Modus</p> <p>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.</p> <p>Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden APs diese Kanäle auch unter-</p>

Feld	Beschreibung
	<p>stützen.</p> <p>Mögliche Werte (entsprechend dem gewählten Funkmodulprofil):</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>2,4 GHz In/Outdoor</i> <p>Mögliche Werte sind <i>1 bis 13</i> und <i>Auto</i> (Standardwert).</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz Indoor</i> <p>Mögliche Werte sind <i>36, 40, 44, 48</i> und <i>Auto</i> (Standardwert)</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Outdoor</i> <p>Hier ist nur die Option <i>Auto</i> möglich.</p>
Verwendeter Kanal	<p>Nur für Managed APs.</p> <p>Zeigt den aktuell benutzten Kanal.</p>
Sendeleistung	<p>Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet. • <i>5 dBm</i> • <i>8 dBm</i> • <i>11 dBm</i> • <i>14 dBm</i> • <i>16 dBm</i>
Zugewiesene Drahtlosnetzwerke (VSS)	<p>Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.</p>

12.3.2 Funkmodulprofile

Slave Access Points Funkmodulprofile Drahtlosnetzwerke (VSS)				
Funkmodulprofil	Konfigurierte Funkmodule	Frequenzband	Drahtloser Modus	
2.4 GHz Radio Profile	0	2,4 GHz In/Outdoor	802.11 b/g/n	
5 GHz Radio Profile	0	5 GHz Indoor	802.11 a/n	 

Neu

Abb. 57: 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**).

12.3.2.1 Bearbeiten oder Neu

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

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

Funkmodulprofil-Konfiguration											
Beschreibung	2.4 GHz Radio Profile										
Betriebsmodus	Access-Point										
Frequenzband	2,4 GHz In/Outdoor										
Anzahl der Spatial Streams	2										
Performance-Einstellungen											
Drahtloser Modus	802.11b/g/n										
Max. Übertragungsrate	Auto										
Burst-Mode	<input type="checkbox"/> Aktiviert										
Erweiterte Einstellungen											
Kanalplan	Benutzerdefiniert										
Benutzerdefinierter Kanalplan	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Kanal</th> <th style="width: 50%;"></th> </tr> </thead> <tbody> <tr> <td>1</td> <td></td> </tr> <tr> <td>6</td> <td></td> </tr> <tr> <td>11</td> <td></td> </tr> <tr> <td colspan="2" style="text-align: center;">Hinzufügen</td> </tr> </tbody> </table>	Kanal		1		6		11		Hinzufügen	
Kanal											
1											
6											
11											
Hinzufügen											
Beacon Period	100 ms										
DTIM Period	2										
RTS Threshold	2347										
Short Guard Interval	<input type="checkbox"/> Aktiviert										
Short Retry Limit	7										
Long Retry Limit	4										
Fragmentation Threshold	2346 Bytes										
OK Abbrechen											

Abb. 58: 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 Funkmodulprofil betrieben werden soll.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Das Funkmodulprofil ist nicht aktiv. • <i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk.
Frequenzband	<p>Wählen Sie das Frequenzband des Funkmodulprofils aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2,4 GHz In/Outdoor</i> (Standardwert): Ihr Gerät wird mit 2,4 GHz (Mode 802.11b, Mode 802.11g und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. • <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb von Gebäuden betrieben. • <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) außerhalb von Gebäuden betrieben. • <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. • <i>5,8 GHz Outdoor</i>: 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	<p>Nicht für Frequenzband = <i>2,4 GHz In/Outdoor</i></p> <p>Wählen Sie aus, wieviele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>20 MHz</i> (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • <i>40 MHz</i>: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal.
Anzahl der Spatial Streams	<p>Wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • 2 (Standardwert): Zwei Datenströme werden verwendet. • 1: Ein Datenstrom wird verwendet.

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	<p>Wählen Sie die Wireless-Technologie aus, die der Access-Point anwenden soll.</p> <p>Für Frequenzband = 2,4 GHz In/Outdoor</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>802.11g</i>: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • <i>802.11b</i>: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • <i>802.11 mixed (b/g)</i> : Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. • <i>802.11 mixed long (b/g)</i>: 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. • <i>802.11 mixed short (b/g)</i>: 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). • <i>802.11b/g/n</i>: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. • <i>802.11g/n</i>: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n. • <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. <p>Für Frequenzband = 5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor oder 5,8 GHz Outdoor</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>802.11a</i>: Ihr Gerät arbeitet ausschließlich nach 802.11a. • <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. • <i>802.11a/n</i>: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n.
Max. Übertragungsrate	<p>Wählen Sie die Übertragungsgeschwindigkeit aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt. • <i><Wert></i>: Je nach Einstellung für Frequenzband, Bandbreite, Anzahl der Spatial Streams und Drahtloser Modus stehen verschiedene feste Werte in MBit/s zur Auswahl.
Burst-Mode	<p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion nicht aktiv sein.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Kanalplan	<p>Wählen Sie den gewünschten Kanalplan aus.</p> <p>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.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Alle</i>: Alle Kanäle können bei der Kanalwahl gewählt werden. • <i>Auto</i>: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • <i>Benutzerdefiniert</i>: Sie können die gewünschten Kanäle selbst auswählen.
Benutzerdefinierter Kanalplan	<p>Nur für Kanalplan = <i>Benutzerdefiniert</i></p> <p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <p>Mit Hinzufügen können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen.</p> <p>Mithilfe von -Symbol können Sie Einträge löschen.</p>
Beacon Period	<p>Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an.</p> <p>Dieser Wert wird in Beacon und Probe Response Frames übermittelt.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Standardwert ist 100.</p>
DTIM Period	<p>Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an.</p> <p>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.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 2.</p>
RTS Threshold	<p>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</p>

Feld	Beschreibung
	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	<p>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.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 7.</p>
Long Retry Limit	<p>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.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 4.</p>
Fragmentation Threshold	<p>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.</p> <p>Möglich Werte sind 256 bis 2346.</p> <p>Der Standardwert ist 2346.</p>

12.3.3 Drahtlosnetzwerke (VSS)

[Slave Access Points](#) | [Funkmodulprofile](#) | **Drahtlosnetzwerke (VSS)**

VSS-Beschreibung	Netzwerkname (SSID)	Anzahl der zugeordneten Funkmodule	Sicherheit	Status	Aktion		
vss-1	default	0	WPA-PSK				
Nicht zugewiesenes VSS allen Funkmodulen zuweisen		<input type="button" value="START"/>					
<input type="button" value="Neu"/>							

Abb. 59: 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.

12.3.3.1 Bearbeiten oder Neu

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

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

Service Set Parameter	
Netzwerkname (SSID)	<input type="text"/> <input checked="" type="checkbox"/> Sichtbar
Intra-cell Repeating	<input checked="" type="checkbox"/> Aktiviert
ARP Processing	<input type="checkbox"/> Aktiviert
WMM	<input checked="" type="checkbox"/> Aktiviert
Max. Clients	<input type="text" value="32"/>
Sicherheitseinstellungen	
Sicherheitsmodus	<input type="text" value="Inaktiv"/> ▼
MAC-Filter	
ACL-Modus	<input type="checkbox"/> Aktiviert
Erlaubte Adressen	<input type="text" value="MAC-Adresse"/> <input type="button" value="Hinzufügen"/>
VLAN	
VLAN	<input type="checkbox"/> Aktiviert

Abb. 60: 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)	<p>Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.</p> <p>Wählen Sie außerdem aus, ob der Netzwerkname (SSID) übertragen werden soll.</p> <p>Mit Auswahl von <i>Sichtbar</i> wird der Netzwerkname sichtbar übertragen.</p> <p>Standardmäßig ist er sichtbar.</p>
Intra-cell Repeating	<p>Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
ARP Processing	<p>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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Beachten Sie, dass ARP Processing nicht zusammen mit der Funktion MAC-Bridge angewendet werden kann.</p>
WMM	<p>Wählen Sie aus, ob für das Drahtlosnetzwerk Sprach- oder Videodaten- Priorisierung mittels WMM (Wireless Multimedia) aktiviert sein soll, um stets eine optimale Übertragungsqualität bei zeitkritischen Anwendungen zu erreichen. Es wird Datenpriorisierung nach DSCP (Differentiated Services Code Point) oder IEEE802.1d unterstützt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Max. Clients	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl kann auf alle konfigurierten Drahtlosnetzwerke aufgeteilt werden. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p>

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	<p>Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): weder Verschlüsselung noch Au-

Feld	Beschreibung
	<p>thentifizierung</p> <ul style="list-style-type: none"> • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Key • <i>WPA-Enterprise</i>: 802.11x
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Standardwert ist <i>Schlüssel 1</i>.</p>
WEP-Schlüssel 1-4	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> , <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein.</p> <p>Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen, z. B. <i>hallo</i> für <i>WEP 40</i>, <i>teldat-wep104</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> und <i>WPA 2</i> (Standardwert): WPA und WPA 2 können angewendet werden. • <i>WPA</i> : Nur WPA wird angewendet. • <i>WPA 2</i> : Nur WPA2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA</i> und <i>WPA</i> und <i>WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): TKIP wird angewendet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>AES</i> : AES wird angewendet.
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA 2</i> und <i>WPA</i> und <i>WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): AES wird angewendet. • <i>TKIP</i> : TKIP wird angewendet.
Preshared Key	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.</p> <p>Beachten Sie: Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p>
RADIUS-Server	<p>Sie können den Zugang zu einem Drahtlosnetzwerk über einen RADIUS-Server regeln.</p> <p>Mit Hinzufügen können Sie neue Einträge anlegen. Geben Sie die IP-Adresse und das Passwort des RADIUS-Servers ein.</p>
EAP-Vorabauthentifizierung	<p>Nur für Sicherheitsmodus = <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob EAP-Vorabauthentifizierung aktiviert werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü MAC-Filter

Feld	Beschreibung
ACL-Modus	<p>Wählen Sie aus, ob für dieses Drahtlosnetzwerk nur bestimmte Clients zugelassen werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erlaubte Adressen	<p>Legen Sie Einträge mit Hinzufügen an und geben Sie die MAC-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.</p>

Felder im Menü VLAN

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

12.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.

12.4.1 Aktive Clients

Aktive Clients
[Drahtlosnetzwerke \(VSS\)](#)
[Benachbarte APs](#)
[Rogue APs](#)

Automatisches Aktualisierungsintervall Sekunden

Ansicht pro Seite Filtern in gleich

Standort	Name	VSS	Client MAC	Client-IP-Adresse	Signal : Noise (dBm)	Status	Uptime
Seite: 1							

Abb. 61: 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.

12.4.2 Drahtlosnetzwerke (VSS)



Abb. 62: **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, VSS, MAC-Adresse (VSS), Kanal, Clients, Status**).

12.4.3 Benachbarte APs



Abb. 63: **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 Rogue 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.

12.4.4 Rogue APs



Abb. 64: **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.

12.5 Wartung

Dieses Menü dient zur Wartung Ihrer managed APs.

12.5.1 Firmware-Wartung

Firmware-Wartung

Managed Access Points						
Firmware aktualisieren Alle auswählen / Alle deaktivieren	Standort ▲	Gerät	IP-Adresse	LAN-MAC-Adresse	Firmware-Version	Status
Aktion		Systemsoftware aktualisieren ▼				
Quelle		HTTP-Server ▼				
URL		<input type="text"/>				
		<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>				

Abb. 65: 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	<p>Wählen Sie die Aktion aus, die Sie ausführen wollen.</p> <p>Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware initiieren. • <i>Konfiguration mit Statusinformationen sichern</i>: Sie können eine Konfiguration sichern, welche Statusinformationen der APs enthält.
Quelle	<p>Wählen Sie die Quelle für die Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>HTTP-Server</i> (Standardwert): Die Datei ist bzw. wird auf dem entfernten Server gespeichert, der in der URL angegeben wird.

Feld	Beschreibung
	<ul style="list-style-type: none">• <i>Aktuelle Software vom Teldat-Server</i>: Die Datei liegt auf dem offiziellen Teldat-Update-Server. (Nur für Aktion = <i>Systemsoftware aktualisieren</i>)• <i>TFTP-Server</i>: Die Datei ist bzw. wird auf dem TFTP-Server gespeichert, der in der URL angegeben wird.
URL	Nur für Quelle = <i>HTTP-Server</i> oder <i>TFTP-Server</i> Geben Sie die URL des Servers ein, von dem die Systemsoftware-Datei geladen werden soll bzw. auf dem die Konfigurationsdatei gespeichert werden soll.

Kapitel 13 Netzwerk

13.1 Routen

Standard-Route (Default Route)

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

13.1.1 IPv4-Routen

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

13.1.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere IPv4-Routen anzulegen.

Routenklasse	
Erweiterte Route	<input type="checkbox"/> Aktiviert
Routenparameter	
Routentyp	Netzwerkroute ▾
Ziel-IP-Adresse/Netzmaske	<input type="text"/> / <input type="text"/>
Schnittstelle	Keine ▾
Netzwerktyp	Direkt ▾
Lokale IP-Adresse	0.0.0.0
Metrik	1 ▾
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 66: Netzwerk->Routen->IPv4-Routen->Neu mit **Erweiterte Route** = nicht aktiviert

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

Routenklasse	
Erweiterte Route	<input checked="" type="checkbox"/> Aktiviert
Routenparameter	
Routentyp	Netzwerkroute ▾
Ziel-IP-Adresse/Netzmaske	<input type="text"/> / <input type="text"/>
Schnittstelle	Keine ▾
Netzwerktyp	Direkt ▾
Lokale IP-Adresse	0.0.0.0
Metrik	1 ▾
Erweiterte Routenparameter	
Quellschnittstelle	Keine ▾
Quell-IP-Adresse/Netzmaske	0.0.0.0 / 0.0.0.0
Layer 4-Protokoll	Beliebig ▾
Quellport	Beliebig ▾ Port -1 bis Port -1
Zielpport	Beliebig ▾ Port -1 bis Port -1
DSCP-/TOS-Wert	Nicht beachten ▾
Modus	Wählen und warten ▾
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 67: Netzwerk->Routen->IPv4-Routen->Neu mit **Erweiterte Route** = Aktiviert

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

Feld im Menü Routenklasse

Feld	Beschreibung
Erweiterte Route	<p>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 Geräteschnittstelle angelegt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Routenparameter

Feld	Beschreibung
Routentyp	<p>Wählen Sie die Art der Route aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Netzwerkroute</i> (Standardwert): Route zu einem Netzwerk. • <i>Standardroute</i>: Wird benutzt, wenn keine andere passende Route verfügbar ist. • <i>Hostroute</i>: Route zu einem einzelnen Host.
Ziel-IP-Adresse/Netzmaske	<p>Nur für Routentyp <i>Hostroute</i> oder <i>Netzwerkroute</i></p> <p>Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein.</p> <p>Bei Routentyp = <i>Netzwerkroute</i> Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.</p>
Schnittstelle	<p>Wählen Sie ggf. die Schnittstelle aus, welche für diese Route verwendet werden soll.</p>
Netzwerktyp	<p>Nicht für Routentyp = <i>Standardroute</i></p> <p>Wählen Sie zusätzlich den Netzwerktyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Direkt</i> (Standardwert):

Feld	Beschreibung
	<ul style="list-style-type: none"> • im LAN: Sie definieren eine weitere IP-Adresse für die Schnittstelle. • im WAN: Sie definieren eine Route ohne Transitnetzwerk. • <i>Indirekt</i>: <ul style="list-style-type: none"> • im LAN: Sie definieren eine Gateway-Route. • im WAN: Sie definieren eine Route mit Transitnetzwerk.
Lokale IP-Adresse	<p>Nur für Netzwerktyp = <i>Direkt</i></p> <p>Geben Sie die IP-Adresse des Gateways ein, an das Ihr Gerät die IP-Pakete weitergeben soll.</p>
Gateway	<p>Nur für Netzwerktyp = <i>Indirekt</i></p> <p>Geben Sie die IP-Adresse des Hosts ein, an den Ihr Gerät die IP-Pakete weitergeben soll.</p>
Metrik	<p>Wählen Sie die Priorität der Route aus.</p> <p>Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.</p> <p>Wertebereich von <i>0</i> bis <i>15</i> . Standardwert ist <i>1</i> .</p>

Felder im Menü Erweiterte Routenparameter

Feld	Beschreibung
Quellschnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen.</p> <p>Standardwert ist <i>Keine</i> .</p>
Neue Quell-IP-Adresse/Netzmaske	<p>Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.</p>
Layer 4-Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Mögliche Werte: <i>ICMP, IGMP, TCP, UDP, GRE, ESP, AH, OSPF, PIM, L2TP, Beliebig</i> .</p> <p>Standardwert ist <i>Beliebig</i> .</p>
Quellport	<p>Nur für Layer 4-Protokoll = <i>TCP</i> oder <i>UDP</i></p>

Feld	Beschreibung
	<p>Geben Sie den Quellport an.</p> <p>Wählen Sie zunächst den Portnummernbereich aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Route gilt für alle Port-Nummern. • <i>Einzeln</i>: Ermöglicht Eingabe einer Port-Nummer. • <i>Bereich</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • <i>Privilegiert</i>: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • <i>Server</i>: Eingabe von Server Port-Nummern: 5000 ... 32767. • <i>Clients 1</i>: Eingabe von Client Port-Nummern: 1024 ... 4999. • <i>Clients 2</i>: Eingabe von Client Port-Nummern: 32768 ... 65535. • <i>Nicht privilegiert</i>: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. <p>Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in Port (einzelner bzw. Anfangsport) und ggf. in bis Port (Endport) die entsprechenden Werte ein.</p>
Zielport	<p>Nur für Layer 4-Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie den Zielport an.</p> <p>Wählen Sie zunächst den Portnummernbereich aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Route gilt für alle Port-Nummern. • <i>Einzeln</i>: Ermöglicht Eingabe einer Port-Nummer. • <i>Bereich</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • <i>Privilegiert</i>: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • <i>Server</i>: Eingabe von Server Port-Nummern: 5000 ... 32767.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Clients 1</i>: Eingabe von Client Port-Nummern: 1024 ... 4999. • <i>Clients 2</i>: Eingabe von Client Port-Nummern: 32768 ... 65535. • <i>Nicht privilegiert</i>: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. <p>Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in Port (einzelner bzw. Anfangsport) und ggf. in bis Port (Endport) die entsprechenden Werte ein.</p>
DSCP-/TOS-Wert	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F. <p>Geben Sie für <i>DSCP-Binärwert</i>, <i>DSCP-Dezimalwert</i>, <i>DSCP-Hexadezimalwert</i>, <i>TOS-Binärwert</i>, <i>TOS-Dezimalwert</i> und <i>TOS-Hexadezimalwert</i> den entsprechenden Wert ein.</p>
Modus	<p>Wählen Sie aus, wann die in Routenparameter->Schnittstelle definierte Schnittstelle benutzt werden soll.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Wählen und warten</i> (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", wird solange gewählt und gewartet, bis die Schnittstelle "aktiv" ist. • <i>Verbindlich</i>: Die Route ist immer benutzbar. • <i>Wählen und fortfahren</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", wird solange gewählt und eine alternative Route verwendet (Rerouting), bis die Schnittstelle "aktiv" ist. • <i>Nie einwählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. • <i>Immer wählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wird solange gewählt und gewartet, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

13.1.2 IPv6-Routen

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

13.1.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Routen anzulegen.

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

[IPv4-Routen](#) | [IPv6-Routen](#) | [Optionen](#)

Routenparameter	
Beschreibung	<input type="text"/>
Route aktiv	<input checked="" type="checkbox"/> Aktiviert
Routentyp	Indirekt ▾
Zielschnittstelle	Eine auswählen ▾
Quelladresse/Länge	<input type="text"/> /64
Zieladresse/Länge	<input type="text"/> /64
Gateway-Adresse	<input type="text"/>

|

Abb. 68: **Netzwerk->Routen->IPv6-Routen->Neu**

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

Feld im Menü Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IPv6-Route an.
Route aktiv	Wählen Sie, ob die Route aktiv oder inaktiv sein soll. Mit <i>Aktiviert</i> wird die Route auf den Status aktiv gesetzt. Standardmäßig ist die Funktion aktiv.
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Indirekt</i> (Standardwert): Zielknoten sind nur indirekt zu erreichen. Geben Sie eine gültige IPv6-Adresse für den nächsten Hop an. • <i>Direkt</i> : Alle Zielknoten können über eine direkte Route erreicht werden.
Zielschnittstelle	Wählen Sie die IPv6-Schnittstelle aus, welche für diese Route verwendet werden soll.
Quelladresse/Länge	Geben Sie die Quell-IPv6-Adresse mit der entsprechenden Präfixlänge ein. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.

Feld	Beschreibung
Zieladresse/Länge	Geben Sie die Ziel-IPv6-Adresse mit der entsprechenden Präfixlänge ein. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.
Gateway-Adresse	Nur für Routentyp = <i>Indirekt</i> Geben Sie die IPv6-Adresse für den nächsten Hop ein.

13.1.3 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.

IPv4-Routen IPv6-Routen Optionen

Überprüfung der Rückroute

Modus
 Für alle Schnittstellen aktivieren
 Für bestimmte Schnittstellen aktivieren
 Für alle Schnittstellen deaktivieren

Ansicht 20 pro Seite Filtern in Keiner gleich Los

Nr.	Schnittstelle	Überprüfung der Rückroute
1	en1-0	<input type="checkbox"/> Aktiviert
2	en1-4	<input type="checkbox"/> Aktiviert
3	en1-0-1	<input type="checkbox"/> Aktiviert

Seite: 1, Objekte: 1 - 3

Allgemein

Löschen/Editieren aller Routing-Einträge erlauben Aktiviert

OK Abbrechen

Abb. 69: Netzwerk->Routen->Optionen

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

Felder im Menü Überprüfung der Rückroute

Feld	Beschreibung
Modus	<p>Wählen Sie hier aus, wie die Schnittstellen spezifiziert werden sollen, für die eine Überprüfung der Rückroute aktiviert wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Für alle Schnittstellen aktivieren</i>: Überprüfung der Rückroute wird für alle Schnittstellen aktiviert. • <i>Für bestimmte Schnittstellen aktivieren</i> (Standardwert): Eine Liste aller Schnittstellen wird angezeigt, in der Überprüfung der Rückroute nur für spezifische Schnittstellen aktiviert wird. • <i>Für alle Schnittstellen deaktivieren</i>: Überprüfung der Rückroute wird für alle Schnittstellen deaktiviert.
Nr.	<p>Nur für Modus = <i>Für bestimmte Schnittstellen aktivieren</i></p> <p>Zeigt die laufende Nummer des Listeneintrags an.</p>
Schnittstelle	<p>Nur für Modus = <i>Für bestimmte Schnittstellen aktivieren</i></p> <p>Zeigt den Namen der Schnittstelle an.</p>
Überprüfung der Rückroute	<p>Nur für Modus = <i>Für bestimmte Schnittstellen aktivieren</i></p> <p>Wählen Sie aus, ob <i>Überprüfung der Rückroute</i> für diese Schnittstelle aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion für alle Schnittstellen deaktiviert.</p>

Felder im Menü Allgemein

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

13.2 IPv6-Präfixe

In diesem Menü definieren Sie die von Ihrem Router verwendeten IPv6-Präfixe (Subnetze).

13.2.1 IPv6-Präfixe

Im Menü **Netzwerk->IPv6-Präfixe->IPv6-Präfixe** wird eine Liste aller konfigurierter IPv6-Präfixe angezeigt.

IPv6-Präfixe

Präfix	Typ	Upstream-Schnittstelle	Subnetze	Präfix aktiv		
::/48	dynamisch	en1-0-1	Ja	<input checked="" type="checkbox"/> Aktiviert		
2001:db8:85a3::/48	statisch	en1-0-1	Nein	<input checked="" type="checkbox"/> Aktiviert		

Seite: 1, Objekte: 1 - 2

Abb. 70: **Netzwerk->IPv6-Präfixe->IPv6-Präfixe**

13.2.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Präfixe anzulegen.

IPv6-Präfixe

Basisparameter											
Präfix aktiv	<input checked="" type="checkbox"/> Aktiviert										
Konfigurationsmodus	<input checked="" type="radio"/> Dynamisch <input type="radio"/> Statisch										
Upstream-Schnittstelle	Eine auswählen										
Link-Präfix	<table border="1"> <tr> <td>Downstream-Schnittstelle</td> <td>Subnetz</td> <td>Link-Präfix</td> <td>Link-Präfix aktiv</td> <td></td> </tr> <tr> <td colspan="5" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	Downstream-Schnittstelle	Subnetz	Link-Präfix	Link-Präfix aktiv		<input type="button" value="Hinzufügen"/>				
Downstream-Schnittstelle	Subnetz	Link-Präfix	Link-Präfix aktiv								
<input type="button" value="Hinzufügen"/>											

Abb. 71: **Netzwerk->IPv6-Präfixe->IPv6-Präfixe->Neu**

Das Menü **Netzwerk->IPv6-Präfixe->IPv6-Präfixe->Neu** besteht aus folgenden Feldern:

Feld im Menü **Basisparameter**

Feld	Beschreibung
Präfix aktiv	<p>Wählen Sie, ob das Präfix aktiv oder inaktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird das Präfix auf den Status aktiv gesetzt.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Konfigurationsmodus	<p>Wählen Sie, wie der Adressraum zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Dynamisch</i> (Standardwert): Der Adressraum wird dynamisch mittels einer DHCP-Übertragung des Präfixes festgesetzt. • <i>Statisch</i>: Das Präfix wird durch Sie fest vorgegeben.
Upstream-Schnittstelle	<p>Wählen Sie eine IPv6-Schnittstelle aus, welcher ein Adressraum zugewiesen werden soll.</p> <p>Für Unique Local Addresses (ULAs) gibt es oft keine Upstream-Schnittstelle, zu der Pakete transportiert werden können. In diesem Fall können Sie die Einstellung <i>Keiner</i> verwenden. Dazu muss der Konfigurationsmodus <i>Statisch</i> ausgewählt sein.</p>
Benutzer Präfix/Länge	<p>Nur für Konfigurationsmodus = <i>Statisch</i></p> <p>Geben Sie das Präfix ein, das verwendet werden soll. Geben Sie die zugehörige Länge ein.</p> <p>Standardmäßig ist die Länge /48 vorgegeben.</p>
Netzwerktyp	<p>Nur für Konfigurationsmodus = <i>Statisch</i></p> <p>Wählen Sie die Art der Route aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Indirekt</i> (Standardwert): Zielknoten sind nur indirekt zu erreichen. Geben Sie eine gültige IPv6-Adresse für den nächsten Hop an. • <i>Direkt</i>: Alle Zielknoten können über eine direkte Route erreicht werden.
Gateway-Adresse	<p>Nur für Konfigurationsmodus = <i>Statisch</i> und Netzwerktyp = <i>Indirekt</i></p> <p>Geben Sie die IPv6-Adresse für den nächsten Hop ein.</p>

Feld	Beschreibung
Link-Präfix	Mithilfe von Hinzufügen legen Sie ein neues Link-Präfix an.

Im Feld **Link-Präfix** fügen Sie Präfixe hinzu und konfigurieren diese. Sie können auch Präfixe löschen.

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

Abb. 72: Netzwerk->IPv6-Präfixe->IPv6-Präfixe->Hinzufügen

Felder im Menü Basisparameter

Feld	Beschreibung
Link-Präfix aktiv	<p>Wählen Sie, ob das Link-Präfix aktiv oder inaktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird das Link-Präfix auf den Status aktiv gesetzt.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Downstream-Schnittstelle	<p>Wählen Sie eine IPv6-Schnittstelle aus, welcher ein Adressraum zugewiesen werden soll.</p> <p>Hier werden alle Schnittstellen angezeigt, die nicht als Upstream-Schnittstellen konfiguriert sind.</p>

Feld	Beschreibung
Automatische Subnetzerstellung	<p>Wählen Sie, ob das Subnetz automatisch konfiguriert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Das erste, automatisch erzeugte Subnetz ist das Subnetz "0".</p>
Subnetz	<p>Kann nur konfiguriert werden, falls die Automatische Subnetzerstellung deaktiviert ist. Andernfalls wird hier das automatisch generierte Subnetz angezeigt.</p> <p>Wählen Sie das verwendete Subnetz.</p>
Präfix	<p>Nur für Automatische Subnetzerstellung = <i>Aktiviert</i></p> <p>Zeigt das automatisch erzeugte Präfix an.</p>

Das Menü **Erweitert** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
On Link Flag	<p>Wählen Sie, ob das On-Link Flag (L-Flag) gesetzt werden soll. Dadurch fügt der Host das Präfix der Präfixliste hinzu.</p> <p>Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Autonomous Flag	<p>Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll. Dadurch nutzt der Host das Präfix und die 64-Bit-Interface-ID, um daraus seine Adresse abzuleiten.</p> <p>Ein Präfix mit diesem Flag kann nur automatisch konfiguriert werden.</p> <p>Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

13.3 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (= Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in *NAT-Konfiguration* auf Seite 188).

13.3.1 NAT-Schnittstellen

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



Abb. 73: **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

Feld	Beschreibung
	<p>Server Services testen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Verwerfen ohne Rückmeldung	<p>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.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
PPTP-Passthrough	<p>Wählen Sie aus, ob auch bei aktiviertem NAT der Aufbau und Betrieb mehrerer gleichzeitig ausgehender PPTP-Verbindungen von Hosts im Netzwerk erlaubt sein soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn PPTP-Passthrough aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpunkt konfiguriert werden.</p>
Portweiterleitungen	<p>Zeigt die Anzahl der in Netzwerk->NAT->NAT-Konfiguration konfigurierten Portweiterleitungsregeln an.</p>

13.3.2 NAT-Konfiguration

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

13.3.2.1 Neu

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

NAT-Schnittstellen
NAT-Konfiguration

Basisparameter	
Beschreibung	<input type="text"/>
Schnittstelle	Beliebig ▾
Art des Datenverkehrs	eingehend (Ziel-NAT) ▾
Ursprünglichen Datenverkehr angeben	
Dienst	Benutzerdefiniert ▾
Protokoll	Beliebig ▾
Quell-IP-Adresse/Netzmaske	Beliebig ▾
Original Ziel-IP-Adresse/Netzmaske	Beliebig ▾
Substitutionswerte	
Neue Ziel-IP-Adresse/Netzmaske	Host ▾ <input type="text" value="0.0.0.0"/>
OK Abbrechen	

Abb. 74: 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	<p>Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Beliebig</i> (Standardwert): NAT wird für alle Schnittstellen konfiguriert. <i><Schnittstellename></i>: Wählen Sie eine der Schnittstellen aus der Liste aus.
Art des Datenverkehrs	<p>Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>eingehend (Ziel-NAT)</i> (Standardwert): Der Datenverkehr, der von außen kommt. <i>ausgehend (Quell-NAT)</i>: Der Datenverkehr, der nach außen geht. <i>exklusiv (ohne NAT)</i>: Der Datenverkehr, der von NAT

Feld	Beschreibung
	ausgenommen ist.
NAT-Methode	<p>Nur für Art des Datenverkehrs = <i>ausgehend</i> (<i>Quell-NAT</i>)</p> <p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>full-cone</i> (nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiiierende Quelladresse und den initialen Quellport senden. • <i>restricted-cone</i> (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen. • <i>port-restricted-cone</i> (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • <i>symmetrisch</i> (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	<p>Nicht für Art des Datenverkehrs = <i>ausgehend</i> (<i>Quell-NAT</i>) und NAT-Methode = <i>full-cone</i>, <i>restricted-cone</i> oder <i>port-restricted-cone</i>.</p> <p>Wählen Sie einen der vorkonfigurierten Dienste aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Benutzerdefiniert</i> (Standardwert) • <i><Dienstname></i>
Protokoll	<p>Nur für bestimmte Dienste.</p> <p>Nicht für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i> und NAT-Methode = <i>full-cone, restricted-cone oder port-restricted-cone</i>. In diesem Fall wird UDP automatisch festgelegt.</p> <p>Wählen Sie ein Protokoll aus. Je nach ausgewähltem Dienst stehen verschiedene Protokolle zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>AH</i> • <i>Chaos</i> • <i>EGP</i> • <i>ESP</i> • <i>GGP</i> • <i>GRE</i> • <i>HMP</i> • <i>ICMP</i> • <i>IGMP</i> • <i>IGP</i> • <i>IGRP</i> • <i>IP</i> • <i>IPinIP</i> • <i>IPv6</i> • <i>IPX in IP</i> • <i>ISO-IP</i> • <i>Kryptolan</i> • <i>L2TP</i> • <i>OSPF</i> • <i>PUP</i> • <i>RDP</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>RSVP</i> • <i>SKIP</i> • <i>TCP</i> • <i>TLSP</i> • <i>UDP</i> • <i>VRRP</i> • <i>XNS-IDP</i>
Quell-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i> oder <i>exklusiv (ohne NAT)</i></p> <p>Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
Original Ziel-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i></p> <p>Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
Original Ziel-Port/Bereich	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i></p> <p>Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> bedeutet, dass der Port nicht näher spezifiziert ist.</p>
Originale Quell-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i></p> <p>Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
Original Quellport	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i>, NAT-Methode = <i>symmetrisch</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i></p> <p>Geben Sie den Quellport der ursprünglichen Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> bedeutet, dass der Port nicht näher spezifiziert ist.</p>
Quell-Port/Bereich	<p>Nur für Art des Datenverkehrs = <i>exklusiv (ohne NAT)</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP,</i></p>

Feld	Beschreibung
	<p><i>TCP/UDP</i></p> <p>Geben Sie den Quellport der ursprünglichen Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> bedeutet, dass der Port nicht näher spezifiziert ist.</p>
Ziel-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i> bzw. <i>exklusiv (ohne NAT)</i> und NAT-Methode = <i>symmetrisch</i></p> <p>Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
Ziel-Port/Bereich	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i>, NAT-Methode = <i>symmetrisch</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i> oder Art des Datenverkehrs = <i>exklusiv (ohne NAT)</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i></p> <p>Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der ursprünglichen Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> bedeutet, dass der Port nicht näher spezifiziert ist.</p>

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	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i></p> <p>Geben Sie diejenige Ziel-IP-Adresse ein, auf welche die ursprüngliche Ziel-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.</p>
Neuer Ziel-Port	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i></p> <p>Belassen Sie den Ziel-Port oder geben Sie denjenigen Ziel-Port ein, auf den der ursprüngliche Ziel-Port umgesetzt werden soll.</p> <p>Mit Auswahl von <i>Original</i> belassen Sie den ursprünglichen Ziel-Port. Wenn Sie <i>Original</i> deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Ziel-Port eingeben.</p>

Feld	Beschreibung
	Standardmäßig ist <i>Original</i> aktiv.
Neue Quell-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>ausgehend</i> (<i>Quell-NAT</i>) und NAT-Methode = <i>symmetrisch</i></p> <p>Geben Sie diejenige Quell-IP-Adresse ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.</p>
Neuer Quell-Port	<p>Nur für Art des Datenverkehrs = <i>ausgehend</i> (<i>Quell-NAT</i>) und NAT-Methode = <i>symmetrisch</i></p> <p>Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-Port ein, auf den der ursprüngliche Quell-Port umgesetzt werden soll.</p> <p>Mit Auswahl von <i>Original</i> belassen Sie den ursprünglichen Quell-Port. Wenn Sie <i>Original</i> deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Quell-Port eingeben. Standardmäßig ist <i>Original</i> aktiv.</p>

13.4 Lastverteilung

Zunehmender Datenverkehr über das Internet erfordert die Möglichkeit, Daten über unterschiedliche Schnittstellen senden zu können, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. IP-Lastverteilung ermöglicht die geregelte Verteilung von Datenverkehr innerhalb einer bestimmten Gruppe von Schnittstellen.

13.4.1 Lastverteilungsgruppen

Wenn Schnittstellen zu Gruppen zusammengefasst sind, wird der Datenverkehr innerhalb einer Gruppe nach folgenden Prinzipien aufgeteilt:

- Im Unterschied zu Multilink-PPP-basierten Lösungen funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.
- Session-based Load Balancing wird realisiert.
- Zusammenhängende (abhängige) Sessions werden immer über dieselbe Schnittstelle geroutet.
- Eine Distributionsentscheidung fällt nur bei ausgehenden Sessions.

Im Menü **Netzwerk->Lastverteilung->Lastverteilungsgruppen** wird eine Liste aller konfi-

gurierten Lastverteilungsgruppen angezeigt. Mit einem Klick auf das -Symbol neben einem Listeneintrag gelangen Sie zu einer Übersicht, in der die wichtigsten Parameter dieser Gruppe zusammengefasst sind.



Hinweis

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

13.4.1.1 Neu

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

Lastverteilungsgruppen Special Session Handling

Basisparameter			
Gruppenbeschreibung	<input type="text"/>		
Verteilungsrichtlinie	Sitzungs-Round-Robin ▼		
Verteilungsmodus	<input checked="" type="radio"/> Immer <input type="radio"/> Nur aktive Schnittstellen verwenden		
Schnittstellenauswahl für Verteilung			
Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung
<input type="button" value="Hinzufügen"/>			
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>			

Abb. 75: **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine beliebige Beschreibung der Schnittstellen-Gruppe ein.
Verteilungsrichtlinie	<p>Wählen Sie aus, auf welche Art der Datenverkehr auf die für die Gruppe konfigurierten Schnittstellen verteilt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Sitzungs-Round-Robin</i> (Standardwert): Eine neu hinzukommende Session wird je nach prozentualer Belegung der Schnittstellen mit Sessions einer der Gruppen-Schnittstellen

Feld	Beschreibung
	<p>zugewiesen. Die Anzahl der Sessions ist maßgeblich.</p> <ul style="list-style-type: none"> • <i>Lastabhängige Bandbreite</i>: Eine neu hinzukommende Session wird je nach Anteil der Schnittstellen an der Gesamtdatenrate einer der Gruppen-Schnittstellen zugewiesen. Maßgeblich ist die aktuelle Datenrate, wobei der Datenverkehr sowohl in Sende- als auch in Empfangsrichtung berücksichtigt wird.
Berücksichtigen	<p>Nur für Verteilungsrichtlinie = <i>Lastabhängige Bandbreite</i></p> <p>Wählen Sie aus, in welcher Richtung die aktuelle Datenrate berücksichtigt werden soll.</p> <p>Optionen:</p> <ul style="list-style-type: none"> • <i>Download</i>: Nur die Datenrate in Empfangsrichtung wird berücksichtigt. • <i>Upload</i>: Nur die Datenrate in Senderichtung wird berücksichtigt. <p>Standardmäßig sind die Optionen <i>Download</i> und <i>Upload</i> deaktiviert.</p>
Verteilungsmodus	<p>Wählen Sie aus, welchen Zustand die Schnittstellen der Gruppe haben dürfen, damit sie in die Lastverteilung einbezogen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Immer</i> (Standardwert): Auch Schnittstellen im Zustand ruhend werden einbezogen. • <i>Nur aktive Schnittstellen verwenden</i>: Es werden nur Schnittstellen im Zustand aktiv berücksichtigt.

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

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

The screenshot shows a configuration window for 'Lastverteilungsgruppen' with the following details:

- Header:** Lastverteilungsgruppen | Special Session Handling
- Basisparameter:**
 - Gruppenbeschreibung: [Empty text box]
 - Verteilungsrichtlinie: Sitzungs-Round-Robin (dropdown)
 - Schnittstelle: Keiner (dropdown)
 - Verteilungsverhältnis: 0 %
- Erweiterte Einstellungen:**
 - Routenselektor: Keiner (dropdown)
 - IP-Adresse zur Nachverfolgung: Keiner (dropdown)
- Buttons:** Übernehmen, Abbrechen

Abb. 76: Netzwerk->Lastverteilung->Lastverteilungsgruppen->Hinzufügen

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Zeigt die Beschreibung der Schnittstellen-Gruppe an.
Verteilungsrichtlinie	Zeigt die gewählte Art des Datenverkehrs an.

Felder im Menü Schnittstellenauswahl für Verteilung

Feld	Beschreibung
Schnittstelle	Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, die der Gruppe angehören sollen.
Verteilungsverhältnis	<p>Geben Sie an, welchen Prozentsatz des Datenverkehrs eine Schnittstelle übernehmen soll.</p> <p>Die Bedeutung unterscheidet sich je nach verwendetem Verteilungsverhältnis:</p> <ul style="list-style-type: none"> • Für <i>Sitzungs-Round-Robin</i> wird die Anzahl verteilter Sessions zugrunde gelegt. • Für <i>Lastabhängige Bandbreite</i> ist die Datenrate maßgeblich.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<p>Routenselektor</p>	<p>Der Parameter Routenselektor ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten Anwendungsfällen notwendig, um die vom Router verwalteten IP Sessions eindeutig je Loadbalancing-Gruppe bilanzieren zu können. Für die Anwendung des Parameters gelten folgende Regeln:</p> <ul style="list-style-type: none"> • Ist eine Schnittstelle nur einer Lastverteilungsgruppe zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig. • Ist eine Schnittstelle mehreren Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich. • Innerhalb einer Lastverteilungsgruppe muss der Routenselektor aller Schnittstelleneinträge identisch konfiguriert sein. <p>Wählen Sie die Ziel-IP-Adresse der gewünschten Route aus.</p> <p>Sie können unter allen Routen und allen erweiterten Routen wählen.</p>
<p>IP-Adresse zur Nachverfolgung</p>	<p>Mit dem Parameter IP-Adresse zur Nachverfolgung können Sie eine bestimmte Route überwachen lassen.</p> <p>Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die Konfiguration von Host-Überwachungseinträgen zwingend erforderlich. Konfiguriert werden kann dies im Menü Lokale Dienste->Überwachung->Hosts. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion Überwachung berücksichtigt werden. Über die Konfiguration der IP-Adresse zur Nachverfolgung im Menü Lastverteilung->>Last-</p>

Feld	Beschreibung
	<p>verteilungsgruppen->Erweiterte Einstellungen erfolgt die Verknüpfung zwischen der Lastverteilungsfunktion und der Host-Überwachungsfunktion. Der Lastverteilungsstatus der Schnittstelle wechselt nun in Abhängigkeit zum Status des zugewiesenen Host-Überwachungseintrages.</p> <p>Wählen Sie die IP-Adresse der Route, die überwacht werden soll.</p> <p>Sie können unter den IP-Adressen wählen, die Sie im Menü Lokale Dienste->Überwachung->Hosts->Neu unter Überwachte IP-Adresse eingegeben haben und die mit Hilfe des Feldes Auszuführende Aktion überwacht werden (Aktion = <i>überwachen</i>).</p>

13.4.2 Special Session Handling

Special Session Handling ermöglicht Ihnen einen Teil des Datenverkehrs auf Ihrem Gerät über eine bestimmte Schnittstelle zu leiten. Dieser Datenverkehr wird von der Funktion **Lastverteilung** ausgenommen.

Die Funktion **Special Session Handling** können Sie zum Beispiel beim Online Banking verwenden, um sicherzustellen, dass der HTTPS-Datenverkehr auf einen bestimmten Link übertragen wird. Da beim Online Banking geprüft wird, ob der gesamte Datenverkehr aus derselben Quelle stammt, würde ohne **Special Session Handling** die Datenübertragung bei Verwendung von **Lastverteilung** unter Umständen abgebrochen.

Im Menü **Netzwerk->Lastverteilung->Special Session Handling** wird eine Liste mit Einträgen angezeigt. Wenn Sie noch keine Einträge konfiguriert haben, ist die Liste leer.

Jeder Eintrag enthält u. a. Parameter, welche die Eigenschaften eines Datenpakets mehr oder weniger detailliert beschreiben. Das erste Datenpaket, auf das die hier konfigurierten Eigenschaften zutreffen, legt die Route für bestimmte nachfolgende Datenpakete fest.

Welche Datenpakete danach über diese Route geleitet werden, wird im Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu->Erweiterte Einstellungen** konfiguriert.

Wenn Sie zum Beispiel im Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu** den Parameter **Dienst** = `http (SSL)` wählen (und bei allen anderen Parametern die Standardwerte belassen), so legt das erste HTTPS-Paket die **Zieladresse** und den **Zielport** (d. h. Port 443 bei HTTPS) für später gesendete Datenpakete fest.

Wenn Sie unter **Unveränderliche Parameter** für die beide Parameter **Zieladresse** und

Zielport die Standardeinstellung *aktiviert* belassen, so werden die HTTPS-Pakete mit derselben Quell-IP-Adresse wie das erste HTTPS-Paket über Port 443 zur selben **Zieladresse** über dieselbe Schnittstelle wie das erste HTTPS-Paket geroutet.

13.4.2.1 Bearbeiten oder Neu

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

Lastverteilungsgruppen Special Session Handling

Basisparameter	
Admin-Status	<input checked="" type="checkbox"/> Aktiviert
Beschreibung	<input style="width: 100%;" type="text"/>
Dienst	Benutzerdefiniert ▾
Protokoll	nicht überprüfen ▾
Ziel-IP-Adresse/Netzmaske	Beliebig ▾
Ziel-Port/Bereich	-Alle- ▾ -1 bis -1
Quellschnittstelle	Keine ▾
Quell-IP-Adresse/Netzmaske	Beliebig ▾
Quell-Port/Bereich	-Alle- ▾ -1 bis -1
Special Handling Timer	900 Sekunden

Erweiterte Einstellungen

Unveränderliche Parameter	
	<input checked="" type="checkbox"/> Quell-IP-Adresse
	<input checked="" type="checkbox"/> Zieladresse
	<input checked="" type="checkbox"/> Zielport

OK
Abbrechen

Abb. 77: Netzwerk->Lastverteilung->Special Session Handling->Neu

Das Menü **Netzwerk->Lastverteilung->Special Session Handling->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<p>Wählen Sie aus, ob Special Session Handling aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.
Dienst	<p>Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>
Protokoll	Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
Ziel-IP-Adresse/Netzmaske	<p>Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	<p>Geben Sie, falls gewünscht, eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Zielport ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Ziel-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Ziel-Port-Bereich ein.

Feld	Beschreibung
Quellschnittstelle	Wählen Sie, falls gewünscht, die Quellschnittstelle Ihres Geräts aus.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port/Bereich	Geben Sie, falls gewünscht, eine Quell-Port-Nummer bzw. einen Bereich von Quell-Port-Nummern ein. Mögliche Werte: <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Quell-Port ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Quell-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Quell-Port-Bereich ein.
Special Handling Timer	Geben Sie ein, während welcher Zeitspanne die spezifizierten Datenpakete über den festgelegten Weg geroutet werden sollen. Der Standardwert ist <i>900</i> Sekunden.

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

Felder im Menü **Erweiterte Einstellungen**

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

Feld	Beschreibung
	<p>Belassen Sie die Voreinstellung <i>Aktiviert</i> bei einem oder bei beiden Parametern, so muss der Wert des jeweiligen Parameters bei den später gesendeten Datenpaketen derselbe sein wie beim ersten Datenpaket.</p> <p>Sie können, falls gewünscht, einen oder beide Parameter deaktivieren.</p> <p>Der Parameter Quell-IP-Adresse muss bei später gesendeten Datenpaketen immer denselben Wert haben wie beim ersten Datenpaket. Er kann daher nicht deaktiviert werden.</p>

13.5 QoS

QoS (Quality of Service) ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt und Bandbreite für diese reserviert werden. Vor allem für zeitkritische Anwendungen wie z. B. Voice over IP ist das von Vorteil.

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen
- Daten klassifizieren
- Daten priorisieren.

13.5.1 QoS-Filter

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

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

13.5.1.1 Neu

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

QoS-Filter QoS-Klassifizierung QoS-Schnittstellen/Richtlinien

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	Benutzerdefiniert ▾
Protokoll	Beliebig ▾
Ziel-IP-Adresse/Netzmaske	Beliebig ▾
Quell-IP-Adresse/Netzmaske	Beliebig ▾
DSCP/TOS-Filter (Layer 3)	Nicht beachten ▾
COS-Filter (802.1p/Layer 2)	Nicht beachten ▾

Abb. 78: 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	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	Nur für Protokoll = <i>ICMP</i>

Feld	Beschreibung
	<p>Wählen Sie einen Typ aus.</p> <p>Mögliche Werte: <i>Beliebig, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply</i></p> <p>Siehe RFC 792.</p> <p>Standardwert ist <i>Beliebig</i>.</p>
Verbindungsstatus	<p>Bei Protokoll = <i>TCP</i> können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.
Ziel-IP-Adresse/Netzmaske	<p>Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p>
Ziel-Port/Bereich	<p>Nur für Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Ziel-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Ziel-Port-Bereich ein.
Quell-IP-Adresse/Netzmaske	<p>Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p>
Quell-Port/Bereich	<p>Nur für Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie eine Quell-Port-Nummer bzw. einen Bereich von Quell-Port-Nummern ein.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Quell-Port ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Quell-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Quell-Port-Bereich ein.
<p>DSCP/TOS-Filter (Layer 3)</p>	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
<p>COS-Filter (802.1p/Layer 2)</p>	<p>Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS).</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Standardwert ist <i>Nicht beachten</i>.</p>

13.5.2 QoS-Klassifizierung

Im Menü **Netzwerk->QoS->QoS-Klassifizierung** wird der Datenverkehr klassifiziert, d. h. der Datenverkehr wird mittels Klassen-ID verschiedenen Klassen zugeordnet. Sie erstellen dazu Klassenpläne zur Klassifizierung von IP-Paketen anhand zuvor definierter IP-Filter. Jeder Klassenplan wird über seinen ersten Filter mindestens einer Schnittstelle zugeordnet.

13.5.2.1 Neu

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

Abb. 79: **Netzwerk->QoS->QoS-Klassifizierung->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Klassenplan	<p>Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an. <i><Name des Klassenplans></i>: Zeigt einen bereits angeleg-

Feld	Beschreibung
	ten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	Nur für Klassenplan = <i>Neu</i> . 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: <ul style="list-style-type: none">• <i>Eingehend</i>: Eingehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet.• <i>Ausgehend</i> (Standardwert): Ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet.• <i>Beide</i>: 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 <i>Aktiviert</i> 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
	<p>weist.</p> <div data-bbox="544 266 1316 457" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Hinweis</p> <p>Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.)</p> </div> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 254.</p>
<p>Setze DSCP/TOS Wert (Layer 3)</p>	<p>Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (Klassen-ID) setzen bzw. ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erhalten</i> (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
<p>Setze COS Wert (802.1p/Layer 2)</p>	<p>Hier können Sie die Serviceklasse (Layer-2-Priorität) im VLAN Ethernet Header der IP-Pakete in Abhängigkeit zur definierten Klasse (Klassen-ID) setzen/ändern.</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Standardwert ist <i>Erhalten</i>.</p>

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

13.5.3 QoS-Schnittstellen/Richtlinien

Im Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien** legen Sie die Priorisierung der Daten fest.



Hinweis

Daten können nur ausgehend priorisiert werden.

Pakete der High-Priority-Klasse haben immer Vorrang vor Daten mit Klassen-ID 1 - 254.

Es ist möglich, jeder Queue und somit jeder Datenklasse einen bestimmten Anteil an der Gesamtbandbreite der Schnittstelle zuzuweisen bzw. zu garantieren. Darüber hinaus können Sie die Übertragung von Sprachdaten (Real-Time-Daten) optimieren.

Abhängig von der jeweiligen Schnittstelle wird für jede Klasse automatisch eine Queue (Warteschlange) angelegt, jedoch nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr. Den automatisch angelegten Queues wird hierbei eine Priorität zugeordnet. Der Wert der Priorität ist dabei gleich dem Wert der Klassen-ID. Sie können diese standardmäßig gesetzte Priorität einer Queue ändern. Wenn Sie neue Queues hinzufügen, können Sie über die Klassen-ID auch Klassen anderer Klassenpläne verwenden.

13.5.3.1 Neu

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

QoS-Filter
QoS-Klassifizierung
QoS-Schnittstellen/Richtlinien

Basisparameter													
Schnittstelle	en1-0 ▼												
Priorisierungsalgorithmus	Priority Queueing ▼												
Traffic Shaping	<input type="checkbox"/> Aktiviert												
Queues/Richtlinien	<p>Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag mit der niedrigsten Priorität erstellt.</p> <table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr> <th style="width: 40%;">Beschreibung</th> <th style="width: 10%;">Typ</th> <th style="width: 10%;">Klassen-ID</th> <th style="width: 10%;">Priorität</th> <th style="width: 10%;">Bandbreite für Traffic Shaping</th> <th style="width: 10%;"></th> </tr> </thead> <tbody> <tr> <td colspan="6" style="text-align: center; padding: 5px;"> Hinzufügen </td> </tr> </tbody> </table>	Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping		Hinzufügen					
Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping									
Hinzufügen													

OK
Abbrechen

Abb. 80: 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	<p>Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausgewählten Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Priority Queueing</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. • <i>Weighted Round Robin</i>: 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. • <i>Weighted Fair Queueing</i>: 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. • <i>Deaktiviert</i> (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	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate in Senderichtung.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upload-Geschwindigkeit	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie für die Queue eine maximale Datenrate in kBits pro Sekunde in Senderichtung ein.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000000</i>.</p> <p>Der Standardwert ist <i>0</i>, d.h. es erfolgt keine Begrenzung, die Queue kann die maximale Bandbreite belegen.</p>
Größe des Protokoll-Headers unterhalb Layer 3	<p>Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Benutzerdefiniert</i>: Wert in Byte; Mögliche Werte sind <i>0</i> bis <i>100</i>. • <i>Undefiniert (Protocol Header Offset=0)</i> (Standardwert) <p>Nur für Ethernet-Schnittstellen auswählbar</p> <ul style="list-style-type: none"> • <i>Ethernet</i> • <i>Ethernet und VLAN</i> • <i>PPP over Ethernet</i> • <i>PPPoE und VLAN</i> <p>Nur für IPSec-Schnittstellen auswählbar:</p> <ul style="list-style-type: none"> • <i>IPSec über Ethernet</i> • <i>IPSec über Ethernet und VLAN</i> • <i>IPSec via PPP over Ethernet</i> • <i>IPSec via PPPoE und VLAN</i>
Verschlüsselungsme-	<p>Nur wenn als Schnittstelle ein IPSec Peer gewählt ist, Traffic</p>

Feld	Beschreibung
thode	<p>Shaping <i>Aktiviert</i> ist und die Größe des Protokoll-Headers unterhalb Layer 3 nicht <i>Undefiniert (Protocol Header Offset=0)</i> ist.</p> <p>Wählen Sie die Verschlüsselungsmethode, die für die IPSec-Verbindung genutzt wird. Der Verschlüsselungsalgorithmus bestimmt die Länge der Blockchiffre, die bei der Bandbreitenkalkulation berücksichtigt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DES, 3DES, Blowfish, Cast</i> - (Cipher-Blockgröße = 64 Bit) • <i>AES128, AES192, AES256, Twofish</i> - (Cipher-Blockgröße = 128 Bit)
Real Time Jitter Control	<p>Nur für Traffic Shaping = aktiviert</p> <p>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.</p> <p>Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s).</p> <p>Aktivieren oder deaktivieren Sie Real Time Jitter Control.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Kontrollmodus	<p>Nur für Real Time Jitter Control = aktiviert.</p> <p>Wählen Sie den Modus für die Optimierung der Sprachübertragung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream erkannt wurde. • <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachda-

Feld	Beschreibung
	<p>ten wird nicht durchgeführt.</p> <ul style="list-style-type: none"> • <i>Nur kontrollierte RTP-Streams</i>: 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. • <i>Immer</i>: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.
Queues/Richtlinien	<p>Konfigurieren Sie die gewünschten QoS-Queues.</p> <p>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).</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu. Das Menü Queue/Richtlinie bearbeiten öffnet sich.</p> <p>Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag DEFAULT mit der niedrigsten Priorität 255 erstellt.</p>

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	<p>Wählen Sie den Typ für die Priorisierung der Queue aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Klassenbasiert</i> (Standardwert): Queue für "normal"-klassifizierte Daten. • <i>Hohe Priorität</i>: Queue für "high-priority"-klassifizierte Daten. • <i>Standard</i>: Queue für Daten, die nicht klassifiziert wurden

Feld	Beschreibung
	bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	<p>Nur für Priorisierungsqueue = <i>Klassenbasiert</i></p> <p>Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll.</p> <p>Dazu muss vorher im Menü Netzwerk->QoS->QoS-Klassifizierung mindestens eine Klassen-ID vergeben worden sein.</p>
Priorität	<p>Nur für Priorisierungsqueue = <i>Klassenbasiert</i></p> <p>Wählen Sie die Priorität der Queue. Mögliche Werte sind <i>1 (hohe Priorität) bis 254 (niedrige Priorität)</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
Gewichtung	<p>Nur für Priorisierungsalgorithmus = <i>Weighted Round Robin oder Weighted Fair Queueing</i></p> <p>Wählen Sie die Gewichtung der Queue. Mögliche Werte sind <i>1 bis 254</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
RTT-Modus (Realtime-Traffic-Modus)	<p>Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>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.</p> <p>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.</p>
Traffic Shaping	Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung.

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

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Dropping-Algorithmus	<p>Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Tail Drop</i> (Standardwert): Das neu hinzugekommene Paket wird verworfen. • <i>Head Drop</i>: Das älteste Paket in der Queue wird verworfen. • <i>Random Drop</i>: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Vermeidung von Datenstau (RED)	<p>Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen.</p> <p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Min. Queue-Größe	<p>Geben Sie die minimale Größe der Queue in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 0.</p>
Max. Queue-Größe	<p>Geben Sie die maximale Größe der Queue in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 16384.</p>

13.6 Zugriffsregeln

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

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

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

Möchten z.B. Standorte, deren LANs über ein **bintec**-Gateway miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access-Listen ein effektives Mittel.

Access-Filter auf dem Gateway basieren auf der Kombination von Filtern und Aktionen zu Filterregeln (= rules) und der Verknüpfung dieser Regeln zu sogenannten Regelketten. Sie wirken auf die eingehenden Datenpakete und können so bestimmten Daten den Zutritt zum Gateway erlauben oder verbieten.

Ein Filter beschreibt einen bestimmten Teil des IP-Datenverkehrs, basierend auf Quell- und/oder Ziel-IP-Adresse, Netzmaske, Protokoll, Quell- und/ oder Ziel-Port.

Mit den Regeln, die Sie in Access Lists organisieren, teilen Sie dem Gateway mit, wie es mit gefilterten Datenpaketen umgehen soll – ob es sie annehmen oder abweisen soll. Sie können auch mehrere Regeln definieren, die Sie in Form einer Kette organisieren und ihnen damit eine bestimmte Reihenfolge geben.

Für die Definition von Regeln bzw. Regelketten gibt es verschiedene Ansätze:

Nehme alle Pakete an, die nicht explizit verboten sind, d. h.:

- Weise alle Pakete ab, auf die Filter 1 zutrifft.
- Weise alle Pakete ab, auf die Filter 2 zutrifft.
- ...
- Lass den Rest durch.

oder

Nehme nur Pakete an, die explizit erlaubt sind, d. h.:

- Nehme alle Pakete an, auf die Filter 1 zutrifft.
- Nehme alle Pakete an, auf die Filter 2 zutrifft.
- ...
- Weise den Rest ab.

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

Es können mehrere getrennte Regelketten angelegt werden. Eine gemeinsame Nutzung von Filtern in verschiedenen Regelketten ist dabei möglich.

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.



Achtung

Achten Sie darauf, dass Sie sich beim Konfigurieren der Filter nicht selbst aussperren:

Greifen Sie zur Filter-Konfiguration möglichst über die serielle Konsolen-Schnittstelle oder mit ISDN-Login auf Ihr Gateway zu.

13.6.1 Zugrifffilter

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->Zugriffsfiler** wird eine Liste aller Access-Filter angezeigt.



Abb. 81: **Netzwerk->Zugriffsregeln->Zugriffsfiler**

13.6.1.1 Bearbeiten oder Neu

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

Zugriffsfilter Regelketten Schnittstellenzuweisung

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	Benutzerdefiniert ▼
Protokoll	Bellebig ▼
Ziel-IP-Adresse/Netzmaske	Bellebig ▼
Quell-IP-Adresse/Netzmaske	Bellebig ▼
DSCP/TOS-Filter (Layer 3)	Nicht beachten ▼
COS-Filter (802.1p/Layer 2)	Nicht beachten ▼

OK Abbrechen

Abb. 82: 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	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>

Feld	Beschreibung
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	<p>Nur bei Protokoll = <i>ICMP</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>Echo reply</i> • <i>Destination unreachable</i> • <i>Source quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time exceeded</i> • <i>Timestamp</i> • <i>Timestamp reply</i> • <p>Standardwert ist <i>Beliebig</i>.</p> <p>Siehe RFC 792.</p>
Verbindungsstatus	<p>Nur bei Protokoll = <i>TCP</i></p> <p>Sie können ein Filter definieren, das den Status von TCP-Verbindung berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete. • <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden.
Ziel-IP-Adresse/Netzmaske	<p>Definieren Sie die Ziel-IP-Adresse und die Netzmaske der Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert)

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	<p>Nur bei Protokoll = <i>TCP, UDP</i></p> <p>Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein, auf den das Filter passt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Das Filter gilt für alle Port-Nummern • <i>Port angeben</i>: Ermöglicht Eingabe einer Port-Nummer. • <i>Portbereich angeben</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern.
Quell-IP-Adresse/Netzmaske	<p>Geben Sie die Quell-IP-Adresse und die Netzmaske der Datenpakete ein.</p>
Quell-Port/Bereich	<p>Nur bei Protokoll = <i>TCP, UDP</i></p> <p>Geben Sie die Quell-Port-Nummer bzw. den Bereich von Quell-Port-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Das Filter gilt für alle Port-Nummern. • <i>Port angeben</i>: Ermöglicht Eingabe einer Port-Nummer. • <i>Portbereich angeben</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern.
DSCP/TOS-Filter (Layer 3)	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	<p>Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS).</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Standardwert ist <i>Nicht beachten</i>.</p>

13.6.2 Regelketten

Im Menü **Regelketten** werden Regeln für IP-Filter konfiguriert. Diese können separat angelegt oder in Regelketten eingebunden werden.

Im Menü **Netzwerk->Zugriffsregeln->Regelketten** werden alle angelegten Filterregeln aufgelistet.



Abb. 83: **Netzwerk->Zugriffsregeln->Regelketten**

13.6.2.1 Bearbeiten oder Neu

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

[Zugriffsfilter](#) | [Regelketten](#) | [Schnittstellenzuweisung](#)

Basisparameter	
Regelkette	Neu ▾
Beschreibung	<input type="text"/>
Zugriffsfilter	Eines auswählen ▾
Aktion	Zulassen, wenn Filter passt ▾

Abb. 84: Netzwerk->Zugriffsregeln->Regelketten->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Regelkette	<p>Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an. • <i><Name der Regelkette></i>: Wählen Sie eine bereits angelegte Regelkette aus und fügen ihr somit eine weitere Regel hinzu.
Beschreibung	Geben Sie die Bezeichnung der Regelkette ein.
Zugriffsfilter	<p>Wählen Sie ein IP-Filter aus.</p> <p>Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll.</p> <p>Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll.</p>
Aktion	<p>Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zulassen, wenn Filter passt</i> (Standardwert): Paket annehmen, wenn das Filter passt. • <i>Zulassen, wenn Filter nicht passt</i>: Paket anneh-

Feld	Beschreibung
	<p>men, wenn das Filter nicht passt.</p> <ul style="list-style-type: none"> • <i>Verweigern, wenn Filter passt</i>: Paket abweisen, wenn das Filter passt. • <i>Verweigern, wenn Filter nicht passt</i>: Paket abweisen, wenn das Filter nicht passt. • <i>Nicht beachten</i>: 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 *übereine* andere Regel dieser Regelkette verschoben wird.

13.6.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten den einzelnen Schnittstellen zugeordnet und das Verhalten des Gateways beim Abweisen von IP-Paketen festgelegt.

Im Menü **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.



Abb. 85: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung**

13.6.3.1 Bearbeiten oder Neu

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

Zugriffsfiler Regelketten Schnittstellenzuweisung

Basisparameter	
Schnittstelle	Eine auswählen ▾
Regelkette	Eine auswählen ▾
Verwerfen ohne Rückmeldung	<input checked="" type="checkbox"/> Aktiviert
Berichtsmethode	Info ▾

OK Abbrechen

Abb. 86: 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. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiviert.
Berichtsmethode	Legen Sie fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Kein Bericht</i>: Keine Syslog-Meldung. • <i>Info</i> (Standardwert): Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IP-Adresse und Quell-Port-Nummer wird generiert. • <i>Dump</i>: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Paketes wird generiert.

13.7 Drop-In

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

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

13.7.1 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.

13.7.1.1 Neu

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

Drop-In-Gruppen

Basisparameter	
Gruppenbeschreibung	<input type="text"/>
Modus	Transparent <input type="button" value="v"/>
Netzwerkconfiguration	Statisch <input type="button" value="v"/>
Netzwerkadresse	<input type="text"/>
Netzmaske	<input type="text"/>
Lokale IP-Adresse	<input type="text"/>
ARP Lifetime	3600 Sekunden
DNS-Zuweisung über DHCP	Unverändert <input type="button" value="v"/>
Vom NAT ausnehmen (DMZ)	<input type="checkbox"/> Aktiviert
Schnittstellenauswahl	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> Schnittstelle <input style="width: 50px; height: 15px;" type="text"/> </div> <input type="button" value="Hinzufügen"/>

Abb. 87: **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: <ul style="list-style-type: none"> • <i>Transparent</i> (Standardwert): ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet. • <i>Proxy</i>: ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden mit der MAC-Adresse der entsprechenden Schnittstelle weitergeleitet.
Netzwerkconfiguration	Wählen Sie aus, auf welche Weise dem Drop-In -Netzwerk eine IP-Adresse/Netzmaske zugewiesen wird. Mögliche Werte: <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert) • <i>DHCP</i>
Netzwerkadresse	Nur für Netzwerkconfiguration = <i>Statisch</i> Geben Sie die Netzwerkadresse des Drop-In -Netzwerks ein.
Netzmaske	Nur für Netzwerkconfiguration = <i>Statisch</i> Geben Sie die zugehörige Netzmaske ein.
Lokale IP-Adresse	Nur für Netzwerkconfiguration = <i>Statisch</i> Geben Sie die lokale IP-Adresse ein. Diese IP-Adresse muss für alle Ethernet-Ports eines Netzwerks identisch sein.
DHCP Client an Schnittstelle	Nur für Netzwerkconfiguration = <i>DHCP</i> Hier können Sie eine Ethernet-Schnittstelle Ihres Routers wählen, die als DHCP-Client agieren soll. Diese Einstellung benötigen Sie zum Beispiel, wenn der Router

Feld	Beschreibung
	<p>Ihres Providers als DHCP-Server dient.</p> <p>Sie können unter den Schnittstellen wählen, welche Ihr Gerät zur Verfügung stellt, die Schnittstelle muss jedoch Mitglied der Drop-In-Gruppe sein.</p>
ARP Lifetime	<p>Legt die Zeitspanne fest, während derer ARP-Einträge im Cache gehalten werden.</p> <p>Der Standardwert ist <i>3600</i> Sekunden.</p>
DNS-Zuweisung über DHCP	<p>Das Gateway kann DHCP-Pakete, die die Drop-In-Gruppe durchlaufen, modifizieren und sich selbst als angebotenen DNS-Server eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Unverändert</i> (Standardwert) • <i>Eigene IP-Adresse</i>
Vom NAT ausnehmen (DMZ)	<p>Hier können Sie Datenverkehr von NAT ausnehmen.</p> <p>Verwenden Sie diese Funktion, um zum Beispiel die Erreichbarkeit bestimmter Web-Server in einer DMZ sicherzustellen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Schnittstellenauswahl	<p>Wählen Sie alle Ports aus, die in der Drop-In-Gruppe (im Netzwerk) enthalten sein sollen.</p> <p>Fügen Sie mit Hinzufügen weitere Einträge hinzu.</p>

Kapitel 14 Routing-Protokolle

14.1 RIP

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

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

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

14.1.1 RIP-Schnittstellen

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

RIP-Schnittstellen RIP-Filter RIP-Optionen

Nr.	Schnittstelle	Version in Senderichtung	Version in Empfangsrichtung	Routenankündigung	
1	en1-4	Keine	Keine	Nur aktiv	
2	en1-0	Keine	Keine	Nur aktiv	

Seite: 1, Objekte: 1 - 2

Abb. 88: **Routing-Protokolle -> RIP -> RIP-Schnittstellen**

14.1.1.1 Bearbeiten

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

RIP-Schnittstellen RIP-Filter RIP-Optionen

RIP-Parameter für: en1-4

Version in Senderichtung	Keine 
Version in Empfangsrichtung	Keine 
Routenankündigung	Nur aktiv 

OK Abbrechen

Abb. 89: Routing-Protokolle->RIP->RIP-Schnittstellen-> 

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

Felder im Menü RIP-Parameter für

Feld	Beschreibung
Version in Senderichtung	<p>Entscheiden Sie, ob über RIP-Routen propagiert werden sollen, und wenn ja, wählen Sie die RIP-Version für das Senden von RIP-Paketen über die Schnittstelle in Senderichtung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): RIP ist nicht aktiv. • <i>RIP V1</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • <i>RIP V2</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • <i>RIP V1/V2</i>: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • <i>RIP V2 Multicast</i>: Ermöglicht das Senden von RIP-V2-Nachrichten über die Multicast-Adresse 224.0.0.9. • <i>RIP V1 Triggered</i>: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • <i>RIP V2 Triggered</i>: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet

Feld	Beschreibung
	(Triggered RIP).
Version in Empfangsrichtung	<p>Entscheiden Sie, ob über RIP Routen importiert werden sollen und wenn ja, wählen Sie die RIP-Version für das Empfangen von RIP-Paketen über die Schnittstelle in Empfangsrichtung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): RIP ist nicht aktiv. • <i>RIP V1</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • <i>RIP V2</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • <i>RIP V1/V2</i>: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • <i>RIP V1 Triggered</i>: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • <i>RIP V2 Triggered</i>: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP).
Routenankündigung	<p>Wählen Sie aus, wann ggf. aktivierte Routing-Protokolle (z. B. RIP) die für diese Schnittstelle definierten IP-Routen propagieren sollen.</p> <p>Beachten Sie: Diese Einstellung hat keinen Einfluss auf die oben erwähnte Schnittstellen-spezifische RIP-Konfiguration.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv oder Ruhend</i> (nicht für LAN-Schnittstellen, Schnittstellen im Bridge-Modus und Schnittstellen für Standleitungen): Routen werden propagiert, wenn der Status der Schnittstelle auf aktiv oder bereit steht. • <i>Nur aktiv</i> (Standardwert): Routen werden nur propagiert, wenn der Status der Schnittstelle auf aktiv steht. • <i>Immer</i>: Routen werden immer propagiert unabhängig vom Betriebsstatus.

14.1.2 RIP-Filter

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

Hierbei können Sie nach folgenden Strategien vorgehen:

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

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

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

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



Abb. 90: **Routing-Protokolle->RIP->RIP-Filter**

Mit der Schaltfläche  können Sie vor dem Listeneintrag ein weiteres Filter einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen eines neuen Filters.

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

14.1.2.1 Neu

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

RIP-Schnittstellen RIP-Filter RIP-Optionen

Basisparameter	
Schnittstelle	Keine ▾
IP-Adresse/Netzmaske	<input type="text"/> / <input type="text"/>
Richtung	<input checked="" type="radio"/> Importieren <input type="radio"/> Exportieren
Metrik-Offset für Aktive Schnittstellen	0 ▾
Metrik-Offset für Inaktive Schnittstellen	0 ▾

OK Abbrechen

Abb. 91: Routing-Protokolle->RIP->RIP-Filter->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie aus, für welche Schnittstelle die zu konfigurierende Regel gilt.
IP-Adresse/Netzmaske	<p>Geben Sie die IP-Adresse und Netzmaske ein, auf welche die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen.</p> <p>Die Regeln für eingehende und ausgehende RIP-Pakete (Importieren oder Exportieren) müssen für dieselbe IP-Adresse getrennt konfiguriert werden.</p> <p>Sie können einzelne Host-Adressen ebenso angeben wie Netz-adressen.</p>
Richtung	<p>Wählen Sie aus, ob das Filter für das Exportieren oder das Im-portieren von Routen gilt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Importieren</i> (Standardwert) • <i>Exportieren</i>
Metrik-Offset für Aktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Ak-tiv" ist. Beim Export wird der Wert der exportierten Metrik hinzu-gefügt, wenn der Status der Schnittstelle "Aktiv" ist.

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

14.1.3 RIP-Optionen

RIP-Schnittstellen RIP-Filter **RIP-Optionen**

Globale RIP-Parameter	
RIP-UDP-Port	520
Standardmäßige Routenverteilung	<input checked="" type="checkbox"/> Aktiviert
Poisoned Reverse	<input type="checkbox"/> Aktiviert
RFC 2453-Variabler Timer	<input checked="" type="checkbox"/> Aktiviert
RFC 2091-Variabler Timer	<input type="checkbox"/> Aktiviert
Timer für RIP V2 (RFC 2453)	
Aktualisierungstimer	30 Sekunden
Routentimeout	180 Sekunden
Garbage Collection Timer	120 Sekunden

OK Abbrechen

Abb. 92: Routing-Protokolle->RIP->RIP-Optionen

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

Felder im Menü Globale RIP-Parameter

Feld	Beschreibung
RIP-UDP-Port	Die Einstellungsmöglichkeit des UDP-Ports, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, dass Ihr Gerät auf einem Port sendet und lauscht, den keine weiteren Geräte benutzen. Der Stan-

Feld	Beschreibung
	<p>Standardwert <i>520</i> sollte eingestellt bleiben.</p>
<p>Standardmäßige Routenverteilung</p>	<p>Wählen Sie aus, ob die Standard-Route Ihres Geräts über RIP-Updates propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>Poisoned Reverse</p>	<p>Wählen Sie das Verfahren zur Verhinderung von Routing-Schleifen.</p> <p>Bei Standard RIP werden die gelernten Routen über alle Schnittstellen mit aktiviertem RIP SENDEN propagiert. Bei Poisoned Reverse propagiert Ihr Gerät jedoch über die Schnittstelle, über die es die Routen gelernt hat, diese mit der Metrik (Next Hop Count) 16 (= "Netz ist nicht erreichbar").</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>RFC 2453-Variabler Timer</p>	<p>Wählen Sie aus, ob für die in RFC 2453 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für RIP V2 (RFC 2453) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Wenn Sie die Funktion deaktivieren, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.</p>
<p>RFC 2091-Variabler Timer</p>	<p>Wählen Sie aus, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für Triggered RIP (RFC 2091) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion nicht aktiv ist, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.</p>

Felder im Menü Timer für RIP V2 (RFC 2453)

Feld	Beschreibung
Aktualisierungstimer	<p>Nur für RFC 2453-Variabler Timer = <i>Aktiviert</i></p> <p>Nach Ablauf dieses Zeitraums wird eine RIP-Aktualisierung gesendet.</p> <p>Der Standardwert ist <i>30</i> (Sekunden).</p>
Routentimeout	<p>Nur für RFC 2453-Variabler Timer = <i>Aktiviert</i></p> <p>Nach der letzten Aktualisierung einer Route wird der Routentimeout aktiv.</p> <p>Nach dessen Ablauf wird die Route deaktiviert und der Garbage Collection Timer gestartet.</p> <p>Der Standardwert ist <i>180</i> (Sekunden).</p>
Garbage Collection Timer	<p>Nur für RFC 2453-Variabler Timer = <i>Aktiviert</i></p> <p>Der Garbage Collection Timer wird gestartet, sobald der Routentimeout abgelaufen ist.</p> <p>Nach Ablauf dieses Zeitraums wird die ungültige Route aus der IPROUTETABLE gelöscht, sofern keine Aktualisierung für die Route erfolgt.</p> <p>Der Standardwert ist <i>120</i> (Sekunden).</p>

Felder im Menü Timer für Triggered RIP (RFC 2091)

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

Feld	Beschreibung
	Der Standardwert ist 5 (in Sekunden).

14.2 OSPF

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

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

- Verringerte Netzwerklast: Nach einer kurzen Initialisierungsphase werden Routing Informationen nicht wie mit RIP periodisch übertragen, sondern nur geänderte Routing Informationen.
- Authentifizierung: Zur Erhöhung der Sicherheit beim Austausch von Routing Informationen kann eine Gateway-Authentifizierung konfiguriert werden.
- Routing Traffic Kontrolle: Um den Traffic, der durch Austausch von Routing Informationen entsteht, zu begrenzen, können Gateways zu Areas zusammengefasst werden.
- Verbindungskosten: Im Unterschied zu RIP wird für die Kalkulation der Verbindungskosten nicht die Anzahl der Next Hops berücksichtigt, sondern die Bandbreite des jeweiligen Transportmediums.
- Keine Einschränkung der Hop-Anzahl: Die Einschränkung der maximalen Hop-Anzahl 16 bei RIP besteht für OSPF nicht.

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

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

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

Man unterscheidet vier Arten von Link State Paketen: Router Links geben den Status der

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

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

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

Der Verwendungszweck von Virtuellen Links ist die Anbindung von Areas, bei denen keine physikalische Anbindung an den Backbone möglich ist und das Aufrechterhalten der Verbindung des Backbone im Falle eines Ausfalls der 0.0.0.0 Area.

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

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

14.2.1 Bereiche

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

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

Abb. 93: Routing-Protokolle->OSPF->Bereiche

14.2.1.1 Bearbeiten oder Neu

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

Abb. 94: Routing-Protokolle->OSPF->Bereiche->Neu

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
Routen	<p>Definieren Sie, ob Summary LSAs (vom Area Border Gateway generierte Routing-Informationen) in die Stub Area gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert): Aktiviert den Import. • <i>Deaktiviert</i>: Deaktiviert den Import.
Standardroute für Bereich eintragen (nur ABR)	<p>Nur für Externe Routen importieren = <i>Deaktiviert</i></p> <p>Wählen Sie aus, ob das Area Border Gateway keine LSAs in die Stub Area senden, sondern nur eine Default Route propagieren soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiviert.</p>

Felder im Menü Route Aggregation

Feld	Beschreibung
IP-Adresse	<p>Definieren Sie den OSPF-Bereich.</p> <ul style="list-style-type: none"> • IP-Adresse: Geben Sie hier die IP-Adresse des Bereichs ein, der zusammengefasst werden soll. • Netzmaske: Geben Sie hier die Netzmaske ein. • Ankündigen: Subnetze, die zu Bereichen zusammengefasst sind, lösen entweder das Propagieren des angegebenen Verbunds aus (<i>Ja</i>, Standardwert), oder führen dazu, dass das Subnetz gar nicht außerhalb des Bereichs propagiert wird (<i>Nein</i>), d.h. weder die eigentlichen Subnetze noch das zusammengefasste Gesamtnetz werden propagiert. <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p>

14.2.2 Schnittstellen

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

Bereiche Schnittstellen Globale Einstellungen										
Ansicht	20	pro Seite	<<	>>	Filtern in	Keiner	>	gleich	>	Los
Schnittstelle	Bereichs-ID	IP-Adresse	Admin-Status	Status	Metrik					
en1-4	n/v	n/v	Passiv	n/v	n/v					
en1-0	n/v	n/v	Passiv	n/v	n/v					
Seite: 1, Objekte: 1 - 2										

Abb. 95: Routing-Protokolle->OSPF->Schnittstellen



Achtung

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

14.2.2.1 Bearbeiten

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

Bereiche Schnittstellen Globale Einstellungen	
OSPF-Schnittstellenkonfiguration	
Admin-Status	Passiv
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 96: Routing-Protokolle->OSPF->Schnittstellen->

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

Felder im Menü OSPF-Schnittstellenkonfiguration

Feld	Beschreibung
Admin-Status	Der Status einer OSPF-Schnittstelle definiert, ob über die Schnittstelle Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden. Wenn OSPF noch nicht aktiviert wurde, wird nur das Admin-Status-Feld angezeigt (in diesem Fall sind Änderungen irrelevant).

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d.h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Passiv</i>: OSPF ist nicht für diese Schnittstelle aktiviert, d.h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing-Informationen berücksichtigt und über aktive Schnittstelle propagiert. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle komplett deaktiviert.
Bereichs-ID	<p>Wählen Sie die ID des Bereichs aus, dem diese Schnittstelle zugeordnet werden soll.</p> <p>Wenn Ihre Schnittstelle nicht nur der Backbone Area 0.0.0.0 zugewiesen werden sollen, müssen Sie im Menü Routing-Protokolle->OSPF->Bereiche zunächst OSPF-Bereiche definieren.</p>
Metrikbestimmung	<p>Legen Sie fest, wie die Metrik dieser Schnittstelle berechnet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto (Schnittstellengeschwindigkeit)</i> (Standardwert): Die Metrik wird anhand der Geschwindigkeit der Schnittstelle automatisch festgelegt. • <i>Fest eingestellt</i>: Geben Sie einen festen Wert in Metrik (Direkte Routen) ein.
Metrik (Direkte Routen)	<p>Geben Sie den Basismetrikwert an. Die tatsächlich für eine Route verwendete Metrik beruht auf einem Base Metric Value, der sich aus der Bandbreite der Schnittstelle errechnet: $BMV = 100.000.000 / \text{Bandbreite in bps}$. Für Metrikbestimmung Auto (Schnittstellengeschwindigkeit) wird hier der automatisch ermittelte Wert angezeigt und kann nicht verändert werden.</p> <p>Der Basismetrikwert ist für Bandbreiten $\geq 100.000.000$ bps immer <i>1</i>. Der Basismetrikwert von Gigabit-Schnittstellen und</p>

Feld	Beschreibung
	100-MBit-Schnittstellen ist somit identisch. Um dies zu ändern müssen Sie einen festen Wert in Metrikbestimmung einstellen.
Authentifizierungstyp	<p>Wählen Sie die Art der Authentifizierung aus, die angewendet wird, wenn OSPF-Pakete über diese OSPF-Schnittstelle verschickt (oder eingehende geprüft) werden. Diese legt fest, wie der Schlüssel im Feld Schlüssel zur Authentisierung verwendet wird.</p> <p>Standardmäßig ist der Wert auf <i>Keiner</i> gesetzt. Bei <i>Klartext</i> wird der Schlüssel als Textfolge in jedem Paket verschickt. Bei <i>MD5</i> wird der Schlüssel verwendet, um einen Hash zu erstellen, der in jedem Paket mitgeschickt wird.</p>
Schlüssel zur Authentisierung	Geben Sie eine Textfolge ein, die in Verbindung mit dem definierten Authentifizierungstyp verwendet wird.
Indirekte, statische Routen exportieren	Wenn dieser Wert auf <i>Nein</i> (Standardwert) gesetzt ist, werden nur direkte Routen (d.h. Routen zu direkt über diese Schnittstelle erreichbaren Netzen) über aktive OSPF-Schnittstelle propagiert (siehe Admin-Status). Wenn der Wert auf <i>Ja</i> gesetzt ist, werden auch indirekte statische Routen über aktive Schnittstellen propagiert.
Demand Circuit Options	Legen Sie fest, ob auf dieser Schnittstelle Demand OSPF Prozeduren (Hello Unterdrückung an FULL Neighbors und das Setzen des DoNotAge Flags auf der propagierten LSA) durchgeführt werden sollen (<i>Ja</i> , Standardwert) oder nicht (<i>Nein</i>). Diese Option sollte insbesondere bei Verbindungen deren Kosten zeitabhängig berechnet werden (z.B. ISDN-Wählverbindungen, Internetverbindungen ohne Flatrate) aktiviert werden.

14.2.3 Globale Einstellungen

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

Bereiche
Schnittstellen
Globale Einstellungen

Globale OSPF-Einstellungen	
OSPF-Status	<input type="checkbox"/> Aktiviert
Standardroute für AS eintragen	<input type="checkbox"/> Aktiviert
Auf Discard/Refuse-Schnittstelle gebundene Routen propagieren	<input type="checkbox"/> Aktiviert
Dynamic LS Update Compression	<input type="checkbox"/> Aktiviert

OK
Abbrechen

Abb. 97: Routing-Protokolle->OSPF->Globale Einstellungen

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

Felder im Menü Globale OSPF-Einstellungen

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

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Kapitel 15 Multicast

Was ist Multicasting?

Viele jüngere Kommunikations-Technologien basieren auf der Kommunikation von einem Sender zu mehreren Empfängern. Daher liegt auf der Reduzierung des Datenverkehrs ein Hauptaugenmerk von modernen Telekommunikationssystemen wie Voice-over-IP oder Video- und Audio-Streaming (z. B. IPTV oder Webradio), z. B. im Rahmen von TriplePlay (Voice, Video, Daten). Multicast bietet eine kostengünstige Lösung zur effektiven Bandbreitennutzung, dadurch dass der Sender das Datenpaket, welches mehrere Empfänger empfangen können, nur einmal senden muss. Dabei wird an eine virtuelle Adresse gesendet, die als Multicast-Gruppe bezeichnet wird. Interessierte 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.

15.1 Allgemein

15.1.1 Allgemein

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

Abb. 98: **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 <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

15.2 IGMP

Mit IGMP (Internet Group Management Protocol, siehe RFC 3376) werden die Informationen über die Gruppen (zugehörigkeit) in einem Subnetz signalisiert. Somit gelangen nur diejenigen Pakete in das Subnetz, die explizit von einem Host gewünscht sind.

Spezielle Mechanismen sorgen für die Vereinigung der Wünsche der einzelnen Clients.

Derzeit gibt es drei Versionen von IGMP (V1 - V3), wobei aktuelle Systeme meist V3, seltener V2, benutzen.

Bei IGMP spielen zwei Paketarten die zentrale Rolle: Queries und Reports.

Queries werden ausschließlich von einem Router versendet. Sollten mehrere IGMP-Router in einem Netzwerk existieren, so wird der Router mit der niedrigeren IP-Adresse der sogenannte Querier. Hierbei unterscheidet man das General Query (versendet an 224.0.0.1), die Group-Specific Query (versendet an jeweilige Gruppenadresse) und die Group-and-Source-Specific Query (versendet an jeweilige Gruppenadresse). Reports werden ausschließlich von Hosts versendet, um Queries zu beantworten.

15.2.1 IGMP

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

15.2.1.1 Bearbeiten oder Neu

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

IGMP Optionen

IGMP-Einstellungen	
Schnittstelle	Keine ▼
Abfrage Intervall	125 Sekunden
Maximale Antwortzeit	10,0 Sekunden
Robustheit	2 ▼
Antwortintervall (Letztes Mitglied)	1,0 Sekunden
Maximale Anzahl der IGMP-Statusmeldungen	0 Meldungen pro Sekunde
Modus	<input type="radio"/> Host <input checked="" type="radio"/> Routing
Erweiterte Einstellungen	
IGMP Proxy	<input type="checkbox"/> Aktiviert
OK Abbrechen	

Abb. 99: 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	<p>Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen.</p> <p>Möglich Werte sind 0 bis 600.</p> <p>Der Standardwert ist 125.</p>
Maximale Antwortzeit	<p>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.</p> <p>Möglich Werte sind 0,0 bis 25,0.</p> <p>Der Standardwert ist 10,0.</p>
Robustheit	<p>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).</p> <p>Möglich Werte sind 2 bis 8.</p> <p>Der Standardwert ist 2.</p>
Antwortintervall (Letztes Mitglied)	<p>Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet.</p> <p>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.</p> <p>Möglich Werte sind 0,0 bis 25,0.</p> <p>Der Standardwert ist 1,0.</p>

Feld	Beschreibung
Maximale Anzahl der IGMP-Statusmeldungen	Limitieren Sie die Anzahl der Reports/Queries pro Sekunde für die gewählte Schnittstelle.
Modus	<p>Wählen Sie aus, ob die hier definierte Schnittstelle nur im Host-Modus oder auch im Routing Modus arbeitet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Routing</i> (Standardwert): Die Schnittstelle wird im Routing-Modus betrieben. • <i>Host</i>: 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 IGMP-Proxy-Schnittstelle weitergeleitet.

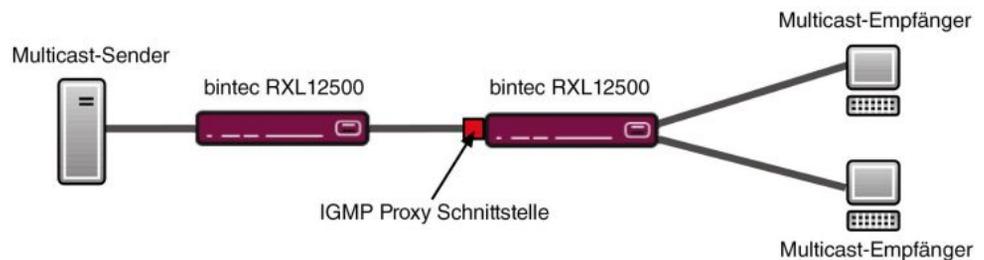


Abb. 100: IGMP Proxy

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	<p>Nur für IGMP Proxy = aktiviert</p> <p>Wählen Sie die Schnittstelle Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen.</p>

15.2.2 Optionen

In diesem Menü haben Sie die Möglichkeit, IGMP auf Ihrem System zu aktivieren bzw. zu deaktivieren. Außerdem können Sie bestimmen, ob IGMP im Kompatibilitätsmodus verwendet werden soll oder nur IGMP V3-Hosts akzeptiert werden sollen.

Grundeinstellungen	
IGMP-Status	<input type="radio"/> Aktiv <input type="radio"/> Inaktiv <input checked="" type="radio"/> Auto
Modus	<input checked="" type="radio"/> Kompatibilitätsmodus <input type="radio"/> Nur Version 3
Maximale Gruppen	64
Maximale Quellen	64
Maximale Anzahl der IGMP-Statusmeldungen	0 Meldungen pro Sekunde

Abb. 101: Multicast->IGMP->Optionen

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
IGMP-Status	<p>Wählen Sie den IGMP-Status aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Multicast wird für Hosts automatisch eingeschaltet, wenn diese Anwendungen öffnen, die Multicast verwenden. • <i>Aktiv</i>: Multicast ist immer aktiv. • <i>Inaktiv</i>: Multicast ist immer inaktiv.
Modus	<p>Nur für IGMP-Status = Aktiv oder <i>Auto</i></p> <p>Wählen Sie den Multicast-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Kompatibilitätsmodus</i> (Standardwert): Der Router verwendet IGMP Version 3. Bemerkt er eine niedrigere Version im Netz, verwendet er die niedrigste Version, die er erkennen

Feld	Beschreibung
	<p>konnte.</p> <ul style="list-style-type: none"> • <i>Nur Version 3</i>: 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 Reports der Version 3 spezifiziert sind, als auch die maximale Anzahl der intern verwalteten Quellen pro Gruppe.
Maximale Anzahl der IGMP-Statusmeldungen	<p>Geben Sie die maximale Anzahl der insgesamt möglichen eingehenden Queries bzw. Meldungen pro Sekunde ein.</p> <p>Der Standardwert ist 0, d. h. die Anzahl der IGMP-Statusmeldungen ist nicht begrenzt.</p>

15.3 Weiterleiten

15.3.1 Weiterleiten

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

15.3.1.1 Neu

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

Weiterleiten

Basisparameter	
Alle Multicast-Gruppen	<input type="checkbox"/> Aktiviert
Multicast-Gruppen-Adresse	<input type="text"/>
Quellschnittstelle	Keine ▾
Zielschnittstelle	Keine ▾

Abb. 102: Multicast->Weiterleiten->Weiterleiten->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Alle Multicast-Gruppen	<p>Wählen Sie aus, ob alle Multicast-Gruppen, d. h. der komplette Multicast-Adressraum 224.0.0.0/4, von der definierten Quellschnittstelle an die definierte Zielschnittstelle weitergeleitet werden soll. Setzen Sie dazu den Haken für <i>Aktiviert</i>.</p> <p>Möchten Sie nur eine definierte Multicast-Gruppe an eine bestimmte Schnittstelle weiterleiten, deaktivieren Sie die Option.</p> <p>Standardmäßig ist die Option nicht aktiv.</p>
Multicast-Gruppen-Adresse	<p>Nur für Alle Multicast-Gruppen = nicht aktiv</p> <p>Geben Sie hier die Adresse der Multicast-Gruppe ein, die Sie von einer definierten Quellschnittstelle an eine definierte Zielschnittstelle weiterleiten möchten.</p>
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.

15.4 PIM

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

Bei Multicast-Routing-Protokollen unterscheidet man grundsätzlich zwischen Sparse Mode und Dense Mode. Beim Dense Mode werden alle Pakete weitergeleitet und nur die Pakete an Gruppen verworfen, die explizit abbestellt wurden. Beim Sparse Mode werden nur Pakete an Gruppen weitergeleitet, die von diesen bestellt wurden. Ihr Gerät verwendet PIM im Sparse Mode.

15.4.1 PIM-Schnittstellen

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

The screenshot shows a web interface for configuring PIM interfaces. At the top, there are three tabs: **PIM-Schnittstellen** (selected), **PIM-Rendezvous-Punkte**, and **PIM-Optionen**. Below the tabs is a control bar with 'Ansicht' set to 20, 'pro Seite' with navigation arrows, 'Filtern in' set to 'Keiner', and a 'Los' button. A table header is visible with columns: 'Schnittstelle', 'IP-Version', 'Designated Router (DR)', 'Stub Interface Mode', 'Status', and 'Aktion'. The table content shows 'Seite: 1'. At the bottom center, there is a 'Neu' button.

Abb. 103: **Multicast->PIM->PIM-Schnittstellen**

15.4.1.1 Bearbeiten oder Neu

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

The screenshot shows the 'PIM-Schnittstelleneinstellungen' dialog box. It has three tabs: **PIM-Schnittstellen** (selected), **PIM-Rendezvous-Punkte**, and **PIM-Optionen**. The dialog is divided into two sections: 'PIM-Schnittstelleneinstellungen' and 'Erweiterte Einstellungen'.
 In the 'PIM-Schnittstelleneinstellungen' section, there are four rows:
 - Schnittstelle: Eine auswählen (dropdown)
 - PIM-Modus: Sparse Mode (SM)
 - Stub Interface Mode: Aktiviert
 - Designated-Router-Priorität: 1 (input field)
 In the 'Erweiterte Einstellungen' section, there are seven rows, each with a value in an input field and the unit 'Sekunden':
 - Hello-Intervall: 30
 - Triggered-Hello-Intervall: 5
 - Hello Hold Time: 105
 - Join/Prune-Intervall: 60
 - Join/Prune Hold Time: 210
 - Propagation Delay: 1
 - Override Interval: 3
 At the bottom, there are 'OK' and 'Abbrechen' buttons.

Abb. 104: **Multicast->PIM->PIM-Schnittstellen->Neu**

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

Felder im Menü PIM-Schnittstelleneinstellungen

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Hello-Intervall	<p>Bestimmen Sie, in welchen Zeitabständen (in Sekunden) PIM Hello Messages über diese Schnittstelle gesendet werden.</p> <p>Der Wert <i>0</i> bedeutet, dass auf dieser Schnittstelle keine PIM Hello Messages gesendet werden.</p> <p>Wertebereich: <i>0</i> bis <i>18000</i> Sekunden.</p> <p>Standardwert ist <i>30</i>.</p>
Triggered-Hello-Intervall	Bestimmen Sie, wie lange maximal gewartet werden darf, bis eine PIM Hello Message nach einem Systemstart oder nach einem

Feld	Beschreibung
	<p>Neustart eines Nachbarn gesendet wird.</p> <p>Der Wert <i>0</i> bedeutet, dass PIM Hello Messages immer sofort gesendet werden.</p> <p>Wertebereich: <i>0</i> bis <i>60</i> Sekunden.</p> <p>Standardwert ist <i>5</i>.</p>
Hello Hold Time	<p>Bestimmen Sie den Wert des Holdtime Feldes in einer PIM Hello Message.</p> <p>Daraus ergibt sich, wie lange ein PIM-Router als verfügbar gilt. Sobald die Hello Hold Time abgelaufen ist und keine weitere Hello Message empfangen wurde, wird dieser PIM-Router als nicht erreichbar betrachtet.</p> <p>Wertebereich: <i>0</i> bis <i>65535</i> Sekunden.</p> <p>Standardwert ist <i>105</i>.</p>
Join/Prune-Intervall	<p>Bestimmen Sie die Häufigkeit, mit der PIM Join/Prune Messages auf der Schnittstelle gesendet werden sollen.</p> <p>Der Wert <i>0</i> bedeutet, dass auf dieser Schnittstelle keine periodischen PIM Join/Prune Messages gesendet werden.</p> <p>Wertebereich: <i>0</i> bis <i>18000</i> Sekunden.</p> <p>Standardwert ist <i>60</i>.</p>
Join/Prune Hold Time	<p>Bestimmen Sie den Wert, der in das Holdtime Feld einer PIM Join/Prune Message eingefügt wird.</p> <p>Dies ist die Zeitspanne, die ein Empfänger den Join/Prune State halten muss.</p> <p>Wertebereich: <i>0</i> bis <i>65535</i> Sekunden.</p> <p>Standardwert ist <i>210</i>.</p>
Propagation Delay	<p>Bestimmen Sie den Wert, der in das Propagation Delay Feld eingefügt wird. Dieses Feld ist ein Bestandteil der LAN Prune Delay Option in den PIM Hello Messages, die auf dieser Schnittstelle gesendet werden.</p>

Feld	Beschreibung
	<p>Propagation Delay und Override Interval stellen die sogenannten LAN-Prune-Delay-Einstellungen dar. Sie bewirken eine verzögerte Verarbeitung von Prune-Messages bei Upstream Routern.</p> <p>Wenn Propagation Delay zu klein ist, kann es zum Abbruch der Übertragung von Multicast-Paketen kommen, bevor ein Downstream Router eine Prune Override Message geschickt hat.</p> <p>Wertebereich: 0 bis 32 Sekunden.</p> <p>Standardwert ist 1.</p>
Override Interval	<p>Bestimmen Sie den Wert, den das Gateway in das Feld Override Interval der LAN Prune Delay Option einfügt.</p> <p>Override Interval bestimmt, wie lange ein Downstream Router höchstens warten darf, bis er eine Prune Override Message schickt.</p> <p>Wertebereich: 0 bis 65 Sekunden.</p> <p>Standardwert ist 3.</p>

15.4.2 PIM-Rendezvous-Punkte

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

Es wird eine Liste aller PIM Rendezvous Points angezeigt.



Abb. 105: **Multicast->PIM->PIM-Rendezvous-Punkte**

15.4.2.1 Bearbeiten oder Neu

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

PIM-Schnittstellen
PIM-Rendezvous-Punkte
PIM-Optionen

Einstellungen für PIM-Rendezvous-Punkt	
Multicast-Gruppenbereich	<input type="text" value="Bestimmter Bereich"/>
Multicast-Gruppen-Adresse	<input type="text"/>
Präfixlänge der Multicast-Gruppe	<input type="text" value="4"/>
Rendezvous Point IP-Adresse	<input type="text"/>
Vorrang	<input type="text" value="0"/>

OK
Abbrechen

Abb. 106: Multicast->PIM->PIM-Rendezvous-Punkte->Neu

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

Felder im Menü Einstellungen für PIM-Rendezvous-Punkt

Feld	Beschreibung
Multicast-Gruppenbereich	Wählen Sie die Multicast-Gruppen für den PIM Rendezvous Point aus. Sie können <i>Alle Gruppen</i> (Standardwert) angeben oder mit Auswahl von <i>Specific Range</i> ein Multicast-Netzwerksegment spezifizieren.
Multicast-Gruppen-Adresse	Nur bei Multicast-Gruppenbereich = <i>Bestimmter Bereich</i> Geben Sie hier die IP-Adresse des Multicast-Netzwerksegments ein.
Präfixlänge der Multicast-Gruppe	Nur bei Multicast-Gruppenbereich = <i>Bestimmter Bereich</i> Geben Sie hier die Netzmaskenlänge des Multicast-Netzwerksegments ein. 224.0.0.0/4 bezeichnet das komplette Multicast Class D Segment. Wertebereich: 4 (Standardwert) bis 32.
Rendezvous Point IP-	Geben Sie die IP-Adresse oder den Hostnamen des Rendez-

Feld	Beschreibung
Adresse	vous Points ein.
Vorrang	<p>Geben Sie den Wert für pimGroupMappingPrecedence ein, der für statische RP Konfigurationen verwendet werden soll. Dieses erlaubt die genaue Kontrolle darüber, welche Konfiguration durch diese statische Konfiguration ersetzt werden soll.</p> <p>Wenn die Funktion aktiviert ist, wird pimStaticRPOverrideDynamic ignoriert. Die absoluten Werte dieses Objekts haben nur Bedeutung auf dem lokalen Router und müssen nicht mit anderen Routern abgestimmt werden.</p> <p>Die Funktion ist mit dem Standardwert 0 deaktiviert. Wenn die Funktion durch Setzen eines Wertes nicht 0 aktiviert wird, kann das verschiedene Auswirkungen auf andere Router haben. Verwenden Sie daher diese Funktion nicht, wenn eine genaue Kontrolle des Verhaltens des statischen RP nicht benötigt wird.</p>

15.4.3 PIM-Optionen

PIM-Schnittstellen | PIM-Rendezvous-Punkte | **PIM-Optionen**

Grundeinstellungen	
PIM-Status	<input type="checkbox"/> Aktiviert
Keepalive-Periode	210 Sekunden
Register Suppression Timer	60 Sekunden

OK Abbrechen

Abb. 107: Multicast->PIM->PIM-Optionen

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
PIM-Status	<p>Wählen Sie aus ob PIM aktiviert werden soll. Mit Auswahl von <i>Aktivieren</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Keepalive-Periode	Geben Sie die Zeitspanne in Sekunden ein, in der eine Keepali-

Feld	Beschreibung
	<p>ve Nachricht gesendet werden muss.</p> <p>Mögliche Werte: 0 bis 65535.</p> <p>Der Standardwert ist 210 .</p>
Register Suppression Timer	<p>Geben Sie die Zeit in Sekunden an, nach der ein PIM Designated Router (DR) keine register-encapsulated Daten mehr zum Rendezvous Point (RP) schicken soll, nachdem die Register-Stop-Nachricht empfangen wurde. Dieses Objekt wird verwendet, um sowohl am DR als auch am RP Timer zu nutzen. Dieser Zeitraum wird in der PIM-SM Spezifikation Register_Suppression_Time genannt.</p> <p>Mögliche Werte: 0 bis 65535.</p> <p>Der Standardwert ist 60 .</p>

Kapitel 16 WAN

Dieses Menü stellt Ihnen verschiedene Möglichkeiten zur Verfügung, Zugänge bzw. Verbindungen aus Ihrem LAN zum WAN zu konfigurieren. Außerdem können Sie hier die Sprachübertragung bei Telefongesprächen über das Internet optimieren.

16.1 Internet + Einwählen

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

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 **Benutzernamen**, 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.

16.1.1 PPPoE

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

PPP over Ethernet (PPPoE) ist die Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird heute bei ADSL-Anschlüssen in Deutschland verwendet. In Österreich wurde ursprünglich für ADSL-Zugänge das Point To Point Tunneling Protocol (PPTP) verwendet. Mittlerweile wird allerdings PPPoE auch dort von einigen Providern angeboten.

16.1.1.1 Neu

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

PPPoE PPTP UMTS/LTE IP Pools

Basisparameter	
Beschreibung	<input type="text"/>
PPPoE-Modus	<input checked="" type="radio"/> Standard <input type="radio"/> Mehrfachverbindung
PPPoE-Ethernet-Schnittstelle	Eine auswählen ▼
Benutzername	<input type="text"/>
Passwort	••••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	300 Sekunden
IPv4-Einstellungen	
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
IPv6-Einstellungen	
IPv6	<input checked="" type="checkbox"/> Aktiviert
Sicherheitsrichtlinie	<input checked="" type="radio"/> Unsicher <input type="radio"/> Sicher
Präfixmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Präfix beziehen
Erweiterte Einstellungen	
Blockieren nach Verbindungsfehler für	60 Sekunden
Maximale Anzahl der erneuten Einwählversuche	5
Authentifizierung	PAP ▼
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input type="checkbox"/> Aktiviert
Erweiterte IPv4-Einstellungen	
MTU	<input checked="" type="checkbox"/> Automatisch
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 108: 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

Feld	Beschreibung
	<p>PPPoE (<i>Standard</i>) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll (<i>Mehrfachverbindung</i>). Wählen Sie <i>Mehrfachverbindung</i>, 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.</p> <p>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. <i>en1-1, en1-2</i>.</p> <p>Wenn Sie für PPPoE Multilink zusätzlich ein externes Modem benutzen wollen, müssen Sie den Ethernet-Switch Ihres Geräts im Split-Port-Modus betreiben.</p>
PPPoE-Ethernet-Schnittstelle	<p>Nur für PPPoE-Modus = <i>Standard</i></p> <p>Wählen Sie die Ethernet-Schnittstelle aus, die für eine Standard-PPPoE-Verbindung vorgegeben wird.</p> <p>Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist.</p> <p>Bei Verwendung des internen DSL-Modems, wählen Sie hier die in Physikalische Schnittstellen->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle aus.</p>
PPPoE-Schnittstelle für Mehrfachlink	<p>Nur für PPPoE-Modus= <i>Mehrfachverbindung</i></p> <p>Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die Hinzufügen-Schaltfläche, um weitere Einträge anzulegen.</p>
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.

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

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die statische IP-Adresse des Verbindungspartners ein.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 ... 15). Standardwert ist 1.

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob diese Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Unsicher</i> (Standardwert): Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen. • <i>Sicher</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 367 konfigurieren.</p>
Präfixmodus	<p>Wählen Sie aus, wie das Präfix zugeteilt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Präfix beziehen</i> (Standardwert): Der Schnittstelle wird das Präfix zugewiesen. • <i>Statisch</i>: Das Präfix der Schnittstelle wird manuell festgesetzt.
IPv6-Präfix/Länge	<p>Für IPv6 = <i>Aktiviert</i> und Präfixmodus = <i>Statisch</i></p> <p>Geben Sie für die Schnittstelle das IPv6-Präfix und die entsprechende Länge an.</p> <p>Mit Hinzufügen können Sie weitere Präfix-Einträge hinzufügen.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Standardwert ist <i>60</i>.</p>
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind <i>0</i> bis <i>100</i>.</p> <p>Der Standardwert ist <i>5</i>.</p>

Feld	Beschreibung
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für DNS-Server Primär und DNS-Server Sekundär vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
LCP-Erreichbarkeitsprüfung	<p>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</p>

Feld	Beschreibung
	<p>auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die Verbindung verwendet werden darf.</p> <p>Mit dem Standardwert <i>Automatisch</i> wird der Wert beim Verbindungsaufbau durch das Link Control Protocol vorgegeben.</p> <p>Wenn Sie <i>Automatisch</i> deaktivieren, können Sie einen Wert eingeben.</p> <p>Mögliche Werte sind 1 bis 8192.</p> <p>Standardwert ist 0.</p>

16.1.2 PPTP

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

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

16.1.2.1 Neu

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

Basisparameter	
Beschreibung	<input type="text"/>
PPTP-Schnittstelle	Eine auswählen ▾
Benutzername	<input type="text"/>
Passwort	••••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	300 Sekunden
IPv4-Einstellungen	
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Blockieren nach Verbindungsfehler für	60 Sekunden
Maximale Anzahl der erneuten Einwählversuche	5
Authentifizierung	PAP ▾
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
PPTP-Adressmodus	Statisch
Lokale PPTP-IP-Adresse	10.0.0.140
Entfernte PPTP-IP-Adresse	10.0.0.138
LCP-Erreichbarkeitsprüfung	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 109: 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-Schnittstelle	Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden. Bei Verwendung eines externen DSL-Modems, wählen Sie hier

Feld	Beschreibung
	<p>den Ethernet-Port aus, an dem das Modem angeschlossen ist.</p> <p>Bei Verwendung des internen DSL-Modems, wählen Sie hier die in Physikalische Schnittstellen->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle z. B. <i>ethoa50-0</i>, aus.</p>
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>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.</p> <p>Mögliche Werte sind <i>0</i> bis <i>3600</i> (Sekunden). <i>0</i> deaktiviert den Timeout.</p> <p>Der Standardwert ist <i>300</i> .</p> <p>Bsp. <i>10</i> für FTP-Übertragungen, <i>20</i> für LAN-zu-LAN-Übertragungen, <i>90</i> für Internetverbindungen.</p>

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine temporär gültige IP-Adresse vom Provider.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Weisen Sie der PPTP-Schnittstelle eine IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen PPTP-Partner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • <i>Metrik</i>: 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 <i>60</i> .
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind <i>0</i> bis <i>100</i> .</p> <p>Der Standardwert ist <i>5</i> .</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i> : Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für DNS-Server Primär und DNS-Server Sekundär vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für</p>

Feld	Beschreibung
	<p>asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
PPTP-Adressmodus	<p>Zeigt den Adressmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i>: Die Lokale PPTP-IP-Adresse wird dem ausgewählten Ethernet-Port zugewiesen.
Lokale PPTP-IP-Adresse	<p>Weisen Sie der PPTP-Schnittstelle eine IP-Adresse zu, die als Quelladresse verwendet wird.</p> <p>Standardwert ist <i>10.0.0.140</i>.</p>
Entfernte PPTP-IP-Adresse	<p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p> <p>Standardwert ist <i>10.0.0.138</i>.</p>
LCP-Erreichbarkeitsprüfung	<p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

16.1.3 ISDN

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

In diesem Menü konfigurieren Sie folgende ISDN-Verbindungen:

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

16.1.3.1 Neu

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

PPPoE PPTP PPPoA ISDN AUX IP Pools

Basisparameter													
Beschreibung	<input type="text"/>												
Verbindungstyp	ISDN 64 kbit/s v												
Benutzername	<input type="text"/>												
Entfernter Benutzer (nur Einwahl)	<input type="text"/>												
Passwort	••••••••												
Immer aktiv	<input type="checkbox"/> Aktiviert												
Timeout bei Inaktivität	20 Sekunden												
IP-Modus und Routen													
IP-Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse bereitstellen <input type="radio"/> IP-Adresse abrufen												
Standardroute	<input type="checkbox"/> Aktiviert												
NAT-Eintrag erstellen	<input type="checkbox"/> Aktiviert												
Lokale IP-Adresse	<input type="text"/>												
Routeneinträge	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Entfernte IP-Adresse</th> <th style="width: 30%;">Netzmaske</th> <th style="width: 10%;">Metrik</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td>1 v</td> <td><input type="text"/></td> </tr> <tr> <td colspan="4" style="text-align: center;">Hinzufügen</td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	1 v	<input type="text"/>	Hinzufügen			
Entfernte IP-Adresse	Netzmaske	Metrik											
<input type="text"/>	<input type="text"/>	1 v	<input type="text"/>										
Hinzufügen													
Erweiterte Einstellungen													
Blockieren nach Verbindungsfehler für	300 Sekunden												
Maximale Anzahl der erneuten Einwählversuche	5												
Nutzungsart	<input checked="" type="radio"/> Standard <input type="radio"/> Nur Einwahl <input type="radio"/> Mehrfacheinwahl (Nur Einwahl)												
Authentifizierung	PAP/CHAP/MS-CHAP v												
Callback-Modus	<input checked="" type="radio"/> Keiner <input type="radio"/> Aktiv <input type="radio"/> Passiv												
Optionen für Bandbreite auf Anforderung													
Kanalbündelung	Keine v												
Wahlnummern													
Einträge	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Modus</th> <th style="width: 40%;">Rufnummer</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="2" style="text-align: center;">Hinzufügen</td> </tr> </tbody> </table>	Modus	Rufnummer	<input type="text"/>	<input type="text"/>	Hinzufügen							
Modus	Rufnummer												
<input type="text"/>	<input type="text"/>												
Hinzufügen													
IP-Optionen													
OSPF-Modus	<input checked="" type="radio"/> Passiv <input type="radio"/> Aktiv <input type="radio"/> Inaktiv												
Proxy-ARP-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv												
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert												
OK Abbrechen													

Abb. 110: WAN->Internet + Einwählen->ISDN->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.</p>
Verbindungstyp	<p>Wählen Sie aus, welches Layer-1-Protokoll Ihr Gerät nutzen soll.</p> <p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>ISDN 64 kbit/s</i>: Für ISDN-Datenverbindungen mit 64 kbit/s • <i>ISDN 56 kbit/s</i>: Für ISDN-Datenverbindungen mit 56 kbit/s
Benutzername	<p>Geben Sie die Kennung Ihres Geräts (lokaler PPP-Benutzername) ein.</p>
Entfernter Benutzer (nur Einwahl)	<p>Geben Sie die Kennung der Gegenstelle (entfernter PPP-Benutzername) ein.</p>
Passwort	<p>Geben Sie das Passwort ein.</p>
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen</p>

Feld	Beschreibung
	<p>Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Timeout.</p> <p>Standardwert ist 20 .</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein. • <i>IP-Adresse bereitstellen</i>: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	<p>Nur bei IP-Adressmodus = <i>Statisch</i> und <i>IP-Adresse abrufen</i></p> <p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
NAT-Eintrag erstellen	<p>Nur bei IP-Adressmodus = <i>Statisch</i> und <i>IP-Adresse abrufen</i></p> <p>Wenn eine ISDN-Internetverbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
Lokale IP-Adresse	Nur bei IP-Adressmodus = <i>Statisch</i> Weisen Sie der ISDN-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	Nur bei IP-Adressmodus = <i>Statisch</i> Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 ... 15). Der Standardwert ist 1.
IP-Zuordnungspool	Nur bei IP-Adressmodus = <i>IP-Adresse bereitstellen</i> 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 <i>Noch nicht definiert</i> .

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 von 0 bis 100. Der Standardwert ist 5.

Feld	Beschreibung
Nutzungsart	<p>Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Kein spezieller Typ ist ausgewählt. • <i>Nur Einwahl</i>: Die Schnittstelle wird für eingehende Wählverbindungen und für von außen initiierten Callback verwendet. • <i>Mehrfacheinwahl (Nur Einwahl)</i>: Die Schnittstelle wird als Multi-User-Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen PPTP Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	<p>Nur für Authentifizierung = <i>MS-CHAPv2</i></p> <p>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.</p>

Feld	Beschreibung
	<p>MS-STAC für die Verbindung aktiv ist. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i>: Die MPP-Verschlüsselung V2 mit 128 bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 bit wird kompatibel zu Microsoft und Cisco angewendet.
Callback-Modus	<p>Wählen Sie die Funktion Callback-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Ihr Gerät führt keinen Rückruf aus. • <i>Aktiv</i>: Wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> • <i>Keine PPP-Aushandlung</i>: Ihr Gerät ruft den Verbindungspartner an, um einen Rückruf anzufordern. • <i>Windows-Clientmodus</i>: Ihr Gerät ruft den Verbindungspartner an, um über CBCP (Callback Control Protocol) einen Rückruf anzufordern. Wird für Windows Clients benötigt. • <i>Passiv</i>: Wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> • <i>PPP-Aushandlung oder CLID</i>: Ihr Gerät ruft sofort zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert wird. • <i>Windows-Servermodus</i>: 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 <i>Beide</i>, 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. • <i>Verzögert, nur CLID</i>: Ihr Gerät ruft nach ca. vier Se-

Feld	Beschreibung
	<p>kunden zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert worden ist. Nur sinnvoll bei CLID.</p> <ul style="list-style-type: none"> • <i>Windows-Servermodus, Rückruf optional</i>: Wie <i>Windows-Servermodus</i> mit <i>Abbruchoption</i>. 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	<p>Wählen Sie aus, ob Kanalbündelung bzw. welche Art von Kanalbündelung für ISDN-Verbindungen mit dem Verbindungspartner genutzt werden soll.</p> <p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung. • <i>Statisch</i>: Statische Kanalbündelung. • <i>Dynamisch</i>: 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)

fügen)

Feld	Beschreibung
Modus	<p>Nur wenn Einträge = <i>Hinzufügen</i></p> <p>Wählen Sie aus, ob Rufnummer für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): Für eingehende und ausgehende Rufe. • <i>Eingehend</i>: Für eingehende Rufe, wenn der Verbindungspartner sich bei Ihrem Gerät einwählen soll. • <i>Ausgehend</i>: Für ausgehende Rufe, wenn Sie sich beim Verbindungspartner einwählen wollen. <p>Die Calling Party Number des eingehenden Rufes wird mit der unter Rufnummer eingetragenen Nummer verglichen.</p>
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	<p>Wählen Sie aus, ob und wie über die Schnittstellen Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (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. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	Wählen Sie aus, ob und wie ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantwortet werden.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für DNS-Server Primär und Sekundär und WINS-Server Primär und Sekundär vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

16.1.4 UMTS/LTE



Hinweis

Beachten Sie, dass das Menü **UMTS/LTE** nur bei Verwendung eines UMTS/HSD-PA/LTE-USB-Sticks verfügbar ist!

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

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

16.1.4.1 Neu

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

PPPoE PPTP **UMTS/LTE** IP Pools

Basisparameter	
Beschreibung	<input type="text"/>
UMTS/LTE-Schnittstelle	UMTS-6-0 ▼
Benutzername	<input type="text"/>
Passwort	••••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	300 Sekunden
IP-Modus und Routen	
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Blockieren nach Verbindungsfehler für	60 Sekunden
Maximale Anzahl der erneuten Einwählversuche	5
Authentifizierung	PAP ▼
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 111: **WAN->Internet + Einwählen->UMTS/LTE->Neu**

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte sind 0 bis 3600 (Sekunden). 0 deaktiviert den Short-Hold.</p> <p>Der Standardwert ist 300.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) akti-

Feld	Beschreibung
	<p>viert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die statische IP-Adresse des Verbindungspartners ein.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • <i>Metrik</i>: 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	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist 60.</p>
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte von 0 bis 100.</p> <p>Der Standardwert ist 5.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
<p>DNS-Aushandlung</p>	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für DNS-Server Primär und DNS-Server Sekundär vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>TCP-ACK-Pakete priorisieren</p>	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>LCP-Erreichbarkeitsprüfung</p>	<p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

16.15 IP Pools

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

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

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adress-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft Ihr Gerät zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann Ihr Gerät eine IP-Adresse aus einem Adress-Pool zuweisen (falls verfügbar). Bei Adress-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher Verbindungspartner welche Adresse bekommt. Die Adressen werden zunächst einfach der Reihe nach vergeben. Bei einer erneuten Einwahl innerhalb eines Intervalls von einer Stunde wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

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

Abb. 112: WAN->Internet + Einwählen->IP Pools->Hinzufügen

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

Felder im Menü IP Pools

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

Feld	Beschreibung
	<p>ein.</p> <p>Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.</p>

16.2 IPv6-Tunnel

16.2.1 IPv6-Tunnel

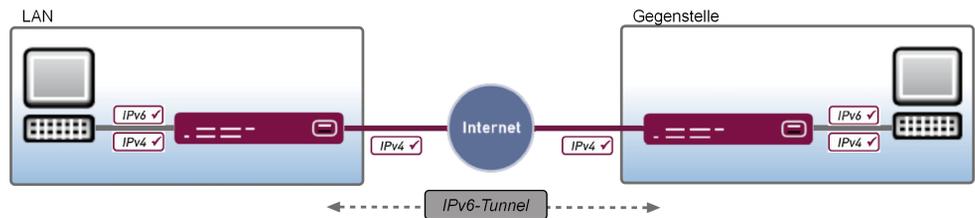


Abb. 113: IPv6-Tunneling-Szenario

Beim IPv6-Tunneling wird ein IPv6-Datenpaket aus dem LAN vom Router in ein IPv4--Datenpaket gekapselt. Dieses Paket kann anschließend über das IPv4-Netzwerk des WANs weitergeleitet werden. Ein Router auf der anderen Seite des IPv6-Tunnels entfernt den IPv4-Header wieder und erhält damit das Original-IPv6-Paket. Auf diese Weise ist ein sanfter Übergang zwischen IPv4- und IPv6-Netzwerken möglich.

In den Geräten der Teldat GmbH sind mehrere IPv6-Tunneling-Mechanismen implementiert.

16.2.1.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Tunnel einzurichten.

IPv6-Tunnel

Basisparameter	
Beschreibung	<input type="text"/>
Tunnelmodus	Eine auswählen ▾
Sicherheitsrichtlinie	<input checked="" type="radio"/> Unsicher <input type="radio"/> Sicher
Über Schnittstelle	Keine ▾

Abb. 114: WAN->IPv6-Tunnel->IPv6-Tunnel->Neu

Das Menü **WAN->IPv6-Tunnel->IPv6-Tunnel->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den IPv6-Tunnel ein.
Tunnelmodus	<p>Wählen Sie den Tunnel-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>6in4 Relay</i>: Eine Standard-6in4-Tunnel-Schnittstelle wird verwendet. • <i>SixXS</i>: Ein SixXS-Tunnel (SixXS-Konfigurationsprofil für eine 6in4-Tunnel-Konfiguration) wird verwendet. • <i>Hurricane Electric</i>: Ein Hurricane-Electric-Tunnel (Hurricane-Electric-Konfigurationsprofil für eine 6in4-Tunnel-Konfiguration) wird verwendet. • <i>6to4 RFC</i>: Eine Standard-6to4-Tunnel-Schnittstelle wird verwendet.
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Unsicher</i> (Standardwert): Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Sicher</i>: Es werden alle IP-Pakete durchgelassen, außer de-

Feld	Beschreibung
	<p>nen, die explizit verboten sind.</p> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 367 konfigurieren.</p>
Über Schnittstelle	Wählen Sie eine IPv4-Schnittstelle bzw. den gewünschten Verbindungspartner als Start-/ Endpunkt des Tunnels aus.
6in4 Relay IPv4-Adresse	<p>Nur für Tunnelmodus = <i>6in4 Relay</i></p> <p>Geben Sie die IPv4-Adresse der Tunnelgegenstelle ein.</p>
Benutzername	<p>Nur für Tunnelmodus = <i>SixXS</i></p> <p>Geben Sie den SixXS-Benutzernamen ein, der für Ihren Tunnel konfiguriert ist. Sie haben diesen Benutzernamen von SixXS erhalten.</p>
Nutzerkennung	<p>Nur für Tunnelmodus = <i>Hurricane Electric</i></p> <p>Geben Sie die Hurricane Electric User ID ein, die für Ihren Tunnel konfiguriert ist. Sie haben diese User ID von Hurricane Electric erhalten.</p>
Passwort	<p>Nur für Tunnelmodus = <i>SixXS</i> oder <i>Hurricane Electric</i></p> <p>Geben Sie das Tunnelpasswort ein, das Sie für Ihren Tunnel bei SixXS bzw. Hurricane Electric konfiguriert haben.</p>
Tunnel-ID	<p>Nur für Tunnelmodus = <i>SixXS</i> oder <i>Hurricane Electric</i></p> <p>Geben Sie die ID Ihres Tunnels ein, die Ihnen SixXS bzw. Hurricane Electric zugeteilt hat.</p>
IPv4-Adresse des Tunnelendpunkts	<p>Nur für Tunnelmodus = <i>Hurricane Electric</i></p> <p>Geben Sie die IPv4-Adresse der Tunnelgegenstelle ein.</p>
Lokale IPv6-Adresse	<p>Nur für Tunnelmodus = <i>Hurricane Electric</i></p> <p>Geben Sie die lokale IPv6-Adresse ein. Sie haben diese Adresse von Hurricane Electric erhalten.</p>

Feld	Beschreibung
Entfernte IPv6-Adresse	Nur für Tunnelmodus = <i>Hurricane Electric</i> Geben Sie die IPv6-Adresse der Tunnelgegenstelle ein. Sie haben diese Adresse von Hurricane Electric erhalten.
Entferntes IPv6-Netzwerk	Nur für Tunnelmodus = <i>6in4 Relay</i> Fügen Sie mit Hinzufügen einen neuen Präfix-Eintrag hinzu und geben Sie das IPv6-Präfix und die entsprechende Länge der Tunnelgegenstelle ein.
Zugewiesener IPv6-Präfix/Länge	Nur für Tunnelmodus = <i>SixXS</i> oder <i>Hurricane Electric</i> Fügen Sie mit Hinzufügen einen neuen Präfix-Eintrag hinzu und geben Sie für die Schnittstelle das IPv6-Präfix und die entsprechende Länge an. Sie haben dieses Präfix von SixXS bzw. Hurricane Electric erhalten.
6to4 Relay Anycast IPv4-Adresse	Nur für Tunnelmodus = <i>6to4 RFC</i> Die globale 6to4-Anycast-Relay-Adresse 192.88.99.1 wird angezeigt. Über diese Adresse erreichen Sie das nächste öffentliche 6to4 Relay, das Ihnen einen Zugang zum IPv6-Netz ermöglicht.

16.3 Standleitung

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

16.3.1 Schnittstellen

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

Schnittstellen

Automatisch generiert von BRI (ISDN-S0)						
Beschreibung	Typ	Protokoll	Port	Status	Aktion	
bri2-0-1	Standleitung B1 64S	PPP	bri2-0	⊖	⬆️⬇️⬆️	🔗

Automatisch generiert von PRI (ISDN-S2M)						
Beschreibung	Typ	Protokoll	Port	Status	Aktion	
pri2-4-0	Standleitung, 1 Hyperchannel (G.703 + G.704)	PPP	pri2-4	⊖	⬆️⬇️⬆️	🔗

Abb. 115: **WAN->Standleitung->Schnittstellen**

16.3.1.1 Bearbeiten

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

Schnittstellen

Basisparameter			
Beschreibung	<input type="text" value="bri2-0-1"/>		
IP-Modus und Routen			
Standardroute	<input type="checkbox"/> Aktiviert		
Lokale IP-Adresse	<input type="text"/>		
Routeneinträge	Entfernte IP-Adresse	Netzmaske	Metrik
	<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>
<input type="button" value="Hinzufügen"/>			
Erweiterte Einstellungen			
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert		
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert		
Komprimierung	<input checked="" type="radio"/> Keine <input type="radio"/> STAC <input type="radio"/> MS-STAC <input type="radio"/> MPPC		
IP-Optionen			
OSPF-Modus	<input checked="" type="radio"/> Passiv <input type="radio"/> Aktiv <input type="radio"/> Inaktiv		
Proxy-ARP-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv		
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>			

Abb. 116: WAN->Standleitung->Schnittstellen->Automatisch generiert von BRI (ISDN-S0)->

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

Felder im Menü Basisparameter

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

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle überprüft werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Komprimierung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande. Mögliche Werte: <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird keine Verschlüsselung angewendet. • <i>STAC</i> • <i>MS-STAC</i> • <i>MPPC</i>: Microsoft Point-to-Point Compression

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus ob über die Schnittstelle OSPF-Protokoll-Pakete gesendet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob und wie die ARP-Requests für diesen spezifischen Verbindungspartner beantwortet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.

16.4 Real Time Jitter Control

Bei Telefongesprächen über das Internet haben Sprachdaten-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 Sprach-

daten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

16.4.1 Regulierte Schnittstellen

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

16.4.1.1 Neu

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

Regulierte Schnittstellen

Grundeinstellungen	
Schnittstelle	Keine ▾
Kontrollmodus	Nur kontrollierte RTP-Streams ▾
Maximale Upload-Geschwindigkeit	<input style="width: 80%;" type="text" value="0"/> kbit/s
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Schnittstelle	Legen Sie fest, für welche Schnittstellen die Sprachübertragung optimiert werden soll.
Kontrollmodus	<p>Wählen Sie den Modus für die Optimierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nur kontrollierte RTP-Streams</i> (Standardwert): Anhand der Daten, die über das Media Gateway geroutet werden, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung. • <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert. • <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachda-

Feld	Beschreibung
	ten wird nicht durchgeführt. <ul style="list-style-type: none"><li data-bbox="631 239 1320 312">• <i>Immer</i>: Die Optimierung für die Übertragung der Sprachdaten wird immer durchgeführt.
Maximale Upload-Geschwindigkeit	Geben Sie die maximal zur Verfügung stehende Bandbreite in Upload-Richtung in kbit/s für die gewählte Schnittstelle ein.

Kapitel 17 VPN

Als VPN (Virtual Private Network) wird eine Verbindung bezeichnet, die das Internet als "Transportmedium" nutzt, aber nicht öffentlich zugänglich ist. Nur berechtigte Benutzer haben Zugang zu einem solchen VPN, das anschaulich auch als VPN-Tunnel bezeichnet wird. Üblicherweise werden die über ein VPN transportierten Daten 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 Pre-shared Keys oder über Zertifikate.

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

17.1 IPSec

IPSec ermöglicht den Aufbau von gesicherten Verbindungen zwischen zwei Standorten (VPN). Hierdurch lassen sich sensible Unternehmensdaten auch über ein unsicheres Medium wie z. B. das Internet übertragen. Die eingesetzten Geräte agieren hierbei als Endpunkte des VPN Tunnels. Bei IPSec handelt es sich um eine Reihe von Internet-Engineering-Task-Force-(IETF)-Standards, die Mechanismen zum Schutz und zur Authentifizierung von IP-Paketen spezifizieren. IPSec bietet Mechanismen, um die in den IP-Paketen übermittelten Daten zu verschlüsseln und zu entschlüsseln. Darüber hinaus kann die IPSec-Implementierung nahtlos in eine Public-Key-Umgebung (PKI, siehe [Zertifikate](#) auf Seite 93) integriert werden. Die bintec-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 Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode ist ausschließlich über das Setup Tool konfigurierbar. Mit dem GUI verwenden Sie die Routing-basierte Methode. (Letztere ist zusätzlich auch über das Setup Tool verfügbar.)

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.

17.1.1 IPSec-Peers

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

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

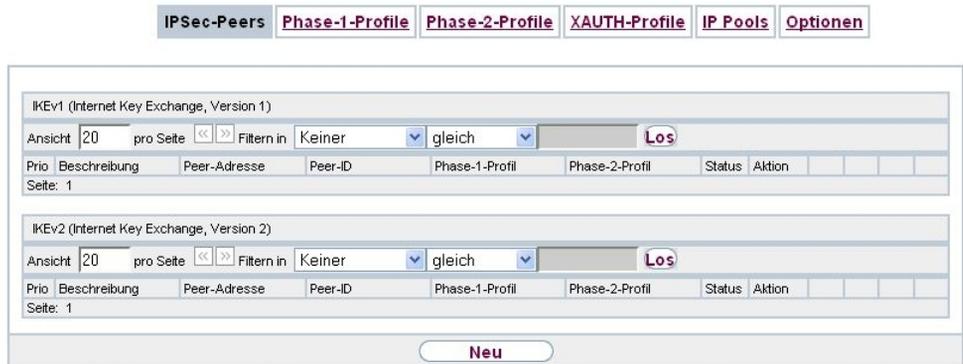


Abb. 118: **VPN->IPSec->IPSec-Peers**

Peer Überwachung

Das Überwachungsmenü eines Peers wird durch Auswahl der -Schaltfläche beim entsprechenden Peer in der Peerliste aufgerufen. Siehe [Werte in der Liste IPSec-Tunnel](#) auf Seite 486.

17.1.1.1 Neu

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [IP Pools](#) | [Optionen](#)

Peer-Parameter													
Administrativer Status	<input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv												
Beschreibung	<input type="text" value="Peer-1"/>												
Peer-Adresse	<input type="text"/>												
Peer-ID	Fully Qualified Domain Name (FQDN) <input type="text" value="Peer-1"/>												
IKE (Internet Key Exchange)	<input type="text" value="IKEv1"/>												
Preshared Key	<input type="text"/>												
Schnittstellenrouten													
IP-Adressenvergabe	<input type="text" value="Statisch"/>												
Standardroute	<input type="checkbox"/> Aktiviert												
Lokale IP-Adresse	<input type="text"/>												
Routeneinträge	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Entfernte IP-Adresse</th> <th style="width: 20%;">Netzmaske</th> <th style="width: 10%;">Metrik</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text" value="1"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="button" value="Hinzufügen"/>			
Entfernte IP-Adresse	Netzmaske	Metrik											
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>										
<input type="button" value="Hinzufügen"/>													
Zusätzlicher Filter des Datenverkehrs													
Zusätzlicher Filter des Datenverkehrs	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Beschreibung</th> <th style="width: 10%;">Protokoll</th> <th style="width: 20%;">Quell-IP/Maske/Port</th> <th style="width: 30%;">Ziel-IP/Maske/Port</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </tbody> </table>	Beschreibung	Protokoll	Quell-IP/Maske/Port	Ziel-IP/Maske/Port	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Hinzufügen"/>			
Beschreibung	Protokoll	Quell-IP/Maske/Port	Ziel-IP/Maske/Port										
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>										
<input type="button" value="Hinzufügen"/>													
Erweiterte Einstellungen													
Erweiterte IPSec-Optionen													
Phase-1-Profil	<input type="text" value="Keines (Standardprofil verwenden)"/>												
Phase-2-Profil	<input type="text" value="Keines (Standardprofil verwenden)"/>												
XAUTH-Profil	<input type="text" value="Eines auswählen"/>												
Anzahl erlaubter Verbindungen	<input checked="" type="radio"/> Ein Benutzer <input type="radio"/> Mehrere Benutzer												
Startmodus	<input checked="" type="radio"/> Auf Anforderung <input type="radio"/> Immer aktiv												
Erweiterte IP-Optionen													
Überprüfung der Rückroute	<input type="checkbox"/> Aktiviert												
Proxy ARP	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv												
IPSec-Callback													
Modus	<input type="text" value="Inaktiv"/>												
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>													

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

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

Felder im Menü Peer-Parameter

Feld	Beschreibung
Administrativer Status	Wählen Sie den Zustand aus, in den Sie den Peer nach dem

Feld	Beschreibung
	<p>Speichern der Peer-Konfiguration versetzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. • <i>Inaktiv</i>: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.
Beschreibung	<p>Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
Peer-Adresse	<p>Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein.</p> <p>Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.</p>
Peer-ID	<p>Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein.</p> <p>Die Eingabe kann in bestimmten Konfigurationen entfallen.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p> <p>Mögliche ID-Typen:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüssel-ID</i>: Beliebige hexadezimale Zeichenfolge mit einer geraden Anzahl an Ziffern <p>Auf dem Peer-Gerät entspricht diese ID dem Parameter Lokaler ID-Wert.</p>
IKE (Internet Key Exchange)	<p>Wählen Sie die Version des Internet-Key-Exchange-Protokolls, die verwendet werden soll.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IKEv1</i> (Standardwert): Internet Key Exchange Protocol Version 1 • <i>IKEv2</i>: Internet Key Exchange Protocol Version 2
Authentifizierungsmethode	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv2</i></p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (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. • <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert.
Lokaler ID-Typ	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv2</i></p> <p>Wählen Sie den Typ der lokalen ID aus.</p> <p>Mögliche ID-Typen:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüssel-ID</i>: Beliebige hexadezimale Zeichenfolge mit einer geraden Anzahl an Ziffern
Lokale ID	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv2</i></p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für Authentifizierungsmethode = <i>DSA-Signatur</i> oder <i>RSA-Signatur</i> wird die Option Subjektnamen aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektnamen aus Zertifikat verwenden aktivieren, wird der erste im Zertifikat angegebene Subjekt-</p>

Feld	Beschreibung
	<p>Alternativname oder, falls keiner angegeben ist, der Subjektnamen des Zertifikats verwendet.</p> <p>Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe Zertifikate auf Seite 93), 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.</p>
Preshared Key	<p>Geben Sie das mit dem Peer vereinbarte Passwort ein.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer <i>0x</i> am Anfang des Eintrags.</p>

Felder im Menü Schnittstellenrouten

Feld	Beschreibung
IP-Adressenvergabe	<p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Geben Sie eine statische IP-Adresse ein. • <i>Client im IKE-Konfigurationsmodus</i> (Nur für IKEv2): Wählen Sie diese Option, wenn Ihr Gateway als IPsec-Client vom Server eine IP-Adresse erhalten soll. • <i>Server im IKE-Konfigurationsmodus</i>: Wählen Sie diese Option, wenn Ihr Gateway als DHCP-Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten IP-Zuordnungspool entnommen.
Konfigurationsmodus	<p>Nur bei IP-Adressenvergabe = <i>Server im IKE-Konfigurationsmodus</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Pull</i> (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage. • <i>Push</i>: 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	<p>Nur bei IP-Adressenvergabe = <i>Server im IKE-Konfigurationsmodus</i></p> <p>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 <i>Noch nicht definiert</i>.</p>
Standardroute	<p>Nur für IP-Adressenvergabe = <i>Statisch</i> und <i>Client im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressenvergabe = <i>Statisch</i> und <i>Server im IKE-Konfigurationsmodus</i></p> <p>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.</p>
Metrik	<p>Nur für IP-Adressenvergabe = <i>Statisch</i> oder <i>Client im IKE-Konfigurationsmodus</i> und Standardroute = <i>Aktiviert</i></p> <p>Wählen Sie die Priorität der Route aus.</p> <p>Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.</p> <p>Wertebereich von 0 bis 15 . Standardwert ist 1 .</p>
Routeneinträge	<p>Nur für IP-Adressenvergabe = <i>Statisch</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <i>Netzmaske</i>: Netzmaske zu <i>Entfernte IP-Adresse</i>. • <i>Metrik</i>: 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	<p>Nur für IKE (Internet Key Exchange) = IKEv1</p> <p>Legen Sie mithilfe von Hinzufügen einen neuen Filter an.</p>

Zusätzlicher Filter des Datenverkehrs

bintec Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode ist ausschließlich über das Setup Tool konfigurierbar. Mit dem GUI verwenden Sie die Routing-basierte Methode. (Letztere ist zusätzlich auch über das Setup Tool verfügbar.)

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.

The screenshot shows the 'IPSec-Peers' configuration page. At the top, there are tabs for 'IPSec-Peers', 'Phase-1-Profile', 'Phase-2-Profile', 'XAUTH-Profile', 'IP Pools', and 'Optionen'. The main area contains a form for 'Peer-Parameter' with fields for 'Administrativer Status' (Aktiv/Inaktiv), 'Beschreibung' (Peer-2), 'Peer-ID', 'IKE (Intern)', 'Preshared', 'Schnittstelle', 'IP-Adresse', 'Standardprotokoll', 'Lokale IP-Adresse' (0.0.0.0), 'Metrik' (1), and 'Zusätzlicher Filter des Datenverkehrs'. A 'Basisparameter' dialog box is overlaid on the form, containing fields for 'Beschreibung', 'Protokoll' (Beliebig), 'Quell-IP-Adresse/Netzmaske', and 'Ziel-IP-Adresse/Netzmaske'. Below the dialog are buttons for 'Übernehmen' and 'Abbrechen'. At the bottom of the main form are buttons for 'Erweiterte Einstellungen', 'OK', and 'Abbrechen'.

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Protokoll	Wählen Sie ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i> (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quellport	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i>

Feld	Beschreibung
	Geben Sie den Quell-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -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.
Zielport	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i> Geben Sie den Ziel-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -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	<p>Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in VPN->IPSec->Phase-1-Profile als Standard markiert ist • <i>*Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü VPN->IPSec->Phase-1-Profile. • <i><Profilname></i>: Verwendet ein Profil, das im Menü VPN->IPSec->Phase-1-Profile für Phase 1 konfiguriert wurde.
Phase-2-Profil	<p>Wählen Sie ein Profil für die Phase 2 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in VPN->IPSec->Phase-2-Profile als Standard markiert ist • <i>*Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 2 die Proposals 3DES/MD5, AES-128/MD5 und Blow-

Feld	Beschreibung
	<p>fish/MD5 enthält ungeachtet der Proposalauswahl im Menü VPN->IPSec->Phase-2-Profile.</p> <ul style="list-style-type: none"> • <i><Profilname></i>: Verwendet ein Profil, das im Menü VPN->IPSec->Phase-2-Profile für Phase 2 konfiguriert wurde.
XAUTH-Profil	<p>Wählen Sie ein in VPN->IPSec->XAUTH-Profile angelegtes Profil aus, wenn Sie zur Authentifizierung dieses IPSec-Peers XAuth verwenden möchten.</p> <p>Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.</p>
Anzahl erlaubter Verbindungen	<p>Wählen Sie aus, wie viele Benutzer sich mit diesem Peer-Profil verbinden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ein Benutzer</i> (Standardwert): Es kann sich nur ein Peer mit den in diesem Profil definierten Daten verbinden. • <i>Mehrere Benutzer</i>: Es können sich mehrere Peers mit den in diesem Profil definierten Daten verbinden. Bei jeder Verbindungsanfrage mit den in diesem Profil definierten Daten, wird der Peer-Eintrag dupliziert.
Startmodus	<p>Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auf Anforderung</i> (Standardwert): Der Peer wird durch einen Trigger in den aktiven Zustand versetzt. • <i>Immer aktiv</i>: Der Peer ist immer aktiv.

Felder im Menü Erweiterte IP-Optionen

Feld	Beschreibung
Überprüfung der Rückroute	<p>Wählen Sie aus, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer <i>aktiv</i> (aktiv) oder <i>ruhend</i> (ruhend) ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum IPSec-Peer besteht.

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen **bintec**-Geräte den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit IPSec-Callback geschaffen: 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.teldat.de. 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 319 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.

Felder im Menü IPsec-Callback

Feld	Beschreibung
Modus	<p>Wählen Sie den Callback-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): IPsec-Callback ist deaktiviert. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • <i>Passiv</i>: 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. • <i>Aktiv</i>: 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. • <i>Beide</i>: 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	<p>Nur für Modus = <i>Passiv</i> oder <i>Beide</i></p> <p>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.</p>

Feld	Beschreibung
Ausgehende Rufnummer	<p>Nur für Modus = <i>Aktiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.</p>
Eigene IP-Adresse per ISDN/GSM übertragen	<p>Wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Geräts über ISDN übertragen werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Übertragungsmodus	<p>Nur für Eigene IP-Adresse per ISDN/GSM übertragen = aktiviert</p> <p>Wählen Sie aus, in welchem Modus Ihr Gerät versuchen soll, seine IP-Adresse an den Peer zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung des besten Modus</i>: 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.) • <i>Nur D-Kanalmodi automatisch erkennen</i>: Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. • <i>Spezifischen D-Kanalmodus verwenden</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. • <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i>: 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 übertragen. (Dies verursacht Kosten.) • <i>Nur B-Kanalmodus verwenden</i>: Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.
Modus des D-Kanals	<p>Nur für Übertragungsmodus = <i>Spezifischen D-Kanalmodus verwenden</i> oder <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i></p>

Feld	Beschreibung
	<p>Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LLC</i> (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen. • <i>SUBADDR</i> : Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen. • <i>LLC und SUBADDR</i> : Die IP-Adresse wird sowohl in den "LLC" als auch in den "Subaddress Information Elements" übertragen.

17.1.2 Phase-1-Profile

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

IPSec-Peers
Phase-1-Profile
Phase-2-Profile
XAUTH-Profile
IP Pools
Optionen

IKEv1 (Internet Key Exchange, Version 1)

Ansicht pro Seite Filtern in gleich

Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer

Seite: 1

Neues IKEv1-Profil erstellen Neu

IKEv2 (Internet Key Exchange, Version 2)

Ansicht pro Seite Filtern in gleich

Beschreibung	Proposals	Lebensdauer

Seite: 1

Neues IKEv2-Profil erstellen Neu

OK
Abbrechen

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

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

17.1.2.1 Neu

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

IPSec-Peers	Phase-1-Profile	Phase-2-Profile	XAUTH-Profile	IP Pools	Optionen												
Phase-1-Parameter (IKE)																	
Beschreibung	IKE-1																
Proposals	<table border="1"> <thead> <tr> <th>Verschlüsselung</th> <th>Authentifizierung</th> <th>Aktiviert</th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>					Verschlüsselung	Authentifizierung	Aktiviert	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>
Verschlüsselung	Authentifizierung	Aktiviert															
AES	MD5	<input type="checkbox"/>															
AES	MD5	<input type="checkbox"/>															
AES	MD5	<input type="checkbox"/>															
DH-Gruppe	<input type="radio"/> 1 (768 Bit) <input checked="" type="radio"/> 2 (1024 Bit) <input type="radio"/> 5 (1536 Bit)																
Lebensdauer	14400 Sekunden 0 kBytes Lebensdauer																
Authentifizierungsmethode	Preshared Keys																
Modus	<input type="radio"/> Main Modus (ID Protect) <input checked="" type="radio"/> Aggressiv <input type="checkbox"/> Strikt																
Lokaler ID-Typ	Fully Qualified Domain Name (FQDN)																
Lokaler ID-Wert	r4402																
Erweiterte Einstellungen																	
Erreichbarkeitsprüfung	Automatische Erkennung																
Blockzeit	30 Sekunden																
NAT-Traversal	Aktiviert																
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>																	

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

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

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

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, welche die Art der Regel eindeutig identifiziert.
Proposals	<p>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.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> 3DES (Standardwert): 3DES ist eine Erweiterung des DES Al-

Feld	Beschreibung
	<p>gorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird.</p> <ul style="list-style-type: none"> • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. • <i>AES</i>: 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 <i>AES</i> gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • <i>AES-128</i>: 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. • <i>AES-192</i>: 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. • <i>AES-256</i>: 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. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i> (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>SHA1</i> : 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 IP-Sec verwendet. • <i>RipeMD 160</i>: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt. • <i>Tiger192</i>: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus. <p>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 Gesichtspunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.</p>
DH-Gruppe	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Die Diffie-Hellman-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec-Geräten unterstützt wird, steht für "modular exponentiation".</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>2 (1024 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>5 (1536 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	<p>Legen Sie die Lebensdauer für Phase-1-Schlüssel fest.</p> <p>Der Standardwert beträgt gemäß RFC 2407 acht Stunden, das</p>

Feld	Beschreibung
	<p>bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <ul style="list-style-type: none"> • 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 <i>14400</i>. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-1- Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Standardwert ist <i>0</i>. <p>Der Defaultwert lt. RFC wird verwendet, wenn <i>0</i> Sekunden und <i>0</i> KBytes eingetragen werden.</p>
Authentifizierungsmethode	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Preshared Keys wählen. Diese werden bei der Peerkonfiguration im Menü VPN->IPSec->IPSec-Peers konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • <i>DSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert. • <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert. • <i>RSA-Verschlüsselung</i>: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
Lokales Zertifikat	<p>Nur für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur oder RSA-Verschlüsselung</i></p> <p>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.</p>

Feld	Beschreibung
	<p>Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>
Modus	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie den Phase-1-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aggressiv</i> (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. • <i>Main Modus (ID Protect)</i>: 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. <p>Wählen Sie weiterhin aus, ob der gewählte Modus ausschließlich verwendet werden darf (Strikt) oder der Peer auch einen anderen Modus vorschlagen kann.</p>
Lokaler ID-Typ	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie den Typ der lokalen ID aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i>
Lokaler ID-Wert	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für Authentifizierungsmethode = <i>DSA-Signatur</i>, <i>RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i> wird die Option Sub-</p>

Feld	Beschreibung
	<p>jektname aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektname aus Zertifikat verwenden aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet.</p> <p>Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe Zertifikate auf Seite 93), 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.</p>

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
<p>Erreichbarkeitsprüfung</p>	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Methode aus, mit der die Funktionalität der IP-Sec-Verbindung überprüft werden soll.</p> <p>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</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden & Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • <i>Dead Peer Detection</i>: 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. • <i>Dead Peer Detection (Idle)</i>: 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. <p>Nur für Phase-1-Parameter (IKEv2)</p> <p>Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Blockzeit	<p>Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche.</p> <p>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.</p> <p>Standardwert ist 30.</p>

Feld	Beschreibung
NAT-Traversal	<p>NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.</p> <p>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.</p> <p>Nur für <i>IKEv1-Profile</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert): NAT-Traversal ist aktiv. • <i>Deaktiviert</i>: NAT-Traversal ist deaktiviert. • <i>Erzwingen</i>: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. <p>Nur für <i>IKEv2-Profile</i></p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CA-Zertifikate	<p>Nur für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Wenn Sie die Option Folgenden CA-Zertifikaten vertrauen aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen.</p> <p>Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.</p>

17.1.3 Phase-2-Profile

Ebenso wie für Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren.

Im Menü **VPN->IPSec->Phase-2-Profile** wird eine Liste aller konfigurierten IPSec-Phase-2-Profile angezeigt.

[IPSec-Peers](#) | [Phase-1-Profile](#) | [Phase-2-Profile](#) | [XAUTH-Profile](#) | [IP Pools](#) | [Optionen](#)

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los				
Standard	Beschreibung	Proposals	PFS-Gruppe	Lebensdauer
Seite: 1				
<input type="button" value="Neu"/> <input type="button" value="OK"/> <input type="button" value="Abbrechen"/>				

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

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

17.1.3.1 Neu

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

[IPSec-Peers](#) | [Phase-1-Profile](#) | [Phase-2-Profile](#) | [XAUTH-Profile](#) | [IP Pools](#) | [Optionen](#)

Phase-2-Parameter (IPSEC)													
Beschreibung	IPSec-2												
Proposals	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Verschlüsselung</th> <th>Authentifizierung</th> <th>Aktiviert</th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Verschlüsselung	Authentifizierung	Aktiviert	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>
Verschlüsselung	Authentifizierung	Aktiviert											
AES	MD5	<input type="checkbox"/>											
AES	MD5	<input type="checkbox"/>											
AES	MD5	<input type="checkbox"/>											
PFS-Gruppe verwenden	<input checked="" type="checkbox"/> Aktiviert <input type="radio"/> 1 (768 Bit) <input checked="" type="radio"/> 2 (1024 Bit) <input type="radio"/> 5 (1536 Bit)												
Lebensdauer	7200 Sekunden 0 kBytes Schlüssel erneuert erstellen nach 80 % Lebensdauer												
Erweiterte Einstellungen													
IP-Komprimierung	<input type="checkbox"/> Aktiviert												
Erreichbarkeitsprüfung	Automatische Erkennung												
PMTU propagieren	<input checked="" type="checkbox"/> Aktiviert												
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>													

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

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

Felder im Menü Phase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.

Feld	Beschreibung
	Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IP-Sec Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <i>3DES</i> (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. • -- <i>ALLE</i> --: Alle Optionen können verwendet werden. • <i>AES</i>: 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 <i>AES</i> gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • <i>AES-128</i>: 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. • <i>AES-192</i>: 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. • <i>AES-256</i>: 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. • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish an-

Feld	Beschreibung
	<p>gesehen werden.</p> <ul style="list-style-type: none"> • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i> (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • <i>-- ALLE --</i>: Alle Optionen können verwendet werden. • <i>SHA1</i> : 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. <p>Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.</p>
<p>PFS-Gruppe verwenden</p>	<p>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 (<i>Aktiviert</i>), 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.</p> <p>Das Feld hat folgende Optionen:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>2 (1024 Bit)</i> (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>5 (1536 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	<p>Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen.</p> <p>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.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <ul style="list-style-type: none"> • 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. <p>Schlüssel erneut erstellen nach: Legen Sie fest, bei welchem Prozentsatz des Ablaufes der Lebensdauer die Schlüssel der Phase 2 neu erstellt werden.</p> <p>Die eingegebene Prozentzahl wird sowohl auf die Lebensdauer in Sekunden als auch auf die Lebensdauer in kBytes angewendet.</p> <p>Standardwert ist 80 %.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IP-Komprimierung	<p>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</p>

Feld	Beschreibung
	<p>nicht komprimierbaren Daten wird von der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erreichbarkeitsprüfung	<p>Wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden.</p> <p>Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, ist ein bintec-IPSec-Heartbeat implementiert worden. Dieser sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Automatische Erkennung, ob die Gegenstelle ein bintec-Gerät ist. Wenn ja, wird <i>Heartbeats (Senden &Erwarten)</i> (bei Gegenstelle mit bintec) oder <i>Inaktiv</i> (bei Gegenstelle ohne bintec) gesetzt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden &Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.
PMTU propagieren	<p>Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

17.1.4 XAUTH-Profile

Im Menü **XAUTH-Profile** wird eine Liste aller XAuth-Profile angezeigt.

Extended Authentication für IPSec (XAuth) ist eine zusätzliche Authentifizierungsmethode für Benutzer eines IPSec-Tunnels.

Das Gateway kann bei Nutzung von XAuth zwei verschiedene Rollen übernehmen, es kann als Server oder als Client dienen:

- Das Gateway fordert als Server einen Berechtigungsnachweis an.
- Das Gateway weist als Client seine Berechtigung nach.

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Die Berechtigung wird entweder anhand einer Liste oder über einen RADIUS Server geprüft. Bei Verwendung eines Einmalpassworts (One Time Password, OTP) kann die Passwortüberprüfung von einem Token Server übernommen werden (z. B. beim Produkt SecOVID von Kobil), der hinter dem RADIUS Server installiert ist. Wenn über IPSec eine Firmenzentrale mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden. Je nach Zuordnung verschiedener Profile kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter 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 IPSec (Phase 2) beginnt, wird XAuth realisiert.

Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.

17.1.4.1 Neu

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [IP Pools](#) | [Optionen](#)

Basisparameter	
Beschreibung	<input type="text"/>
Rolle	Server ▾
Modus	RADIUS ▾
RADIUS-Server Gruppen-ID	Kein RADIUS-Server für XAUTH konfiguriert

Abb. 125: VPN->IPSec->XAUTH-Profil->Neu

Das Menü VPN->IPSec->XAUTH-Profil->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: <ul style="list-style-type: none"> • <i>Server</i> (Standardwert): Das Gateway fordert einen Berechtigungsnachweis an. • <i>Client</i>: Das Gateway weist seine Berechtigung nach.
Modus	Nur für Rolle = <i>Server</i> Wählen Sie aus, wie die Authentifizierung durchgeführt wird. Mögliche Werte: <ul style="list-style-type: none"> • <i>RADIUS</i> (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. • <i>Lokal</i>: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.
Name	Nur für Rolle = <i>Client</i> 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-Profiles, indem Sie den Authentifizierungsnamen des Clients (Name) und das Authentifizierungspasswort (Passwort) eingeben. Fügen Sie weitere Mitglieder mit Hinzufügen hinzu.

17.1.5 IP Pools

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

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

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

[IPSec-Peers](#)
[Phase-1-Profile](#)
[Phase-2-Profile](#)
[XAUTH-Profile](#)
[IP Pools](#)
[Optionen](#)

Ansicht: 20 pro Seite << >> Filtern in: Keiner > gleich > Los

IP-Poolname	IP-Poolbereich
	- 0.0.0.0

Seite: 1, Objekte: 1 - 1

Hinzufügen
OK
Abbrechen

Abb. 126: VPN->IPSec->IP Pools->Hinzufügen

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

Felder im Menü IP Pools

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

17.1.6 Optionen

[IPSec-Peers](#)
[Phase-1-Profil](#)
[Phase-2-Profil](#)
[XAUTH-Profil](#)
[IP Pools](#)
[Optionen](#)

Globale Optionen	
IPSec aktivieren	<input type="checkbox"/> Aktiviert
Vollständige IPSec-Konfiguration löschen	<input type="button" value="🗑️"/>
IPSec-Debug-Level	Debug <input type="button" value="v"/>
Erweiterte Einstellungen	
IPSec über TCP	<input type="checkbox"/> NCPPath Finder Technologie
Initial Contact Message senden	<input checked="" type="checkbox"/> Aktiviert
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<input type="checkbox"/> Aktiviert
Zero Cookies verwenden	<input checked="" type="checkbox"/> Aktiviert
Größe der Zero Cookies	32 <input type="text"/> Bit
Dynamische RADIUS-Authentifizierung	<input type="checkbox"/> Aktiviert
PKI-Verarbeitungsoptionen	
Zertifikatsanforderungs-Payloads nicht beachten	<input type="checkbox"/> Aktiviert
Zertifikatsanforderungs-Payloads senden	<input checked="" type="checkbox"/> Aktiviert
Zertifikatsketten senden	<input checked="" type="checkbox"/> Aktiviert
CRLs senden	<input type="checkbox"/> Aktiviert
Key Hash Payloads senden	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 127: VPN->IPSec->Optionen

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

Felder im Menü Globale Optionen

Feld	Beschreibung
IPSec aktivieren	<p>Wählen Sie, ob Sie IPSec aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.</p>
Vollständige IPSec-Konfiguration löschen	<p>Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts.</p> <p>Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen.</p> <p>Das Löschen der Konfiguration ist nur möglich mit IPSec aktivieren = nicht aktiviert.</p>
IPSec-Debug-Level	<p>Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Informationen</i> • <i>Debug</i> (Standardwert, niedrigste Priorität) <p>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.</p>

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen **bintec**-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein,

wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	<p>Wählen Sie aus, ob IPSec über TCP verwendet werden soll.</p> <p>IPSec über TCP basiert auf der NCP-Path-Finder-Technologie. Diese Technologie sorgt dafür, dass der Datenverkehr (IKE, ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session eingebettet wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Initial Contact Message senden	<p>Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von <i>aktiv</i> zu <i>inaktiv</i>, <i>ruhend</i> oder <i>blockiert</i> geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zero Cookies verwenden	<p>Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen.</p> <p>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 <i>Aktiviert</i>.</p>
Größe der Zero Cookies	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten und auf</p>

Feld	Beschreibung
	<p>Null gesetzten SPI in Bytes ein.</p> <p>Der Standardwert ist 32.</p>
Dynamische RADIUS-Authentifizierung	<p>Wählen Sie aus, ob die RADIUS-Authentifizierung über IPSec aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	<p>Wählen Sie aus, ob Zertifikatsanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungs-Payloads senden	<p>Wählen Sie aus, ob während IKE (Phase 1) Zertifikatsanforderungen gesendet werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Zertifikatsketten senden	<p>Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.</p>
CRLs senden	<p>Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Key Hash Payloads senden	<p>Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen.</p> <p>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 <i>Aktiviert</i>, um dieses Verhalten zu unterdrücken.</p>

17.2 L2TP

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

Ihr **bintec**-Gerät unterstützt die folgenden zwei Modi:

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

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

17.2.1 Tunnelprofile

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

17.2.1.1 Neu

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

Tunnelprofile Benutzer Optionen

Basisparameter	
Beschreibung	<input type="text" value="L2TP1"/>
Lokaler Hostname	<input type="text"/>
Entfernter Hostname	<input type="text"/>
Passwort	<input type="password" value="••••••••"/>
Parameter des LAC-Modus	
Entfernte IP-Adresse	<input type="text"/>
UDP-Quellport	<input type="checkbox"/> Fest eingestellt
UDP-Zielport	<input type="text" value="1701"/>
Erweiterte Einstellungen	
Lokale IP-Adresse	<input type="text"/>
Hello-Intervall	<input type="text" value="30"/> Sekunden
Minimale Zeit zwischen Versuchen	<input type="text" value="1"/> Sekunden
Maximale Zeit zwischen Versuchen	<input type="text" value="16"/> Sekunden
Maximale Anzahl Wiederholungen	<input type="text" value="5"/>
Sequenznummern der Datenpakete	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie eine Beschreibung für das aktuelle Profil ein.</p> <p>Ihr Gerät benennt die Profile automatisch mit <i>L2TP</i> und nummeriert diese, der Wert kann jedoch geändert werden.</p>
Lokaler Hostname	<p>Geben Sie den Hostnamen für LNS bzw. LAC ein.</p> <ul style="list-style-type: none"> <i>LAC</i>: 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
	<ul style="list-style-type: none"> • <i>LNS</i>: Entspricht dem Wert für Entfernter Hostname der eingehenden Tunnelaufbaumeldung vom LAC.
Entfernter Hostname	<p>Geben Sie den Hostnamen des LNS bzw. LAC ein:</p> <ul style="list-style-type: none"> • <i>LAC</i>: 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 zum entfernten Hostnamen passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. • <i>LNS</i>: Definiert den Lokaler Hostnamen 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	<p>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 Hostnamen 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.</p> <p>Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.</p>

Felder im Menü Parameter des LAC-Modus

Feld	Beschreibung
Entfernte IP-Adresse	<p>Geben Sie die feste IP-Adresse des LNS ein, die als Zieladresse für Verbindungen genutzt wird, die auf diesem Profil aufbauen.</p> <p>Das Ziel muss ein Gerät sein, welches sich wie ein LNS verhalten kann.</p>
UDP-Quellport	<p>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.</p> <p>Standardmäßig ist die Option Fest eingestellt deaktiviert, was</p>

Feld	Beschreibung
	<p>bedeutet, dass den Verbindungen, die dieses Profil nutzen, Ports dynamisch zugeordnet werden.</p> <p>Wenn Sie einen fixen Port eingeben möchten, aktivieren Sie die Option <i>Fest eingestellt</i>. Wenn Sie Probleme mit der Firewall bzw. NAT feststellen, wählen Sie diese Option.</p> <p>Verfügbare Werte sind dann 0 bis 65535.</p>
UDP-Zielport	<p>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.</p> <p>Mögliche Werte sind 0 ... 65535.</p> <p>Der Standardwert ist 1701 (RFC 2661).</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Lokale IP-Adresse	<p>Geben Sie die IP-Adresse ein, die als Quelladresse für alle L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.</p> <p>Falls dieses Feld frei gelassen wird, nutzt Ihr Gerät die IP-Adresse der Schnittstelle, über das der L2TP-Tunnel die entfernte IP-Adresse erreicht.</p>
Hello-Intervall	<p>Geben Sie den Zeitabstand (in Sekunden) zwischen dem Senden von zwei L2TP-HELLO-Meldungen ein. Diese Meldungen dienen dazu, den Tunnel offen zu halten.</p> <p>Verfügbare Werte sind 0 bis 255, der Standardwert ist 30. Der Wert 0 bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.</p>
Minimale Zeit zwischen Versuchen	<p>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.</p> <p>Die Wartezeit wird dynamisch verlängert, bis sie die Maximale Zeit zwischen Versuchen erreicht hat. Verfügbare Werte sind</p>

Feld	Beschreibung
	1 bis 255, der Standardwert ist 1.
Maximale Zeit zwischen Versuchen	<p>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.</p> <p>Verfügbare Werte sind 8 bis 255, der Standardwert ist 16.</p>
Maximale Anzahl Wiederholungen	<p>Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden.</p> <p>Verfügbare Werte sind 8 bis 255, der Standardwert ist 5.</p>
Sequenznummern der Datenpakete	<p>Wählen Sie aus, ob Ihr Gerät für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folge-nummern benutzen soll oder nicht.</p> <p>Die Funktion wird derzeit nicht verwendet.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

17.2.2 Benutzer

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

17.2.2.1 Neu

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

Tunnelprofile Benutzer Optionen

Basisparameter							
Beschreibung	<input type="text"/>						
Verbindungstyp	<input checked="" type="radio"/> LNS <input type="radio"/> LAC						
Benutzername	<input type="text"/>						
Passwort	••••••••						
Immer aktiv	<input type="checkbox"/> Aktiviert						
Timeout bei Inaktivität	<input type="text" value="300"/> Sekunden						
IP-Modus und Routen							
IP-Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse bereitstellen						
Standardroute	<input type="checkbox"/> Aktiviert						
NAT-Eintrag erstellen	<input type="checkbox"/> Aktiviert						
Lokale IP-Adresse	<input type="text"/>						
Routeneinträge	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td>1</td> </tr> </tbody> </table> <input type="button" value="Hinzufügen"/>	Entfernte IP-Adresse	Netzmaske	Metrik	<input type="text"/>	<input type="text"/>	1
Entfernte IP-Adresse	Netzmaske	Metrik					
<input type="text"/>	<input type="text"/>	1					
Erweiterte Einstellungen							
Blockieren nach Verbindungsfehler für	<input type="text" value="300"/> Sekunden						
Authentifizierung	MS-CHAPv2						
Verschlüsselung	<input type="radio"/> Keine <input checked="" type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel						
Komprimierung	<input checked="" type="radio"/> Keine <input type="radio"/> STAC <input type="radio"/> MS-STAC <input type="radio"/> MPPC						
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert						
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert						
IP-Optionen							
OSPF-Modus	<input checked="" type="radio"/> Passiv <input type="radio"/> Aktiv <input type="radio"/> Inaktiv						
Proxy-ARP-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv						
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert						
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen beliebigen Namen ein, um den L2TP-Partner eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.</p>

Feld	Beschreibung
	Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.
Verbindungstyp	<p>Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerkserver (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LNS</i> (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • <i>LAC</i>: 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	<p>Nur für Verbindungstyp = <i>LAC</i></p> <p>Wählen Sie ein im Menü Tunnelprofil erstelltes Profil für die Verbindung zu diesem L2TP-Partner aus.</p>
Benutzername	Geben Sie die Kennung Ihres Geräts ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>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 Nutzdatenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Zur Verfügung stehen Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Short-Hold. Der Standardwert ist 300.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein. • <i>IP-Adresse bereitstellen</i>: Nur für Verbindungstyp = <i>LNS</i> . Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Nur für Verbindungstyp = <i>LAC</i> . Ihr Gerät erhält dynamisch eine IP-Adresse.
IP-Zuordnungspool (IPCP)	<p>Nur für IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>Wählen Sie einen im Menü WAN->Internet + Einwählen->IP Pools konfigurierten IP Pool aus.</p>
Standardroute	<p>Nur für IP-Adressmodus = <i>IP-Adresse abrufen</i> und <i>Statisch</i></p> <p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv .</p>
NAT-Eintrag erstellen	<p>Nur für IP-Adressmodus = <i>IP-Adresse abrufen</i> und <i>Statisch</i></p> <p>Wählen Sie aus, ob Network Address Translation (NAT) für diese Verbindung aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die WAN-IP-Adresse Ihres Geräts ein.</p>
Routeneinträge	<p>Nur für IP-Adressmodus = <i>Statisch</i></p>

Feld	Beschreibung
	Geben Sie Entfernte IP-Adresse und Netzmaske des LANs des L2TP-Partners und die dazugehörige Metrik ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist <i>300</i> .
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>PAP/CHAP/MS-CHAP</i> (Standardwert): Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>PAP</i>: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keine</i>: 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,

Feld	Beschreibung
	<p>sonst kommt keine Verbindung zustande.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> : Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i>(Standardwert): Die MPP-Verschlüsselung V2 mit 128 Bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.
Komprimierung	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird keine Verschlüsselung angewendet. • <i>STAC</i> • <i>MS-STAC</i> • <i>MPPC</i>: Microsoft Point-to-Point Compression
LCP-Erreichbarkeitsprüfung	<p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (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. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>aktiv</i> (aktiv) oder <i>ruhend</i> (ruhend) ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für DNS-Server Primär und Sekundär und WINS-Server Primär und Sekundär vom L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

17.2.3 Optionen

Abb. 130: VPN->L2TP->Optionen

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

Felder im Menü Globale Optionen

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

17.3 PPTP

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

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

Für diesen Vorgang baut das PPTP-Subsystem eine Kontrollverbindung zwischen den Tunnelendpunkten auf. Diese übermittelt Steuerungsdaten, welche die Verbindung zwi-

schen den zwei PPTP-Tunnelendpunkten aufbauen, aufrechterhalten und beenden. Sobald diese Kontrollverbindung aufgebaut ist, überträgt das PPTP die in GRE-Pakete (GRE = Generic Routing Encapsulation) eingepackten Nutzdaten.

17.3.1 PPTP-Tunnel

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

173.1.1 Neu

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

PPTP-Tunnel
Optionen
IP Pools

PPTP Partner Parameter													
Beschreibung	<input type="text"/>												
PPTP-Modus	<input checked="" type="radio"/> PNS <input type="radio"/> Windows-Client-Modus												
Benutzername	<input type="text"/>												
Passwort	••••••••												
Immer aktiv	<input type="checkbox"/> Aktiviert												
Timeout bei Inaktivität	<input type="text" value="300"/> Sekunden												
Entfernte PPTP-IP-Adresse	<input type="text"/>												
IP-Modus und Routen													
IP-Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse bereitstellen												
Standardroute	<input type="checkbox"/> Aktiviert												
NAT-Eintrag erstellen	<input type="checkbox"/> Aktiviert												
Lokale IP-Adresse	<input type="text"/>												
Routeneinträge	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Entfernte IP-Adresse</th> <th style="width: 20%;">Netzmaske</th> <th style="width: 10%;">Metrik</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td style="text-align: center;">1</td> <td style="text-align: center;">▼</td> </tr> <tr> <td colspan="4" style="text-align: center;">Hinzufügen</td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	1	▼	Hinzufügen			
Entfernte IP-Adresse	Netzmaske	Metrik											
<input type="text"/>	<input type="text"/>	1	▼										
Hinzufügen													
Erweiterte Einstellungen													
Blockieren nach Verbindungsfehler für	<input type="text" value="300"/> Sekunden												
Authentifizierung	MS-CHAPv2 ▼												
Verschlüsselung	<input type="radio"/> Keine <input checked="" type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel												
Komprimierung	<input checked="" type="radio"/> Keine <input type="radio"/> STAC <input type="radio"/> MS-STAC <input type="radio"/> MPPC												
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert												
IP-Optionen													
OSPF-Modus	<input checked="" type="radio"/> Passiv <input type="radio"/> Aktiv <input type="radio"/> Inaktiv												
Proxy-ARP-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv												
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert												
PPTP-Callback													
Callback	<input type="checkbox"/> Aktiviert												
OK Abbrechen													

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

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

Felder im Menü **PPTP Partner Parameter**

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen Namen ein, um den Tunnel eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.</p>
PPTP-Modus	<p>Geben Sie die Rollenverteilung der PPTP-Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PNS</i> (Standardwert): Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Servers zu. • <i>Windows-Client-Modus</i>: 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	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutzdatenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Timeout.</p> <p>Der Standardwert ist 300 .</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>
Entfernte PPTP-IP-Adresse	<p>Nur für PPTP-Modus = <i>PNS</i></p> <p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p>
Entfernte PPTP-IP-Adresse / Hostname	<p>Nur für PPTP-Modus = <i>Windows-Client-Modus</i></p> <p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein. • <i>IP-Adresse bereitstellen</i>: Nur für PPTP-Modus = PNS. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Nur für PPTP-Modus = Windows-Client-Modus. Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	<p>Nur bei IP-Adressmodus = Statisch</p> <p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
NAT-Eintrag erstellen	<p>Nur bei IP-Adressmodus = Statisch</p> <p>Wenn eine PPTP-Verbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = Statisch</p> <p>Weisen Sie der PPTP-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.</p>
Routeneinträge	<p>Nur für IP-Adressmodus = Statisch</p> <p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 - 15). Der Standardwert ist 1.
IP-Zuordnungspool (IPCP)	<p>Nur bei PPTP-Modus = PNS, IP-Adressmodus = IP-Adresse bereitstellen</p> <p>Wählen Sie <i>Neu erstellen</i>, um einen neuen IP Pool zu erstellen. Alternativ können Sie hier einen im Menü VPN->PPTP->IP Pools konfigurierten IP-Pool auswählen.</p>
Beschreibung des IP-Zuordnungspools	<p>Nur bei PPTP-Modus = PNS, IP-Adressmodus = IP-Adresse bereitstellen</p> <p>Geben Sie die Bezeichnung des IP-Pools ein.</p>
IP-Adressbereich	<p>Nur bei PPTP-Modus = PNS, IP-Adressmodus = IP-Adresse bereitstellen</p> <p>Geben Sie im ersten Feld die erste IP-Adresse des Bereiches ein.</p> <p>Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Der Standardwert ist 300 .</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen PPTP-Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i>: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication

Feld	Beschreibung
	<p>Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen.</p> <ul style="list-style-type: none"> • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP-Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>(Standardwert): Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i>: Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i> (Standardwert): Die MPP-Verschlüsselung V2 mit 128 Bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.
Komprimierung	<p>Wählen Sie ggf. die Art der Komprimierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird keine Verschlüsselung angewendet. • <i>STAC</i> • <i>MS-STAC</i> • <i>MPPC</i>: Microsoft Point-to-Point Compression
LCP-Erreichbarkeitsprüfung	<p>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</p>

Feld	Beschreibung
	<p>L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellenrouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (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. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen PPTP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen PPTP-Partner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-Partner <i>aktiv</i> (aktiv) oder <i>ruhend</i> (ruhend) ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-Partner <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum PPTP-

Feld	Beschreibung
	Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für DNS-Server Primär und DNS-Server Sekundär vom PPTP-Partner erhalten soll oder diese zum PPTP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü PPTP-Callback

Feld	Beschreibung
Callback	<p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>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.</p>
Eingehende ISDN-Nummer	<p>Nur wenn Callback aktiviert ist.</p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number).</p>
Ausgehende ISDN-Nummer	<p>Nur wenn Callback aktiviert ist.</p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number).</p>

17.3.2 Optionen

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

Globale Optionen	
GRE-Window-Anpassung	<input checked="" type="checkbox"/> Aktiviert
GRE-Window-Größe	<input type="text" value="0"/>
Max. eingehende Kontrollverbindungen über entfernte IP-Adresse	<input type="text" value="1"/>

Abb. 132: VPN->PPTP->Optionen

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

Felder im Menü Globale Optionen

Feld	Beschreibung
GRE-Window-Anpassung	<p>Wählen Sie, ob Sie GRE Window Adaption aktivieren wollen.</p> <p>Diese Anpassung ist erst notwendig, wenn Sie unter Microsoft Windows XP das Service Pack 1 installiert haben. Da Microsoft mit dem SP1 den Bestätigungsalgorithmus innerhalb des GRE-Protokolls geändert hat, muss bei bintec-Geräten die automatische Window-Anpassung für GRE abgeschaltet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
GRE-Window-Größe	<p>Geben Sie die maximale Anzahl an GRE-Paketen ein, die ohne Bestätigung geschickt werden kann.</p> <p>Windows XP verwendet ein höheres initiales Empfangs-Window im GRE, weshalb hier die maximale Sendewindow-Größe auf der teldat-Seite über den Wert GRE-Window-Größe angepasst werden sollte. Mögliche Werte sind 0 bis 256.</p> <p>Standardwert ist 0.</p>
Max. eingehende Kontrollverbindungen über	Geben Sie die maximale Anzahl der Kontrollverbindungen ein.

Feld	Beschreibung
entfernte IP-Adresse	

17.3.3 IP Pools

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

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

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adress-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft Ihr Gerät zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann Ihr Gerät eine IP-Adresse aus einem Adress-Pool zuweisen (falls verfügbar). Bei Adress-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher Verbindungspartner welche Adresse bekommt. Die Adressen werden zunächst einfach der Reihe nach vergeben. Bei einer erneuten Einwahl innerhalb eines Intervalls von einer Stunde wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

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

Abb. 133: VPN->PPTP->IP Pools->Hinzufügen

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

Felder im Menü IP Pools

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

Feld	Beschreibung
	Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.

17.4 GRE

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

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

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

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

17.4.1 GRE-Tunnel

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

174.1.1 Neu

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

GRE-Tunnel

Basisparameter			
Beschreibung	<input type="text"/>		
Lokale GRE-IP-Adresse	<input type="text"/>		
Entfernte GRE-IP-Adresse	<input type="text"/>		
Standardroute	<input type="checkbox"/> Aktiviert		
Lokale IP-Adresse	<input type="text"/>		
Routeneinträge	Entfernte IP-Adresse	Netzmaske	Metrik
	<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>
	<input type="button" value="Hinzufügen"/>		
MTU	<input type="text" value="1500"/>		
Schlüssel verwenden	<input type="checkbox"/> Aktiviert		

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

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

Felder im Menü **Basisparameter**

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein. Wird keine IP-Adresse (dies entspricht der IP-Adresse 0.0.0.0) angegeben, wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse der GRE-Pakete zum GRE-Partner ein.
Standardroute	Wenn Sie die Standardroute aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
Lokale IP-Adresse	Geben Sie hier die (LAN-seitige) IP-Adresse ein, die als Quelladresse Ihres Gerätes für eigene Pakete durch den GRE-Tunnel verwendet werden soll.
Routeneinträge	<p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standard-Netzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 ... 15). Der Standardwert ist 1.
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf.</p> <p>Mögliche Werte sind 1 bis 8192.</p> <p>Der Standardwert ist 1500.</p>
Schlüssel verwenden	<p>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).</p> <p>Mit <i>Aktiviert</i> wird die Kennung aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Schlüsselwert	<p>Nur wenn Schlüssel verwenden aktiviert ist.</p> <p>Geben Sie die GRE-Verbindungskennung ein.</p> <p>Mögliche Werte sind 0 bis 2147483647.</p> <p>Der Standardwert ist 0.</p>

Kapitel 18 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen **bintec** Gateways über eine leistungsfähige Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann nicht nur aufgrund von Quell- und Zieladressen oder Ports, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung zu einem Partner gefällt werden.

Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören. Die Aushandlung einer FTP-Verbindung findet zum Beispiel über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

SIF und andere Sicherheitsfunktionen

bintecs Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der **bintec**-Geräte ein. Systemen wie Network Address Translation (NAT) und IP-Zugriffs-Listen (IPAL) gegenüber ist der Konfigurationsaufwand der SIF vergleichbar einfach.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muss man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, dass die Regeln der SIF generell global angewendet werden, d. h. nicht auf eine Schnittstelle beschränkt sind.

Grundsätzlich werden aber dieselben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske)
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)
- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der ein-

zelen 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).

18.1 Richtlinien

18.1.1 IPv4-Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Im Menü **Firewall->Richtlinien->IPv4-Filterregeln** wird eine Liste aller konfigurierten IPv4-Filterregeln angezeigt.



Abb. 135: **Firewall->Richtlinien->IPv4-Filterregeln**

Mit der Schaltfläche  können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

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

18.1.1.1 Neu

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

[IPv4-Filterregeln](#) | [IPv6-Filterregeln](#) | [QoS](#) | [Optionen](#)

Basisparameter	
Quelle	--- GROUPS ---
Ziel	--- GROUPS ---
Dienst	--- SERVICES ---
Aktion	Zugriff
QoS anwenden	<input type="checkbox"/> Aktiviert

Abb. 136: Firewall->Richtlinien->IPv4-Filterregeln->Neu

Das Menü **Firewall->Richtlinien->IPv4-Filterregeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	<p>Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus.</p> <p>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, für die IPv4 aktiviert ist.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.</p>
Ziel	<p>Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus.</p> <p>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, für die IPv4 aktiviert ist.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfi-</p>

Feld	Beschreibung
	<p>guriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <i>dns</i> • <i>http</i> • <i>nntp</i> • <i>Internet</i> • <i>Netmeeting</i> <p>Weitere Dienste werden in Firewall->Dienste->Diensteliste angelegt.</p> <p>Außerdem stehen die in Firewall->Dienste->Gruppen konfigurierten Dienstgruppen zur Auswahl.</p>
Aktion	<p>Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll.</p> <p>Möglichen Werte:</p> <ul style="list-style-type: none"> • <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • <i>Verweigern</i>: Die Pakete werden abgewiesen. • <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.
QoS anwenden	<p>Nur für Aktion = <i>Zugriff</i></p> <p>Wählen Sie aus, ob Sie QoS für diese Richtlinie mit der in Priorität ausgewählten Priorität aktivieren möchten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Option nicht aktiv.</p> <p>Wenn QoS für diese Richtlinie nicht aktiv ist, beachten Sie, dass auch sendeseitig keine Priorisierung der Daten erfolgen kann.</p> <p>Eine Richtlinie, für die QoS aktiviert wurde, ist auch für die Firewall eingestellt. Beachten Sie daher, dass Datenverkehr, der</p>

Feld	Beschreibung
	nicht ausdrücklich zugelassen wurde, von der Firewall geblockt wird!
Priorität	<p>Nur für QoS anwenden = <i>Aktiviert</i></p> <p>Wählen Sie aus, mit welcher Priorität die von der Richtlinie spezifizierten Daten sendeseitig behandelt werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Keine Priorität. • <i>Low Latency</i>: Low Latency Transmission (LLT), d. h. Behandlung der Daten mit der geringstmöglichen Latenz, z. B. geeignet für VoIP-Daten. • <i>Hoch</i> • <i>Mittel</i> • <i>Niedrig</i>

18.1.2 IPv6-Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Im Menü **Firewall->Richtlinien->IPv6-Filterregeln** wird eine Liste aller konfigurierter IPv6-Filterregeln angezeigt.

Standardmäßig sind die beiden Filterregeln **Sichere Schnittstelle** und **Unsichere Schnittstelle** angelegt. Diese definieren die **Sicherheitsrichtlinie** *Sicher* bzw. *Unsicher* und können nicht editiert oder gelöscht werden.

Falls Sie die **Sicherheitsrichtlinie** *Sicher* verwenden, werden alle Datenpakete akzeptiert. Sie können nun zusätzliche Filterregeln definieren, die bestimmte Pakete verwerfen. Auf die gleiche Weise können Sie für die Einstellung *Unsicher* ausgewählte Datenpakete

freigegeben.

Datenpakete, die das Neighbour Discovery Protocol verwenden, sind grundsätzlich erlaubt, auch für die Filterregel *Unsicher*.

[IPv4-Filterregeln](#) [IPv6-Filterregeln](#) [QoS](#) [Optionen](#)

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los

Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv			
1	Sichere Schnittstelle	Beliebig	beliebig	Zugriff	<input checked="" type="checkbox"/> Aktiviert			
2	Unsichere Schnittstelle	Beliebig	beliebig	Verweigern	<input checked="" type="checkbox"/> Aktiviert			

Seite: 1

Neu
OK
Abbrechen

Abb. 137: Firewall->Richtlinien->IPv6-Filterregeln

Mit der Schaltfläche  können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

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

18.1.2.1 Neu

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

[IPv4-Filterregeln](#) [IPv6-Filterregeln](#) [QoS](#) [Optionen](#)

Basisparameter

Quelle	--- GROUPS ---
Ziel	--- GROUPS ---
Dienst	--- SERVICES ---
Aktion	Zugriff

OK
Abbrechen

Abb. 138: Firewall->Richtlinien->IPv6-Filterregeln->Neu

Das Menü **Firewall->Richtlinien->IPv6-Filterregeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	<p>Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus.</p> <p>In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->IPv6-Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl, für die IPv6 aktiviert ist.</p>
Ziel	<p>Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus.</p> <p>In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->IPv6-Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl, für die IPv6 aktiviert ist.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <i>dns</i> • <i>http</i> • <i>nntp</i> <p>Weitere Dienste werden in Firewall->Dienste->Diensteliste angelegt.</p> <p>Außerdem stehen die in Firewall->Dienste->Gruppen konfigurierten Dienstgruppen zur Auswahl.</p>
Aktion	<p>Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend

Feld	Beschreibung
	<p>den Angaben weitergeleitet.</p> <ul style="list-style-type: none"> • <i>Verweigern</i> : Die Pakete werden abgewiesen. • <i>Zurückweisen</i> : Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

18.1.3 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.

18.1.3.1 Neu

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

Abb. 139: **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	<p>Wählen Sie aus, ob Sie für die gewählte Schnittstelle das Bandbreitenmanagement aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Bandbreite angeben	<p>Nur für Traffic Shaping = <i>Aktiviert</i></p> <p>Geben Sie die maximal zur Verfügung stehende Bandbreite in kBit/s für die gewählte Schnittstelle ein.</p>
Filterregeln	<p>Dieses Feld enthält eine Liste aller konfigurierten Firewall-Richtlinien, für die QoS aktiviert wurde (QoS anwenden = <i>Aktiviert</i>). Für jeden Listeneintrag stehen folgende Optionen zur Verfügung:</p> <ul style="list-style-type: none"> • Verwenden: Wählen Sie aus, ob dieser Eintrag der QoS-Schnittstelle zugeordnet werden soll. Standardmäßig ist diese Option nicht aktiv. • Bandbreite: Geben Sie die maximal zur Verfügung stehende Bandbreite in Bit/s für den unter Dienst genannten Dienst ein. Standardmäßig ist 0 eingetragen. • Fest: Wählen Sie aus, ob eine längerfristige Überschreitung der in Bandbreite definierten Bandbreite zulässig ist. Die Aktivierung dieses Feldes schließt eine solche Überschreitung aus. Ist die Option deaktiviert, ist die Überschreitung zulässig und die übersteigende Datenrate wird gemäß der in der entsprechenden Firewall-Richtlinie definierten Priorität behandelt. Standardmäßig ist diese Option nicht aktiv.

18.1.4 Optionen

In diesem Menü können Sie die Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wieviel Sekunden Inaktivität eine Sitzung beendet werden soll.

IPv4-Filterregeln
IPv6-Filterregeln
QoS
Optionen

Globale Firewall-Optionen	
Firewall Status	<input checked="" type="checkbox"/> Aktiviert
Protokollierte Aktionen	Alle ▼
Vollständige Filterung	<input checked="" type="checkbox"/> Aktivieren
Sitzungstimer	
UDP-Inaktivität	<input type="text" value="180"/> Sekunden
TCP-Inaktivität	<input type="text" value="3600"/> Sekunden
PPTP-Inaktivität	<input type="text" value="86400"/> Sekunden
Andere Inaktivität	<input type="text" value="30"/> Sekunden

OK
Abbrechen

Abb. 140: Firewall->Richtlinien->Optionen

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

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Firewall Status	<p>Aktivieren oder deaktivieren Sie die Firewall-Funktion.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierte Aktionen	<p>Wählen Sie den Firewall-Syslog-Level aus.</p> <p>Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Alle Firewall-Aktivitäten werden angezeigt. • <i>Verweigern</i> : Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion". • <i>Annehmen</i> : Nur Accept-Ereignisse werden angezeigt. • <i>Keine</i> : Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige Filterung	<p>Hier legen Sie fest, ob nur Pakete gefiltert werden sollen, die an eine andere Schnittstelle gesendet werden als die, welche die Verbindung erzeugt hat.</p>

Feld	Beschreibung
	Mit <i>Aktivieren</i> 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 <i>30</i> bis <i>86400</i> . Der Standardwert ist <i>180</i> .
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 <i>30</i> bis <i>86400</i> . Der Standardwert ist <i>3600</i> .
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 <i>30</i> bis <i>86400</i> . Der Standardwert ist <i>86400</i> .
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 <i>30</i> bis <i>86400</i> . Der Standardwert ist <i>30</i> .

18.2 Schnittstellen

18.2.1 IPv4-Gruppen

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

Sie können die Schnittstellen Ihres Geräts zu Gruppen zusammenfassen. Dieses verein-

facht die Konfiguration von Firewall-Regeln.

18.2.1.1 Neu

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

Basisparameter											
Beschreibung	<input type="text"/>										
Mitglieder	<table border="1"> <thead> <tr> <th>Schnittstelle</th> <th>Auswahl</th> </tr> </thead> <tbody> <tr> <td>LOCAL</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LOCAL</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-0</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-4</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Schnittstelle	Auswahl	LOCAL	<input type="checkbox"/>	LOCAL	<input type="checkbox"/>	LAN_EN1-0	<input type="checkbox"/>	LAN_EN1-4	<input type="checkbox"/>
Schnittstelle	Auswahl										
LOCAL	<input type="checkbox"/>										
LOCAL	<input type="checkbox"/>										
LAN_EN1-0	<input type="checkbox"/>										
LAN_EN1-4	<input type="checkbox"/>										

Abb. 141: Firewall->Schnittstellen->IPv4-Gruppen->Neu

Das Menü **Firewall->Schnittstellen->IPv4-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

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

18.2.2 IPv6-Gruppen

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

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

18.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Schnittstellen-Gruppen einzurichten.

IPv4-Gruppen
IPv6-Gruppen

Basisparameter							
Beschreibung	<input style="width: 90%;" type="text"/>						
Mitglieder	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Schnittstelle</th> <th style="width: 50%;">Auswahl</th> </tr> </thead> <tbody> <tr> <td>LAN_EN1-0-1</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-0-1</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>	Schnittstelle	Auswahl	LAN_EN1-0-1	<input type="checkbox"/>	LAN_EN1-0-1	<input type="checkbox"/>
Schnittstelle	Auswahl						
LAN_EN1-0-1	<input type="checkbox"/>						
LAN_EN1-0-1	<input type="checkbox"/>						
OK Abbrechen							

Abb. 142: Firewall->Schnittstellen->IPv6-Gruppen->Neu

Das Menü **Firewall->Schnittstellen->IPv6-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv6-Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

18.3 Adressen

18.3.1 Adressliste

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

18.3.1.1 Neu

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

Adressliste Gruppen

Basisparameter	
Beschreibung	<input type="text"/>
IPv4	<input checked="" type="checkbox"/> Aktiviert
Adresstyp	<input checked="" type="radio"/> Adresse/Subnetz <input type="radio"/> Adressbereich
Adresse/Subnetz	<input type="text"/> / <input type="text" value="255.255.255.0"/>
IPv6	<input checked="" type="checkbox"/> Aktiviert
Adresse/Präfix	<input type="text"/> / <input type="text" value="128"/>

OK Abbrechen

Abb. 143: 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.
IPv4	Erlaubt die Konfiguration von IPv4-Adresslisten. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Adresstyp	Nur für IPv4 = Aktiviert Wählen Sie aus, welche Art von Adresse Sie angeben wollen. Mögliche Werte: <ul style="list-style-type: none"> <i>Adresse/Subnetz</i> (Standardwert): Sie geben eine IP-Adresse mit Subnetzmaske ein. <i>Adressbereich</i>: Sie geben einen IP-Adressbereich mit Anfangs- und Endadresse ein.
Adresse/Subnetz	Nur für IPv4 = Aktiviert und Adresstyp = Adresse/Subnetz Geben Sie die IP-Adresse des Hosts oder eine Netzwerk-Adresse und die zugehörige Netzmaske ein. Standardwert ist jeweils <i>0.0.0.0</i> .

Feld	Beschreibung
Adressbereich	Nur für IPv4 = <i>Aktiviert</i> und Adresstyp = <i>Adressbereich</i> Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein.
IPv6	Erlaubt die Konfiguration von IPv6-Adresslisten. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Adresse/Präfix	Nur für IPv6 = <i>Aktiviert</i> Geben Sie die IPv6-Adresse und das zugehörige Präfix ein.

18.3.2 Gruppen

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

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

18.3.2.1 Neu

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

Abb. 144: **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.
IP-Version	<p>Wählen Sie die verwendete IP-Version aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • IPv4 • IPv6 <p>Standardmäßig ist IPv4 ausgewählt.</p>
Auswahl	Wählen Sie aus den zur Verfügung stehenden Adressen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

18.4 Dienste

18.4.1 Diensteliste

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

18.4.1.1 Neu

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

Diensteliste Gruppen

Basisparameter	
Beschreibung	<input type="text"/>
Protokoll	Beliebig ▼

OK Abbrechen

Abb. 145: **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	<p>Nur für Protokoll = <i>TCP</i>, <i>UDP/TCP</i> oder <i>UDP</i></p> <p>Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll.</p> <p>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.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>.</p>
Quellportbereich	<p>Nur für Protokoll = <i>TCP</i>, <i>UDP/TCP</i> oder <i>UDP</i></p> <p>Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port an.</p> <p>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.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Das Feld Typ gibt die Klasse der ICMP-Nachrichten an, das Feld Code spezifiziert die Art der Nachricht genauer.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Echo Reply</i> • <i>Destination Unreachable</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Source Quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time Exceeded</i> • <i>Parameter Problem</i> • <i>Timestamp</i> • <i>Timestamp Reply</i> • <i>Information Request</i> • <i>Information Reply</i> • <i>Address Mask Request</i> • <i>Address Mask Reply</i>
Code	<p>Nur für Typ = <i>Destination unreachable</i> stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig (Standardwert)</i> • <i>Net Unreachable</i> • <i>Host Unreachable</i> • <i>Protocol Unreachable</i> • <i>Port Unreachable</i> • <i>Fragmentation Needed</i> • <i>Communication with Destination Network is Administratively Prohibited</i> • <i>Communication with Destination Host is Administratively Prohibited</i>

18.4.2 Gruppen

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

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

18.4.2.1 Neu

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

Diensteliste Gruppen

Basisparameter																																															
Beschreibung	<input style="width: 100%;" type="text"/>																																														
Mitglieder	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Dienst</th> <th style="text-align: left;">Auswahl</th> </tr> </thead> <tbody> <tr><td>activity</td><td><input type="checkbox"/></td></tr> <tr><td>any</td><td><input type="checkbox"/></td></tr> <tr><td>apple-gt</td><td><input type="checkbox"/></td></tr> <tr><td>auth</td><td><input type="checkbox"/></td></tr> <tr><td>chargen</td><td><input type="checkbox"/></td></tr> <tr><td>clients_1</td><td><input type="checkbox"/></td></tr> <tr><td>clients_2</td><td><input type="checkbox"/></td></tr> <tr><td>daytime</td><td><input type="checkbox"/></td></tr> <tr><td>dhcp</td><td><input type="checkbox"/></td></tr> <tr><td>discard</td><td><input type="checkbox"/></td></tr> <tr><td>dns</td><td><input type="checkbox"/></td></tr> <tr><td>echo</td><td><input type="checkbox"/></td></tr> <tr><td>exec</td><td><input type="checkbox"/></td></tr> <tr><td>finger</td><td><input type="checkbox"/></td></tr> <tr><td>ftp</td><td><input type="checkbox"/></td></tr> <tr><td>unpriv</td><td><input type="checkbox"/></td></tr> <tr><td>ups</td><td><input type="checkbox"/></td></tr> <tr><td>uucp-path</td><td><input type="checkbox"/></td></tr> <tr><td>who</td><td><input type="checkbox"/></td></tr> <tr><td>whois</td><td><input type="checkbox"/></td></tr> <tr><td>wins</td><td><input type="checkbox"/></td></tr> <tr><td>x400</td><td><input type="checkbox"/></td></tr> </tbody> </table>	Dienst	Auswahl	activity	<input type="checkbox"/>	any	<input type="checkbox"/>	apple-gt	<input type="checkbox"/>	auth	<input type="checkbox"/>	chargen	<input type="checkbox"/>	clients_1	<input type="checkbox"/>	clients_2	<input type="checkbox"/>	daytime	<input type="checkbox"/>	dhcp	<input type="checkbox"/>	discard	<input type="checkbox"/>	dns	<input type="checkbox"/>	echo	<input type="checkbox"/>	exec	<input type="checkbox"/>	finger	<input type="checkbox"/>	ftp	<input type="checkbox"/>	unpriv	<input type="checkbox"/>	ups	<input type="checkbox"/>	uucp-path	<input type="checkbox"/>	who	<input type="checkbox"/>	whois	<input type="checkbox"/>	wins	<input type="checkbox"/>	x400	<input type="checkbox"/>
Dienst	Auswahl																																														
activity	<input type="checkbox"/>																																														
any	<input type="checkbox"/>																																														
apple-gt	<input type="checkbox"/>																																														
auth	<input type="checkbox"/>																																														
chargen	<input type="checkbox"/>																																														
clients_1	<input type="checkbox"/>																																														
clients_2	<input type="checkbox"/>																																														
daytime	<input type="checkbox"/>																																														
dhcp	<input type="checkbox"/>																																														
discard	<input type="checkbox"/>																																														
dns	<input type="checkbox"/>																																														
echo	<input type="checkbox"/>																																														
exec	<input type="checkbox"/>																																														
finger	<input type="checkbox"/>																																														
ftp	<input type="checkbox"/>																																														
unpriv	<input type="checkbox"/>																																														
ups	<input type="checkbox"/>																																														
uucp-path	<input type="checkbox"/>																																														
who	<input type="checkbox"/>																																														
whois	<input type="checkbox"/>																																														
wins	<input type="checkbox"/>																																														
x400	<input type="checkbox"/>																																														
OK Abbrechen																																															

Abb. 146: 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

Feld	Beschreibung
	die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

Kapitel 19 VoIP

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

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

19.1 SIP

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

19.1.1 Optionen

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

Optionen

Basisparameter	
SIP-Proxy	<input type="checkbox"/> Aktiviert
SIP Port	5060
SIP-Aufrufe priorisieren	<input type="checkbox"/> Aktiviert

Abb. 147: **VoIP->SIP->Optionen**

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

Felder im Menü Basisparameter

Feld	Beschreibung
SIP-Proxy	Wählen Sie, ob Sie den SIP-Proxy aktivieren wollen. Mit <i>Aktiviert</i> wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
SIP Port	<p>Geben Sie den Port ein, der vom Proxy überwacht werden soll.</p> <p>Pro Ziel-Port, zu dem sich VoIP Clients aus dem LAN verbinden können, müssen Sie einen Proxy anlegen.</p> <p>Die Ports können Provider-spezifisch sein.</p> <p>Standardwert ist <i>5060</i>.</p>
SIP-Aufrufe priorisieren	<p>Wählen Sie, ob Sie SIP-Aufrufe priorisieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Kapitel 20 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- Zugriffsbeschränkung auf das Internet (Web-Filter)
- Zuordnung von eingehenden und ausgehenden Daten- und Sprachrufen zu autorisierten Benutzern (CAPI-Server)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Schutz des Benutzer-LAN (Diebstahlsicherung)
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)
- Bereitstellung öffentlicher Internetzugänge (Hotspot).

20.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste->DNS->DNS-Server->Neu** werden die IP-Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der 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 Anfra-

ge sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache Ihres Geräts aufgenommen.

20.1.1 Globale Einstellungen

Globale Einstellungen		DNS-Server	Statische Hosts	Domänenweiterleitung	Cache	Statistik
Basisparameter						
Domänenname	<input type="text"/>					
WINS-Server	Primär	<input type="text" value="0.0.0.0"/>				
	Sekundär	<input type="text" value="0.0.0.0"/>				
Erweiterte Einstellungen						
Positiver Cache	<input checked="" type="checkbox"/> Aktiviert					
Negativer Cache	<input checked="" type="checkbox"/> Aktiviert					
Cache-Größe	<input type="text" value="100"/>	Einträge				
Maximale TTL für positive Cacheeinträge	<input type="text" value="86400"/>	Sekunden				
Maximale TTL für negative Cacheeinträge	<input type="text" value="300"/>	Sekunden				
Alternative Schnittstelle, um DNS-Server zu erhalten	Automatisch <input type="button" value="v"/>					
Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse						
Als DHCP-Server	<input type="radio"/> Keine <input checked="" type="radio"/> Eigene IP-Adresse <input type="radio"/> DNS-Einstellung					
Als IPCP-Server	<input type="radio"/> Keine <input type="radio"/> Eigene IP-Adresse <input checked="" type="radio"/> DNS-Einstellung					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>						

Abb. 148: 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	Geben Sie die IP-Adresse des ersten und, falls erforderlich, des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.
Primär	
Sekundär	

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	<p>Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Negativer Cache	<p>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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Cache-Größe	<p>Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein.</p> <p>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 heruntersgesetzt, 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.</p> <p>Mögliche Werte: <i>0 .. 1000</i>.</p> <p>Standardwert ist <i>100</i>.</p>
Maximale TTL für positive Cacheeinträge	<p>Geben Sie den Wert ein, auf den die TTL für einen positiven dynamischen DNS-Eintrag im Cache gesetzt werden soll, wenn dessen TTL <i>0</i> ist oder dessen TTL den Wert für Maximale TTL für positive Cacheeinträge überschreitet.</p> <p>Standardwert ist <i>86400</i>.</p>
Maximale TTL für negative Cacheeinträge	<p>Geben Sie den Wert ein, auf den die TTL bei einem negativen dynamischen Eintrag im Cache gesetzt werden soll.</p> <p>Standardwert ist <i>86400</i>.</p>

Feld	Beschreibung
Alternative Schnittstelle, um DNS-Server zu erhalten	<p>Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.</p> <p>Standardwert ist <i>Automatisch</i>, d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.</p>

Felder im Menü Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse

Feld	Beschreibung
Als DHCP-Server	<p>Wählen Sie aus, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn Ihr Gerät als DHCP-Server genutzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> : Es wird keine Name-Server-Adresse übermittelt. • <i>Eigene IP-Adresse</i> (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • <i>DNS-Einstellung</i> : Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> : Es wird keine Name-Server-Adresse übermittelt. • <i>Eigene IP-Adresse</i> : Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • <i>DNS-Einstellung</i> (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

20.1.2 DNS-Server

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

20.1.2.1 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.

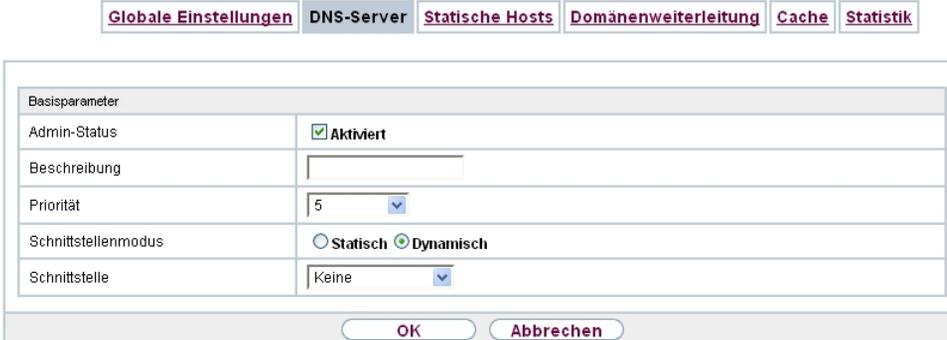


Abb. 149: Lokale Dienste->DNS->DNS-Server->Neu

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 <i>Aktiviert</i> 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
	<p>Priorität, wenn die Schnittstelle im Zustand "up" ist.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 9 (niedrigste Priorität).</p> <p>Standardwert ist 5 .</p>
Schnittstellenmodus	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> • <i>Dynamisch</i> (Standardwert)
Schnittstelle	<p>Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll.</p> <p>Bei Schnittstellenmodus = <i>Dynamisch</i></p> <p>Mit der Einstellung <i>Keine</i> wird ein globaler DNS-Server angelegt.</p> <p>Bei Schnittstellenmodus = <i>Statisch</i></p> <p>Mit der Einstellung <i>Beliebig</i> wird ein DNS-Server für alle Schnittstellen konfiguriert.</p>
Primärer DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie die IP-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie optional die IP-Adresse eines alternativen Name-Servers ein.</p>

20.1.3 Statische Hosts

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

20.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

Basisparameter	
DNS-Hostname	<input type="text"/>
Antwort	Positiv <input type="button" value="v"/>
IP-Adresse	0.0.0.0
TTL	86400 <input type="text"/> Sekunden

Abb. 150: 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	<p>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.</p> <p>Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.teldat.de.</p> <p>Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK "<Name.>" ergänzt.</p> <p>Einträge mit Leerzeichen sind nicht erlaubt.</p>
Antwort	<p>Wählen Sie die Art der Antwort auf DNS-Anfragen zu diesem Eintrag aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Negativ</i>: Eine DNS-Anfrage nach DNS-Hostname wird negativ beantwortet. • <i>Positiv</i> (Standardwert): Eine DNS-Anfrage nach DNS-Hostname wird mit der dazugehörigen IP-Adresse beantwortet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Keine</i> : Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IP-Adresse	<p>Nur bei Antwort = <i>Positiv</i></p> <p>Geben Sie die IP-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>
TTL	<p>Geben Sie die Gültigkeitsdauer der Zuordnung von DNS-Hostname zu IP-Adresse in Sekunden ein (nur relevant bei Antwort = <i>Positiv</i>), die anfragenden Hosts übermittelt wird.</p> <p>Standardwert ist <i>86400</i> (= 24 h).</p>

20.1.4 Domänenweiterleitung

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

20.1.4.1 Neu

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

Abb. 151: **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
	<p>werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Host</i> (Standardwert) • <i>Domäne</i>
Host	<p>Nur für Weiterleiten = <i>Host</i></p> <p>Geben Sie den Namen des Hosts ein, der weitergeleitet werden soll.</p> <p>Der Eintrag kann auch mit dem Wildcard * beginnen, z. B. *.teldat.de. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK " <Default Domain>." ergänzt.</p>
Domäne	<p>Nur für Weiterleiten = <i>Domäne</i></p> <p>Geben Sie den Namen der Domäne ein, die weitergeleitet werden soll.</p> <p>Der Eintrag kann auch mit dem Wildcard * beginnen, z. B. *.teldat.de. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK " <Default Domain>." ergänzt.</p>
Weiterleiten an	<p>Wählen Sie aus, wohin Anfragen an den in Host bzw. Domäne definierten Namen weitergeleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnittstelle</i> (Standardwert): Die Anfrage wird an die definierte Schnittstelle weitergeleitet. • <i>DNS-Server</i>: Die Anfrage wird an den definierten DNS-Server weitergeleitet.
Schnittstelle	<p>Nur für Weiterleiten an = <i>Schnittstelle</i></p> <p>Wählen Sie die Schnittstelle aus, über die Anfragen für die definierte Domäne eingehen und an den DNS-Server weitergeleitet werden sollen.</p>
DNS-Server	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie IP-Adresse des primären und sekundären DNS-</p>

Feld	Beschreibung
	Servers ein.

20.1.5 Cache

Im Menü **Lokale Dienste->DNS->Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

Automatisches Aktualisierungsintervall 60 Sekunden **Übernehmen**

Ansicht 20 pro Seite << >> Filtern in Keiner gleich **Los**

Beschreibung	IP-Adresse	Antwort	TTL	Referenzzähler	Alle auswählen / Alle deaktivieren	Als statisch festlegen
Seite: 1						

OK **Abbrechen**

Abb. 152: **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.

20.1.6 Statistik

Globale Einstellungen	DNS-Server	Statische Hosts	Domänenweiterleitung	Cache	Statistik
---------------------------------------	----------------------------	---------------------------------	--------------------------------------	-----------------------	---------------------------

Automatisches Aktualisierungsintervall	60	Sekunden	Übernehmen
DNS-Statistiken			
Empfangene DNS-Pakete	0		
Ungültige DNS-Pakete	0		
DNS-Anfragen	0		
Cache-Treffer	0		
Weitergeleitete Anfragen	0		
Cache-Trefferrate (%)	0		
Erfolgreich beantwortete Anfragen	0		
Serverfehler	0		

Abb. 153: 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.

20.2 HTTPS

Die Benutzeroberfläche Ihres Geräts können Sie von jedem PC aus mit einem aktuellen Web-Browser auch über eine HTTPS-Verbindung bedienen.

HTTPS (HyperText Transfer Protocol Secure) ist hierbei das Verfahren, um zwischen dem Browser, der zur Konfiguration verwendet wird, und dem Gerät eine verschlüsselte und authentifizierte Verbindung mittels SSL aufzubauen.

20.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

The screenshot shows a configuration window titled "HTTPS-Server". Inside, there is a section labeled "HTTPS-Parameter" containing two input fields. The first field, "HTTPS-TCP-Port", has the value "443" entered. The second field, "Lokales Zertifikat", is a dropdown menu currently set to "Intern". Below the form are two buttons: "Übernehmen" (Accept) and "Abbrechen" (Cancel).

Abb. 154: 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: <ul style="list-style-type: none"> <i>Intern</i> (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möch-

Feld	Beschreibung
	ten. <ul style="list-style-type: none"> • <i><Zertifikatsname></i>: Wählen Sie ein unter Systemverwaltung->Zertifikate->Zertifikatsliste eingetragenes Zertifikat aus.

20.3 DynDNS-Client

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Hostnamens bei einem DynDNS-Provider
- Konfiguration Ihres Geräts

Registrierung

Bei der Registrierung des Hostnamens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Hostname für Ihr Gerät ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt für Sie 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.

20.3.1 DynDNS-Aktualisierung

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

20.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

DynDNS-Aktualisierung DynDNS-Provider

Basisparameter	
Hostname	<input type="text"/>
Schnittstelle	Eine auswählen ▾
Benutzername	<input type="text"/>
Passwort	••••••••
Provider	dyndns ▾
Aktualisierung aktivieren	<input type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Mail-Exchanger (MX)	<input type="text"/>
Wildcard	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 155: 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	<p>Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind.</p> <p>Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden.</p> <p>Weitere DynDNS-Provider können im Menü Lokale</p>

Feld	Beschreibung
	<p>DynDNS-Client->DynDNS-Provider konfiguriert werden.</p> <p>Standardwert ist <i>DynDNS</i> .</p>
Aktualisierung aktivieren	<p>Wählen Sie aus, ob der hier konfigurierte DynDNS-Eintrag aktiviert werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Mail-Exchanger (MX)	<p>Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll.</p> <p>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.</p>
Wildcard	<p>Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von Hostname zur aktuellen IP-Adresse von Schnittstelle aktiviert werden soll (Erweiterte Namensauflösung).</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

20.3.2 DynDNS-Provider

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

20.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

DynDNS-Aktualisierung **DynDNS-Provider**

Basisparameter	
Providername	<input type="text"/>
Server	<input type="text"/>
Aktualisierungspfad	<input type="text"/>
Port	<input type="text" value="80"/>
Protokoll	<input type="text" value="DynDNS"/> ▼
Aktualisierungsintervall	<input type="text" value="300"/> Sekunden

Abb. 156: 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 <i>80</i> .
Protokoll	Wählen Sie eines der implementierten Protokolle aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>DynDNS</i>(Standardwert) • <i>Static DynDNS</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>ODS</i> • <i>HN</i> • <i>DYNS</i> • <i>GnuDIP-HTML</i> • <i>GnuDIP-TCP</i> • <i>Custom DynDNS</i> • <i>DnsExit</i>
Aktualisierungsintervall	<p>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.</p> <p>Standardwert ist <i>300</i> Sekunden.</p>

20.4 DHCP-Server

Sie können Ihr Gerät als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) konfigurieren.

Jeder Rechner in Ihrem LAN benötigt, wie auch Ihr Gerät, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie Ihr Gerät als DHCP-Server einrichten, vergibt es anfragenden Rechnern im LAN automatisch IP-Adressen aus einem definierten IP-Adress-Pool.

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 Teldat 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.

20.4.1 DHCP Pool

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste->DHCP-Server->DHCP Pool** wird eine Liste aller konfigurierter IP-Adresspools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. deaktivieren.

20.4.1.1 Bearbeiten oder Neu

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

DHCP Pool
IP/MAC-Bindung
DHCP-Relay-Einstellungen

Basisparameter					
IP-Poolname	<input type="text"/>				
Schnittstelle	Eine auswählen ▼				
IP-Adressbereich	<input type="text"/> - <input type="text"/>				
Pool-Verwendung	Lokal ▼				
Erweiterte Einstellungen:					
Gateway	Router als Gateway verwenden ▼				
Lease Time	120 Minuten				
DHCP-Optionen	<table border="1" style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr> <th style="width: 50%;">Option</th> <th>Wert</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">Hinzufügen</td> </tr> </tbody> </table>	Option	Wert	Hinzufügen	
Option	Wert				
Hinzufügen					
OK Abbrechen					

Abb. 157: **Lokale Dienste->DHCP-Server->DHCP Pool->Neu**

Das Menü **Lokale Dienste->DHCP-Server->DHCP Pool->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
Schnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die in IP-Adressbereich definierten Adressen an anfragende DHCP-Clients vergeben werden.</p> <p>Wenn eine DHCP-Anfrage über diese Schnittstelle eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.</p>

Feld	Beschreibung
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
Pool-Verwendung	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal</i> (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet. • <i>Relais</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetzen verwendet. • <i>Lokal/Relais</i>: 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	<p>Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Router als Gateway verwenden</i> (Standardwert): Hier wird die für die Schnittstelle definierte IP-Adresse übertragen. • <i>Kein Gateway</i>: Hier wird keine IP-Adresse übermittelt. • <i>Angeben</i>: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	<p>Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll.</p> <p>Nachdem Lease Time abgelaufen ist, kann die Adresse durch den Server neu vergeben werden.</p> <p>Standardwert ist <i>120</i>.</p>
DHCP-Optionen	Geben Sie an, welche zusätzlichen Daten dem DHCP Client

Feld	Beschreibung
	<p>weitergegeben werden sollen.</p> <p>Mögliche Werte für Option:</p> <ul style="list-style-type: none"> • <i>Zeitserver</i> (Standardwert): Geben Sie die IP-Adresse des Zeitserver ein, die dem Client übermittelt werden soll. • <i>DNS-Server</i>: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • <i>DNS-Domänennamen</i>: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • <i>WINS/NBNS-Server</i>: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • <i>WINS/NBT Node Type</i>: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • <i>TFTP-Server</i>: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • <i>CAPWAP Controller</i>: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • <i>URL (Provisionierungsserver)</i>: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. <p>Verwenden Sie diese Option, um anfragenden elmeg-IP1x0-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form <code>http://<IP-Adresse des Provisionierungsservers>/eg_prov</code> haben.</p> <ul style="list-style-type: none"> • <i>Herstellergruppe</i> (Vendor Specific Information): Mit dieser Option können Sie dem Client in einem beliebigen Text-String ggf. herstellerepezifische Informationen übermitteln. <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche Hinzufügen ein.</p>

20.4.2 IP/MAC-Bindung

Im Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus

einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.



Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste->DHCP-Server->DHCP Pool** IP-Adressbereiche konfiguriert sind.

20.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

DHCP Pool
IP/MAC-Bindung
DHCP-Relay-Einstellungen

Basisparameter	
Beschreibung	<input type="text"/>
IP-Adresse	<input type="text"/>
MAC-Adresse	<input type="text"/>

OK
Abbrechen

Abb. 158: **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.
IP-Adresse	Geben Sie die IP-Adresse ein, die der in MAC-Adresse angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in IP-Adresse angegebene IP-Adresse zugewiesen werden soll.

20.4.3 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

Abb. 159: 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.

20.5 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 autorisierte 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

Im Auslieferungszustand ist für das Subsystem CAPI immer ein Benutzer mit dem Benutzernamen *default* ohne Passwort eingetragen. Alle Rufe an die CAPI werden somit allen CAPI-Applikationen im LAN angeboten.

Um die eingehenden Rufe für das Subsystem CAPI auf definierte Benutzer mit Passwort zu verteilen, sollten Sie in diesem Menü Einstellungen vornehmen. Den Benutzer *default* ohne Passwort sollten Sie dann löschen.

20.5.1 Benutzer

Im Menü **Lokale Dienste->CAPI-Server->Benutzer** wird eine Liste aller konfigurierter CAPI Benutzer angezeigt.

20.5.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

Abb. 160: **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

Feld	Beschreibung
	erhalten.
Zugriff	<p>Wählen Sie aus, ob der Zugriff auf den CAPI-Dienst für den Benutzer erlaubt oder gesperrt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

20.5.2 Optionen

Benutzer
Optionen

Basisparameter	
Server aktivieren	<input checked="" type="checkbox"/> Aktiviert
TCP-Port des CAPI-Servers	<input style="width: 100%;" type="text" value="2662"/>

OK
Abbrechen

Abb. 161: Lokale Dienste->CAPI-Server->Optionen

Das Menü **Lokale Dienste->CAPI-Server->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Server aktivieren	<p>Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-Port des CAPI-Servers	<p>Das Feld ist nur editierbar, wenn Server aktivieren aktiviert ist.</p> <p>Geben Sie die TCP-Port-Nummer für Remote-CAPI-Verbindungen ein.</p> <p>Standardwert ist <i>2662</i> .</p>

20.6 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** 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.

20.6.1 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.

20.6.1.1 Neu

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

Auslöser
Aktionen
Optionen

Basisparameter									
Ereignisliste	Neu ▼								
Beschreibung	<input style="width: 90%;" type="text"/>								
Ereignistyp	Zeit ▼								
Zeitintervall auswählen									
Zeitbedingung	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; padding: 2px;">Bedingungstyp</th> <th style="text-align: left; padding: 2px;">Bedingungseinstellungen</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;"><input type="radio"/> Wochentag</td> <td style="padding: 2px;">Montag ▼</td> </tr> <tr> <td style="padding: 2px;"><input checked="" type="radio"/> Perioden</td> <td style="padding: 2px;">Täglich ▼</td> </tr> <tr> <td style="padding: 2px;"><input type="radio"/> Tag des Monats</td> <td style="padding: 2px;">1 ▼</td> </tr> </tbody> </table>	Bedingungstyp	Bedingungseinstellungen	<input type="radio"/> Wochentag	Montag ▼	<input checked="" type="radio"/> Perioden	Täglich ▼	<input type="radio"/> Tag des Monats	1 ▼
Bedingungstyp	Bedingungseinstellungen								
<input type="radio"/> Wochentag	Montag ▼								
<input checked="" type="radio"/> Perioden	Täglich ▼								
<input type="radio"/> Tag des Monats	1 ▼								
Startzeit	Stunde <input style="width: 40px;" type="text"/> Minute <input style="width: 40px;" type="text"/>								
Stopzeit	Stunde <input style="width: 40px;" type="text"/> Minute <input style="width: 40px;" type="text"/>								
OK Abbrechen									

Abb. 162: Lokale Dienste->Scheduling->Auslöser->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Ereignisliste	<p>Mit <i>Neu</i> (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.</p> <p>Wenn Sie eine bestehende Ereignisliste erweitern wollen, wählen Sie die gewünschte Ereignisliste aus und fügen ihr mindestens ein Ereignis hinzu.</p> <p>Über Ereignislisten können auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden. Die Ereignisse werden in derselben Reihenfolge abgearbeitet wie sie in der Liste angelegt sind.</p>
Beschreibung	<p>Nur für Ereignisliste <i>Neu</i></p> <p>Geben Sie eine beliebige Bezeichnung für die Ereignisliste ein.</p>

Feld	Beschreibung
Ereignistyp	<p>Wählen Sie den Typ des Ereignisses aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zeit</i> (Standardwert): Die in Aktionen konfigurierten und zugewiesene Aktionen werden zu bestimmten Zeitpunkten ausgelöst. • <i>MIB/SNMP</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen. • <i>Schnittstellenstatus</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierten Schnittstellen einen bestimmten Status annehmen. • <i>Schnittstellenverkehr</i>: Die in Aktionen konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn der Datenverkehr auf den angegebenen Schnittstellen den definierten Wert unter- oder überschreitet. • <i>Ping-Test</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist. • <i>Lebensdauer eines Zertifikats</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist.
Überwachte Variable	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren definierter Wert als Auslöser konfiguriert werden soll. Wählen Sie zunächst das System aus, in dem die MIB-Variable gespeichert ist, dann die MIB-Tabelle und dann die MIB-Variable selber. Es werden nur die MIB-Tabellen und MIB-Variablen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
Vergleichsbedingung	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie aus, ob die MIB-Variable <i>Größer</i> (Standardwert), <i>Gleich</i>, <i>Kleiner</i>, <i>Ungleich</i> dem in <i>Vergleichswert</i> angegebenen Wert sein oder innerhalb von <i>Bereich</i> liegen muss, um die Aktion auszulösen.</p>
Vergleichswert	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p>

Feld	Beschreibung
	Geben Sie den Wert der MIB-Variable ein.
Indexvariablen	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in der MIB-Tabelle eindeutig zu kennzeichnen, z.B. <i>ConnIfIndex</i>. Aus der Kombination von Indexvariable (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und Indexwert ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere Indexvariablen mit Hinzufügen an.</p>
Überwachte Schnittstelle	<p>Nur für Ereignistyp <i>Schnittstellenstatus</i> und <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.</p>
Schnittstellenstatus	<p>Nur für Ereignistyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Die Schnittstelle ist aktiv. • <i>Inaktiv</i>: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	<p>Nur für Ereignistyp = <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>RX</i> (Standardwert): Der eingehende Datenverkehr wird überwacht. • <i>TX</i>: Der ausgehende Datenverkehr wird überwacht.
Bedingung des Schnittstellenverkehrs	<p>Nur für Ereignistyp = <i>Schnittstellenverkehr</i></p> <p>Wählen Sie aus, ob der Wert für Datenverkehr <i>Größer</i> (Standardwert) oder <i>Kleiner</i> dem in <i>Übertragener Daten-</i></p>

Feld	Beschreibung
	<i>verkehr</i> angegebenen Wert sein muss, um die Aktion auszulösen.
Übertragener Datenverkehr	<p>Nur für Ereignistyp = <i>Schnittstellenverkehr</i></p> <p>Geben Sie den gewünschten Wert für den Datenverkehr mit dem verglichen werden soll in kBytes ein.</p> <p>Standardwert ist <i>0</i>.</p>
Ziel-IP-Adresse	<p>Nur für Ereignistyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
Quell-IP-Adresse	<p>Nur für Ereignistyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Status	<p>Nur für Ereignistyp = <i>Ping-Test</i></p> <p>Wählen Sie aus, ob Ziel-IP-Adresse <i>Erreichbar</i> (Standardwert) oder <i>Nicht erreichbar</i> sein muss, um die Aktion auszulösen.</p>
Intervall	<p>Nur für Ereignistyp = <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Standardwert ist <i>60</i> Sekunden.</p>
Versuche	<p>Nur für Ereignistyp = <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis Ziel-IP-Adresse als <i>Nicht erreichbar</i> gilt.</p>

Feld	Beschreibung
	Standardwert ist 3 .
Überwachtes Zertifikat	Nur für Ereignistyp = <i>Lebensdauer eines Zertifikats</i> Wählen Sie das Zertifikat aus, dessen Gültigkeit überprüft werden soll.
Verbleibende Gültigkeitsdauer	Nur für Ereignistyp = <i>Lebensdauer eines Zertifikats</i> 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 = <i>Zeit</i> Wählen Sie zunächst die Art der Zeitangabe in Bedingungstyp aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Wochentag</i>: Wählen Sie in Bedingungeinstellungen einen Wochentag aus. • <i>Perioden</i> (Standardwert): Wählen Sie in Bedingungeinstellungen einen bestimmten Turnus aus. • <i>Tag des Monats</i>: Wählen Sie in Bedingungeinstellungen einen bestimmten Tag im Monat aus. Mögliche Werte für Bedingungeinstellungen bei Bedingungstyp = <i>Wochentag</i> : <i>Montag</i> (Standardwert) ... <i>Sonntag</i> . Mögliche Werte für Bedingungeinstellungen bei Bedingungstyp = <i>Perioden</i> : <ul style="list-style-type: none"> • <i>Täglich</i>: Der Auslöser wird täglich aktiv (Standardwert). • <i>Montag-Freitag</i>: Der Auslöser wird täglich von Montag bis Freitag aktiv. • <i>Montag-Samstag</i>: Der Auslöser wird täglich von Montag bis Samstag aktiv.

Feld	Beschreibung
	<ul style="list-style-type: none"> <i>Samstag-Sonntag</i>: Der Auslöser wird Samstag und Sonntag aktiv. <p>Mögliche Werte für Bedingungeinstellungen bei Bedingungstyp = Tag des Monats:</p> <p>1 ... 31.</p>
Startzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.
Stoppzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine Stoppzeit eingeben oder Stoppzeit = Startzeit setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.

20.6.2 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.

20.6.2.1 Neu

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

Auslöser Aktionen Optionen

Basisparameter	
Beschreibung	<input type="text"/>
Befehlstyp	Neustart <input type="button" value="v"/>
Ereignisliste	Eine auswählen <input type="button" value="v"/>
Bedingung für Ereignisliste	Alle <input type="button" value="v"/>
Neustart des Geräts nach	<input type="text" value="60"/> Sekunden

Abb. 163: 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	<p>Wählen Sie die gewünschte Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neustart</i> (Standardwert): Ihr Gerät wird neu gestartet. • <i>MIB/SNMP</i>: Für eine MIB-Variable wird der gewünschte Wert eingetragen. • <i>Schnittstellenstatus</i>: Der Status einer Schnittstelle wird verändert. • <i>Softwareaktualisierung</i>: Es wird ein Software-Update initiiert. • <i>Konfigurationsmanagement</i>: Eine Konfigurationsdatei wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert. • <i>Ping-Test</i>: Die Erreichbarkeit einer IP-Adresse wird überprüft. • <i>Zertifikatverwaltung</i>: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • <i>WLC: Neuer Neighbor-Scanvorgang</i>: In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • <i>WLC: VSS-Status</i>: Der Status eines Drahtlosnetzwerkes wird verändert.
Ereignisliste	Wählen Sie die gewünschte Ereignisliste aus, die in Lokale Dienste->Scheduling->Auslöser angelegt ist.
Bedingung für Ereignisliste	<p>Wählen Sie für die gewählte Ereignisliste aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten. • <i>Eins</i>: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt. • <i>Keiner</i>: Die Aktion wird ausgelöst, wenn keines der Ereignis-

Feld	Beschreibung
	<p>se eintritt.</p> <ul style="list-style-type: none"> • <i>Eins nicht</i>: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.
Neustart des Geräts nach	<p>Nur bei Befehlstyp = <i>Neustart</i></p> <p>Geben Sie die Zeitspanne in Sekunden an, die nach dem Eintreten des Ereignisses gewartet werden soll, bis das Gerät neu gestartet wird.</p> <p>Standardwert ist 60 Sekunden.</p>
Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>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.</p>
Befehlsmodus	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie aus, auf welche Weise der MIB-Eintrag manipuliert werden soll.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Vorhandenen Eintrag ändern</i> (Standardwert): Ein bestehender Eintrag soll verändert werden. • <i>Neuen MIB-Eintrag erstellen</i>: Ein neuer Eintrag soll angelegt werden.
Indexvariablen	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in MIB-Tabelle eindeutig zu kennzeichnen, z.B. <i>ConnIfIndex</i>. Aus der Kombination von Indexvariable (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und Indexwert ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere Indexvariablen mit Hinzufügen an.</p>
Status des Auslösers	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p>

Feld	Beschreibung
	<p>Wählen Sie aus, welchen Status das Ereignis haben muss, um die MIB-Variable wie definiert zu verändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Der Wert der MIB-Variable wird verändert, wenn der Auslöser aktiv ist. • <i>Inaktiv</i>: Der Wert der MIB-Variable wird verändert, wenn der Auslöser inaktiv ist. • <i>Beide</i>: Der Wert der MIB-Variable wird unterschiedlich verändert, wenn der Status des Auslösers sich ändert.
MIB-Variablen	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren Wert, abhängig vom Status des Auslösers, verändert werden soll.</p> <p>Ist der Auslöser aktiv (Status des Auslösers <i>Aktiv</i>), wird die MIB-Variable mit dem in Aktiver Wert eingetragenen Wert beschrieben.</p> <p>Ist der Auslöser inaktiv, Status des Auslösers <i>Inaktiv</i>, wird die MIB-Variable mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (Status des Auslösers <i>Beide</i>), 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.</p> <p>Legen Sie weitere Einträge mit Hinzufügen an.</p>
Schnittstelle	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.</p>
Schnittstellenstatus festlegen	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert) • <i>Inaktiv</i> • <i>Zurücksetzen</i>
Quelle	<p>Nur bei Befehlstyp = <i>Softwareaktualisierung</i></p> <p>Wählen Sie die gewünschte Quelle für die Software-Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktuelle Software vom Teldat-Server</i> (Standardwert): Die aktuelle Software wird vom Teldat-Server geladen. • <i>HTTP-Server</i>: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen. • <i>HTTPS-Server</i>: Die aktuelle Software wird von einem HTTPS-Server geladen, den Sie über die <i>Server-URL</i> festlegen. • <i>TFTP-Server</i>: Die aktuelle Software wird von einem TFTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen.
Server-URL	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i></p> <p>wenn Quelle nicht <i>Aktuelle Software vom Teldat-Server</i></p> <p>Geben Sie die URL des Servers ein, von dem die gewünschte Softwareversion geholt werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> mit Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Konfigurationsdatei geholt oder auf den die Konfigurationsdatei gesichert werden soll.</p>
Dateiname	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i></p> <p>Geben Sie den Dateinamen der Softwareversion ein.</p> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> mit Aktion = <i>Zertifikat importieren</i></p>

Feld	Beschreibung
	Geben Sie den Dateinamen der Zertifikatsdatei ein.
Aktion	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Konfiguration importieren</i> (Standardwert) • <i>Konfiguration exportieren</i> • <i>Konfiguration umbenennen</i> • <i>Konfiguration löschen</i> • <i>Konfiguration kopieren</i> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i></p> <p>Wählen Sie aus, welche Aktion auf eine Zertifikatsdatei angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zertifikat importieren</i> (Standardwert) • <i>Zertifikat löschen</i> • <i>SCEP</i>
Protokoll	<p>Nur für Befehlstyp = <i>Zertifikatverwaltung</i> und <i>Konfigurationsmanagement</i> wenn Aktion = <i>Konfiguration importieren</i></p> <p>Wählen Sie das Protokoll für die Dateiübertragung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>HTTP</i> (Standardwert) • <i>HTTPS</i> • <i>TFTP</i>
CSV-Dateiformat	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Datei im CSV-Format übertragen wer-</p>

Feld	Beschreibung
	<p>den soll.</p> <p>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.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Dateiname auf Server	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Für Aktion = <i>Konfiguration importieren</i></p> <p>Geben Sie den Namen der Datei ein, unter dem sie auf dem Server, von dem sie geholt werden soll, gespeichert ist.</p> <p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Geben Sie den Namen der Datei ein, unter dem sie auf dem Server gespeichert werden soll.</p>
Lokaler Dateiname	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren, Konfiguration umbenennen oder Konfiguration kopieren</i></p> <p>Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.</p>
Dateiname in Flash	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Datei aus, die exportiert werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration umbenennen</i></p> <p>Wählen Sie die Datei aus, die umbenannt werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration löschen</i></p> <p>Wählen Sie die Datei aus, die gelöscht werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration kopieren</i></p>

Feld	Beschreibung
	Wählen Sie die Datei aus, die kopiert werden soll.
Konfiguration enthält Zertifikate/Schlüssel	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Konfiguration verschlüsseln	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Nach Ausführung neu starten	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, ob Ihr Gerät nach der gewünschten Aktion neu gestartet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Versionsprüfung	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i></p> <p>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.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Ziel-IP-Adresse	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
Quell-IP-Adresse	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, die als Absendeadresse für den</p>

Feld	Beschreibung
	<p>Ping-Test verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Intervall	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Standardwert ist 1 Sekunde.</p>
Versuche	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis Ziel-IP-Adresse als unerreichbar gilt.</p> <p>Standardwert ist 3.</p>
Serveradresse	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.</p>
Lokale Zertifikatsbeschreibung	<p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie eine Beschreibung für das Zertifikat ein, unter der es im Gerät gespeichert werden soll.</p> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat löschen</i></p> <p>Wählen Sie das Zertifikat aus, das gelöscht werden soll.</p>
Kennwort für geschütztes Zertifikat	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie ein geschütztes Zertifikat verwenden</p>

Feld	Beschreibung
	<p>möchten, das ein Passwort benötigt, und geben Sie dieses in das Eingabefeld ein.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Ähnliches Zertifikat überschreiben	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie ein auf Ihrem Gerät schon vorhandenes Zertifikat mit dem neuen überschreiben wollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikat in Konfiguration schreiben	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungsbeschreibung	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.</p>
SCEP-Server-URL	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B. <i>http://scep.teldat.de:8080/scep/scep.dll</i></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Subjektname	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie einen Subjektnamen mit Attributen ein.</p> <p>Beispiel: <i>"CN=VPNServer, DC=mydomain, DC=com, c=DE"</i></p>

Feld	Beschreibung
CA-Name	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Passwort	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>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.</p>
Schlüsselgröße	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind <i>1024</i> (Standardwert), <i>2048</i> und <i>4096</i>.</p>
Autospeichermodus	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>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.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CRL verwenden	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatssperrlisten-Verteilungspunkt (CDP, CRL Distribution Point) vorhanden ist, soll dieser zusätzlich zu den global im Gerät konfigurierten Sperrlisten ausgewertet werden. • <i>Ja</i>: CRLs werden grundsätzlich überprüft. • <i>Nein</i>: Keine Überprüfung von CRLs.
WLC-SSID	<p>Nur bei Befehlstyp = <i>WLC: VSS-Status</i></p> <p>Wählen Sie das über den WLAN Controller verwaltete Drahtlosnetzwerk aus, dessen Status verändert werden soll.</p>
Status festlegen	<p>Nur bei Befehlstyp = <i>WLC: VSS-Status</i></p> <p>Wählen Sie den Status aus, in den das ausgewählte Drahtlosnetzwerk versetzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert) • <i>Deaktivieren</i>

20.6.3 Optionen

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

Abb. 164: 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.

Feld	Beschreibung
	<p>Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind.</p> <p>Möglich sind Werte zwischen 0 und 65535.</p> <p>Empfohlen wird der Wert 300 (5 Minuten Genauigkeit). Werte kleiner als 60 haben in der Regel keinen Sinn und benötigen unnötig Systemressourcen.</p>

20.7 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.



Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

20.7.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

20.7.1.1 Bearbeiten oder Neu

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

Hosts Schnittstellen Temperatur Ping-Generator

Hostparameter					
Gruppen-ID	Neue ID ▾				
Trigger					
Überwachte IP-Adresse	Standard-Gateway ▾				
Quell-IP-Adresse	Automatisch ▾				
Intervall	10 <input type="text"/> Sekunden				
Erfolgreiche Versuche	3 <input type="text"/>				
Fehlgeschlagene Versuche	3 <input type="text"/>				
Auszuführende Aktion	<table border="1"> <thead> <tr> <th>Aktion</th> <th>Schnittstelle</th> </tr> </thead> <tbody> <tr> <td>Deaktivieren ▾</td> <td>Eine auswählen ▾</td> </tr> </tbody> </table> <p style="text-align: center;">Hinzufügen</p>	Aktion	Schnittstelle	Deaktivieren ▾	Eine auswählen ▾
Aktion	Schnittstelle				
Deaktivieren ▾	Eine auswählen ▾				
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 165: Lokale Dienste->Überwachung->Hosts->Neu

Das Menü **Lokale Dienste->Überwachung->Hosts->Neu** besteht aus folgenden Feldern:

Feld im Menü Hostparameter

Feld	Beschreibung
Gruppen-ID	<p>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.</p> <p>Die Gruppen-IDs werden automatisch von 0 bis 255 angelegt. Ist noch kein Eintrag angelegt, wird durch die Option <i>Neue ID</i> eine neue Gruppe angelegt. Sind Einträge vorhanden, kann man aus den angelegten Gruppen auswählen.</p> <p>Jeder zu überwachende Host muss einer Gruppe zugeordnet werden.</p> <p>Die in Schnittstelle konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied erreichbar ist.</p>

Felder im Menü Trigger

Feld	Beschreibung
Überwachte IP-Adresse	<p>Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Standard-Gateway</i>(Standardwert): Das Standard-Gateway wird überwacht. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse des zu überwachenden Hosts ein.
Quell-IP-Adresse	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse ein.
Intervall	<p>Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p> <p>Standardwert ist <i>10</i> .</p> <p>Innerhalb einer Gruppe wird das kleinste Intervall der Gruppenmitglieder verwendet.</p>
Erfolgreiche Versuche	<p>Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p> <p>Standardwert ist <i>3</i> .</p>
Fehlgeschlagene Versuche	<p>Geben Sie ein, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p>

Feld	Beschreibung
	Standardwert ist 3 .
Auszuführende Aktion	<p>Wählen Sie aus, welche Aktion ausgeführt werden soll. Für die meisten Aktionen wählen Sie eine Schnittstelle, auf die sich die Aktion bezieht.</p> <p>Auswählbar sind alle physikalischen und virtuellen Schnittstellen.</p> <p>Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (<i>Aktivieren</i>), deaktiviert (<i>Deaktivieren</i>, Standardwert) oder zurückgesetzt (<i>Zurücksetzen</i>) werden soll oder ob die Verbindung erneut aufgebaut (<i>Erneut wählen</i>) werden soll.</p> <p>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.</p>

20.7.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

20.7.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Hosts
Schnittstellen
Temperatur
Ping-Generator

Basisparameter	
Überwachte Schnittstelle	<input type="text" value="Eine auswählen"/>
Trigger	<input type="text" value="Schnittstelle wird aktiviert"/>
Schnittstellenaktion	<input type="text" value="Aktivieren"/>
Schnittstelle	<input type="text" value="Eine auswählen"/>

Abb. 166: **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: <ul style="list-style-type: none"> • <i>Schnittstelle wird aktiviert.</i> (Standardwert) • <i>Schnittstelle wird deaktiviert.</i>
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: <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert): Aktivierung der Schnittstelle(n) • <i>Deaktivieren</i>: Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter Schnittstelle festgelegte Aktion ausgeführt werden soll. Wählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle IPSec-Schnittstellen</i> .

20.7.3 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

20.7.3.1 Bearbeiten oder Neu

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

[Hosts](#) | [Schnittstellen](#) | [Temperatur](#) | **Ping-Generator**

Basisparameter	
Ziel-IP-Adresse	<input type="text"/>
Quell-IP-Adresse	Spezifisch <input type="text"/>
Intervall	10 <input type="text"/> Sekunden
Versuche	3 <input type="text"/>

Abb. 167: 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: <ul style="list-style-type: none"> • <i>Automatisch</i>: Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i> (Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in Entfernte IP-Adresse angegebene Adresse abgesetzt werden soll. Mögliche Werte sind 1 bis 65536. Standardwert ist 10.
Versuche	Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden sollen, bis die Ziel-IP-Adresse als <i>Nicht erreichbar</i> gilt. Standardwert ist 3.

20.8 ISDN-Diebstahlsicherung

Mit der Funktion ISDN-Diebstahlsicherung können Sie verhindern, dass sich ein Dieb, der ein Gateway gestohlen hat, Zutritt zum LAN des Gateway-Besitzers verschafft. (Ohne Diebstahlsicherung könnte er sich über ISDN in das LAN einwählen, wenn unter **WAN->Internet + Einwählen->ISDN->** das Feld **Immer aktiv** aktiviert ist.)

20.8.1 Optionen

Alle Schnittstellen, für welche die Diebstahlsicherung aktiv ist, werden beim Booten des Gateways administrativ auf "down" gesetzt.

Anschließend ruft sich das Gateway über ISDN selbst an und überprüft seinen Standort. Wenn die konfigurierten ISDN Rufnummern von den gewählten Rufnummern abweichen, bleiben die Schnittstellen deaktiviert.

Stimmen die Nummern überein, geht das Gerät davon aus, dass es sich am ursprünglichen Standort befindet, und die Schnittstellen werden administrativ auf "up" gesetzt.

Um Kosten zu sparen, nutzt die Funktion den ISDN D-Kanal.



Hinweis

Beachten Sie, dass die Funktion ISDN-Diebstahlsicherung für Ethernet-Schnittstellen nicht zur Verfügung steht.

Optionen

Basisparameter			
ISDN-Diebstahlsicherungsdienst	<input checked="" type="checkbox"/> Aktiviert		
Wählnummer	<input type="text"/>		
Eingehende Nummer	<input type="text"/>		
Ausgehende Nummer	<input type="text"/>		
Überwachte Schnittstellen	<table border="1"> <thead> <tr> <th>Schnittstelle</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> </tr> </tbody> </table> <input type="button" value="Hinzufügen"/>	Schnittstelle	<input type="text"/>
Schnittstelle			
<input type="text"/>			

Erweiterte Einstellungen

Anzahl der Wählversuche	<input type="text" value="3"/>
Timeout	<input type="text" value="5"/> Sekunden

Abb. 168: Lokale Dienste->ISDN-Diebstahlsicherung->Optionen

Das Menü **Lokale Dienste->ISDN-Diebstahlsicherung->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
ISDN-Diebstahlsicherungsdienst	<p>Aktivieren oder deaktivieren Sie die Funktion ISDN-Diebstahlsicherung.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Wählnummer	<p>Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist.</p> <p>Geben Sie die Rufnummer ein, die das Gateway wählt, wenn es sich selbst anruft.</p>
Eingehende Nummer	<p>Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist.</p> <p>Geben Sie die Rufnummer ein, die mit der aktuellen Calling Party Number verglichen werden soll.</p>
Ausgehende Nummer	<p>Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist.</p> <p>Geben Sie die Rufnummer ein, die als Calling Party Number gesetzt wird.</p>

Feld	Beschreibung
Überwachte Schnittstellen	<p>Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist.</p> <p>Fügen Sie mit Hinzufügen eine neue Schnittstelle hinzu.</p> <p>Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, auf welche die Funktion ISDN-Diebstahlsicherung angewendet werden soll.</p>

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Anzahl der Wählversuche	<p>Geben Sie die Anzahl der Wählversuche ein, die das Gateway unternehmen soll, um sich nach einem Neustart über ISDN selbst anzurufen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Standardwert ist 3.</p>
Timeout	<p>Geben Sie die Zeitspanne ein, die das Gateway warten soll, bis es sich nach einem erfolglosen Versuch erneut selbst anruft.</p> <p>Mögliche Werte sind 2 bis 20.</p> <p>Standardwert ist 5.</p>

20.9 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 zugewiesenen Ports liegen im Bereich von *5004* bis *65535*. Die Ports werden gatewayintern bei Anforderung freigegeben, d.h. beim Start einer Audio-/Videoübertragung im Messenger. Nach Beenden der Anwendung werden die Ports sofort wieder geschlossen.

Die Peer-to-Peer-Kommunikation wird über öffentliche SIP Server initiiert, wobei lediglich die Informationen beider Clients weitergereicht werden. Anschließend kommunizieren die Clients direkt miteinander.

Weitere Informationen zu UPnP erhalten Sie auf www.upnp.org.

20.9.1 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.

The screenshot shows a configuration window titled 'Schnittstellen' with the 'Allgemein' tab active. At the top, there are navigation controls: 'Ansicht 20 pro Seite', a filter dropdown set to 'Keiner', and a search bar containing 'Los'. Below this is a table with three columns: 'Schnittstelle', 'Auf Client-Anfrage antworten', and 'Schnittstelle ist UPnP-kontrolliert'. The table contains two rows: 'en1-4' and 'en1-0'. Each row has a checkbox labeled 'Aktiviert' in the second column and another checkbox labeled 'Aktiviert' in the third column. At the bottom of the window, there are 'OK' and 'Abbrechen' buttons. The status bar at the bottom left indicates 'Seite: 1, Objekte: 1 - 2'.

Abb. 169: 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

Feld	Beschreibung
	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 <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Schnittstelle ist UPnP-kontrolliert	Legen Sie fest, ob die NAT Konfiguration dieser Schnittstelle von UPnP kontrolliert wird. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

20.9.2 Allgemein

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

Schnittstellen
Allgemein

Basisparameter	
UPnP-Status	<input type="checkbox"/> Aktiviert
UPnP TCP Port	<input style="width: 80%;" type="text" value="5678"/>

OK
Abbrechen

Abb. 170: Lokale Dienste->UPnP->Globale Einstellungen

Das Menü **Lokale Dienste->UPnP->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
UPnP-Status	Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt. Mit <i>Aktiviert</i> 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 Adres-

Feld	Beschreibung
	<p>se des anfragenden LAN UPnP Clients.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.</p>
UPnP TCP Port	<p>Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht.</p> <p>Mögliche Werte sind 1 bis 65535, der Standardwert ist 5678.</p>

20.10 Hotspot-Gateway

Die **bintec Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen (mittels WLAN oder kabelgebundenem Ethernet). Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **bintec Hotspot Solution** besteht aus einem vor Ort installierten bintec Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

Ablauf der Anmeldeprozedur am Hotspot Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein bintec Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu** mit **Gruppenbeschreibung** *Standardgruppe 0*)
- bintec Hotspot Hosting (Artikelnummer 5510000198)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

- Gehen Sie auf www.teldat.de 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 Teldat 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.teldat.de/
Username	Wird durch Teldat individuell festgelegt
Password	Wird durch Teldat individuell festgelegt



Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf www.teldat.de zum Download zur Verfügung steht.

20.10.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte bintec Gateway für die **bintec Hotspot Solution**.

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller konfigurierter Hotspot Netzwerke angezeigt.



Abb. 171: **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway**

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktivieren.

20.10.1.1 Bearbeiten oder Neu

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->**  konfigurieren Sie die Hotspot Netzwerke. Wählen Sie die Schaltfläche **Neu**, um weitere Hotspot Netzwerke einzurichten.

Hotspot-Gateway Optionen

Basisparameter	
Schnittstelle	LAN_EN1-0
Domäne am Hotspot-Server	
Walled Garden	<input type="checkbox"/> Aktiviert
Sprache für Anmeldefenster	English

Erweiterte Einstellungen

Tickettyp	Benutzername/Passwort
Zulässiger Hotspot-Client	Alle
Anmeldefenster	<input checked="" type="checkbox"/> Aktiv

OK Abbrechen

Abb. 172: 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	<p>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.</p> <div style="display: flex; align-items: center; margin-top: 20px;">  <div> <p>Achtung</p> <p>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!</p> <p>Wenn Sie hier die Schnittstelle auswählen, über die die aktuelle Konfigurationssitzung stattfindet, geht die aktuelle Verbindung verloren. Sie müssen sich dann über eine erreichbare, nicht für den Hotspot konfigurierte Schnittstelle zur weiteren Konfiguration Ihres Geräts erneut anmelden.</p> </div> </div>
Domäne am Hotspot-	Geben Sie den Domännennamen ein, der bei der Einrichtung

Feld	Beschreibung
Server	des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.
Walled Garden	<p>Aktivieren Sie diese Funktion, wenn Sie einen abgegrenzten und kostenfreien Bereich von Webseiten (Intranet) definieren wollen.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>
Walled Network / Netzmaske	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Geben Sie die Netzadresse des Walled Network und die entsprechende Netzmaske des Intranet-Servers ein.</p> <p>Für den aus Walled Network / Netzmaske resultierenden Adressraum benötigen die Clients keine Authentifizierung.</p> <p>Beispiel: Geben Sie 192.168.0.0 / 255.255.255.0 ein, sind alle IPAdressen von 192.168.0.0 bis 192.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IPAdresse 192.168.0.1 frei.</p>
Walled Garden URL	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Geben Sie die Walled Garden URL des Intranet-Servers ein. Frei zugängliche Webseiten müssen über diese Adresse erreichbar sein.</p>
Geschäftsbedingungen	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>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.</p>
Zusätzliche, frei zugängliche Domännennamen	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Fügen Sie mit Hinzufügen weitere URLs oder IP-Adressen hinzu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.</p>
Sprache für Anmeldefenster	Hier können Sie die Sprache für die Start/Login-Seite auswählen.

Feld	Beschreibung
	<p>Folgende Sprachen werden unterstützt: <i>English, Deutsch, Italiano, Français, Español, Português</i> und <i>Nederlands</i>.</p> <p>Die Sprache kann auf der Start/Login-Seite selbst jederzeit umgeschaltet werden.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Tickettyp	<p>Wählen Sie den Tickettyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Voucher</i>: Nur der Benutzername muss eingegeben werden. Definieren Sie im Eingabefeld ein Standardpasswort. • <i>Benutzername/Passwort</i>(Standardwert): Benutzername und Passwort müssen eingegeben werden.
Zulässiger Hotspot-Client	<p>Hier legen Sie fest, welche Art von Benutzern sich am Hotspot anmelden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i>: Alle Clients werden zugelassen. • <i>DHCP-Client</i>: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.
Anmeldefenster	<p>Aktivieren oder deaktivieren Sie das Anmeldefenster.</p> <p>Das Anmeldefenster auf der HTML-Startseite besteht aus zwei Frames.</p> <p>Wenn die Funktion aktiviert ist, wird auf der linken Seite das Anmelde-Formular angezeigt.</p> <p>Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

20.10.2 Optionen

Im Menü **Lokale Dienste->Hotspot-Gateway->Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

Abb. 173: **Lokale Dienste->Hotspot-Gateway->Optionen**

Das Menü **Lokale Dienste->Hotspot-Gateway->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Host für mehrere Standorte	Wenn für einen Kunden auf dem Hotspot Server mehrere Standorte (Filialen) eingerichtet wurden, geben Sie hier den Wert des NAS-Identifiers (RADIUS-Server Parameter) ein, der für diesen Standort auf dem Hotspot Server eingetragen wurde.

20.11 BRRP

Im Menü **BRRP** können Sie eine Redundanz für Ihr Gateway konfigurieren.



Hinweis

Für Geräte der R23x-Serie und der RS-Serie benötigen Sie eine Lizenz.

BRRP (Bintec Router Redundancy Protocol) ist eine Bintec-spezifische Implementierung des VRRP (Virtual Router Redundancy Protocol). Ein Router-Redundanzverfahren dient hauptsächlich dazu, die Verfügbarkeit eines physikalischen Gateways im LAN oder WAN sicherzustellen.

Begriffe und Definitionen

Zur Beschreibung der Funktion werden einige spezielle Begriffe verwendet. Folgende Begriffe werden im entsprechenden RFC und im Internet-Entwurf definiert.

BRRP Begriffe

Feld	Beschreibung
VRRP-Router	"Ein Router, der das Virtual Router Redundancy Protocol benutzt. Er kann in einen oder in mehrere "virtuelle Router" integriert sein."
Virtueller Router	"Ein abstraktes, von VRRP gesteuertes Objekt, das als Standard-Router für Hosts eines LAN verwendet wird. Es besteht aus einem Virtual Router Identifier (ID des virtuellen Routers) und einer IP-Adresse bzw. einer Gruppe zugehöriger IP-Adressen innerhalb eines gemeinsamen LAN. Ein VRRP-Router kann den Datenverkehr eines einzelnen virtuellen Routers oder mehrerer virtueller Router absichern."
IP Address Owner	"Der VRRP-Router, der die IP-Adresse(n) des virtuellen Routers als echte Schnittstellen- Adresse(n) besitzt. Es handelt sich um den Router, der, wenn er aktiv ist, auf Pakete für ICMP-Pings, TCP-Verbindungen etc. an eine dieser IP-Adressen antwortet."
Primary IP Address	"Eine IP-Adresse, die aus der Gruppe der echten Schnittstellenadressen gewählt wird. Eine mögliche Algorithmusoption ist die Auswahl der ersten Adresse. VRRP Advertisements werden immer mit der Primary IP-Adresse als Quelle des IP-Pakets verschickt."
VRRP Advertisement	Ein Keepalive, das der Master zu den Backup-Gateways schickt, um seine Erreichbarkeit zu signalisieren.
Virtual Router Master	"Der VRRP-Router, der das Weiterleiten der Pakete übernimmt, die an die mit dem "virtuellen Router" verbundenen IP-Adressen geschickt wurden, und der für die Beantwortung von ARP (Address Resolution Protocol) Requests an diese IP-Adressen zuständig ist."
Virtual Router Backup	"Die Gruppe der VRRP-Router, welche die Verantwortung für das Weiterleiten übernehmen, falls der Master ausfallen sollte." Im Backup-Status sind diese VRRP-Router inaktiv, d.h. beantworten keine ARP-Requests."

20.11.1 Virtuelle Router

Bei der Verwendung eines Router-Redundanzprotokolls werden mehrere Router zu einer logischen Einheit zusammengefasst. Das Router-Redundanzprotokoll BRRP verwaltet die beteiligten Router und organisiert im einzelnen Folgendes:

Es stellt sicher, dass jeweils nur ein Router innerhalb des logischen Verbunds aktiv ist.

Es gewährleistet, dass bei Ausfall des aktiven Routers ein anderer Router die Funktion des ausgefallenen Geräts übernimmt. Wann welcher Router aktiv ist, wird über eine dem Router zugeordnete Priorität bestimmt.

Nehmen wir als Beispiel ein einfaches Szenario, in dem Gateway A den Internetzugang der Hosts in einem LAN ermöglicht. Wenn dieses Gateway ausfällt, haben alle Hosts keinen Zugang zum Internet, deren Routen statisch konfiguriert sind. Um den Hosts weiterhin Zugang zum Internet zu ermöglichen, bietet Gateway B allen Hosts im LAN den Dienst an, den vorher Gateway A durchgeführt hat. Alle Aufgaben eines virtuellen Routers und das Umschalten von Diensten von einem Gateway auf das andere werden von dem BRRP-Redundanzprotokoll gesteuert.

Das BRRP folgt den Spezifikationen in RFC 2338 und dem entsprechenden Internet- Entwurf (siehe www.ietf.org).

Die Konfiguration des Router-Redundanzverfahrens wird in folgenden Schritten durchgeführt:

- Konfiguration der Schnittstelle, über welche die BRRP-Advertisement-Datenpakete geschickt werden.



Hinweis

Diese Schnittstelle wird zur Übertragung der BRRP-Advertisement-Datenpakete sowie eventuell zur Übertragung von Keepalive-Monitoring-Datenpaketen verwendet. Zur Übertragung der Nutzdaten muss eine andere Schnittstelle im nächsten Schritt konfiguriert werden.

Die Konfiguration der Advertisement-Schnittstelle wird im Menü **Lokale Dienste->BRRP->Virtueller Router->Neu** unter **BRRP Advertisement-Schnittstelle** vorgenommen.

Nur der aktive Router des Routerverbunds sendet Advertisement-Datenpakete. Die IPv4-Multicast-Adresse 224.0.0.18 dient als Zieladresse für alle Router, die Bestandteil des Routerverbundes sind. Alle passiven Router des Verbundes müssen diese Adresse überwachen, damit sie bei Ausbleiben der Advertisement-Datenpakete entsprechend ihrer Priorität und der sonstigen BRRP-Konfiguration reagieren können.

- Konfiguration der Schnittstelle zur Übertragung von Nutzdaten (Konfiguration der virtuellen Schnittstelle).

Eine virtuelle Schnittstelle wird über die Zuweisung zu einem virtuellen Router über das BRRP-Router-Redundanzprotokoll aktiviert bzw. deaktiviert.

Die Konfiguration wird im Menü **Lokale Dienste->BRRP->Virtueller Router->Neu->Ethernet-Schnittstelle** vorgenommen.

In diesem Schritt konfigurieren Sie die IP-Adresseinstellungen und ordnen die Schnittstelle einem virtuellen Router zu. Darüber hinaus werden die Eigenschaften des virtuellen Routers (z. B. die Priorität) festgelegt.



Hinweis

Das System vergibt die MAC-Adresse der virtuellen Schnittstelle nach folgendem Schema automatisch: 00:00:5E:00:01:<ID des virtuellen Routers>. Die ID des virtuellen Routers bestimmt somit die MAC-Adresse der Schnittstelle, die zur Übertragung der Nutzdaten verwendet wird.

Die Konfiguration der virtuellen Schnittstelle (MAC-Adresse, IP-Adresse) sowie die Konfiguration des virtuellen Routers (Sendeintervall für Advertisements, Master down trials) muss innerhalb des logischen Verbundes auf allen Routern mit derselben Virtual Router ID identisch sein.

Sie müssen IP-Adressen aus unterschiedlichen Subnetzen für die Advertisement-Schnittstelle und für die virtuelle Schnittstelle verwenden.

Alle virtuellen Schnittstellen auf einem physikalischen Router sollten normalerweise dieselbe Priorität haben.

- Konfiguration der Synchronisation zwischen den virtuellen Routern, sowie Konfiguration der Ereignisse, die zu einem Umschalten des Betriebszustandes der virtuellen Router führen.

Über die Steuerung des Betriebszustandes eines virtuellen Routers wird implizit auch der Betriebszustand der Schnittstelle gesteuert, die mit dem virtuellen Router verknüpft ist. Da im Fehlerfall alle Schnittstellen eines Geräts deaktiviert werden müssen, muss der Betriebszustand aller Schnittstellen eines Geräts synchronisiert werden. Die Synchronisation ist notwendig, wenn mehrere Schnittstellen auf einem Gerät überwacht werden. Diese Konfiguration wird im Menü **Lokale Dienste->BRRP->VR-Synchronisation->Neu** vorgenommen.

- Einschalten des Redundanzverfahrens. Diese Konfiguration wird im Menü **Lokale Dienste->BRRP->Optionen** vorgenommen.

Im Menü **Lokale Dienste->BRRP->Virtueller Router->Neu** konfigurieren Sie die Advertisement-Schnittstelle und die virtuelle(n) Schnittstelle(n). Sie müssen auf allen physikalischen Routern, die am Redundanzverfahren teilnehmen, dieselben virtuellen Router mit denselben Schnittstellen konfigurieren. (Die virtuellen Router haben jedoch auf den verschiedenen physikalischen Routern unterschiedliche Priorität.)

20.11.1.1 Neu

Wählen Sie die Schaltfläche **Neu** um weitere Virtuelle Router zu konfigurieren.

Virtuelle Router VR-Synchronisation Optionen

BRRP Advertisement-Schnittstelle							
Ethernet-Schnittstelle	<input type="text" value="Eine auswählen"/>						
IP-Adresse	<input type="text" value="IP-Adresse"/> <input type="text" value="Netzmaske"/>						
BRRP Überwachte Schnittstelle							
Schnittstelle des virtuellen Routers	Keine Advertisement-Schnittstelle ausgewählt!						
Router-IP-Adresse	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>IP-Adresse</td> <td>Netzmaske</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text" value="255.255.255.0"/></td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	IP-Adresse	Netzmaske	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="Hinzufügen"/>	
IP-Adresse	Netzmaske						
<input type="text"/>	<input type="text" value="255.255.255.0"/>						
<input type="button" value="Hinzufügen"/>							
ID des virtuellen Routers	<input type="text" value="1"/>						
Priorität des virtuellen Routers	<input type="text" value="100"/>						
Erweiterte Einstellungen							
Sendeintervall für Advertisements	<input type="text" value="1"/>						
Master down trials	<input type="text" value="10"/>						
Pre-Empt-Modus (zurück in Master-Status)	<input checked="" type="checkbox"/> Aktiviert						
Authentisierung aktivieren	<input type="checkbox"/>						
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

Abb. 174: **Lokale Dienste->BRRP->Virtuelle Router->Neu**

Das Menü **Lokale Dienste->BRRP->Virtuelle Router->Neu** besteht aus folgenden Feldern:

Felder im Menü BRRP Advertisement-Schnittstelle

Feld	Beschreibung
Ethernet-Schnittstelle	<p>Wählen Sie die Schnittstelle aus, über die BRRP-Advertisement-Pakete versendet und erwartet werden.</p> <p>Wenn Sie einen virtuellen Router bearbeiten, wird die Ethernet-Schnittstelle angezeigt und kann nicht verändert werden.</p>

Feld	Beschreibung
	Hinweis: Die Ethernet-Schnittstelle zur Versendung der Advertisements ist immer up and running und kann daher nicht als Schnittstelle des virtuellen Routers verwendet werden.
IP-Adresse	Zeigt die IP-Adresse(n) der Schnittstelle an, über die BRRP-Advertisement-Pakete versendet und erwartet werden.

Felder im Menü BRRP Überwachte Schnittstelle

Feld	Beschreibung
Schnittstelle des virtuellen Routers	Zeigt an, auf welcher physikalischen Schnittstelle die virtuelle Schnittstelle basiert, wenn eine neue virtuelle Schnittstelle angelegt wird. Die Bezeichnung der virtuellen Schnittstelle wird beim Anlegen automatisch vergeben. Zeigt die Bezeichnung der virtuellen Schnittstelle an, wenn eine bereits angelegte virtuelle Schnittstelle bearbeitet wird.
IP-Adresse des virtuellen Routers	Geben Sie die IP-Adresse und die Netzmaske des virtuellen Routers ein. Hier geben Sie die IP-Adresse ein, die Sie im lokalen Netz als eigentliche Gateway-IP-Adresse verwenden wollen.
	<div style="border: 1px solid black; padding: 5px;"> <p> Hinweis</p> <p>Um Probleme im LAN zu vermeiden, dürfen die IP-Adresse für Advertisements und die IP-Adresse des virtuellen Routers nicht aus demselben Subnetz stammen.</p> </div>
ID des virtuellen Routers	<p>Wählen Sie die ID des virtuellen Routers.</p> <p>Diese ID identifiziert den "virtuellen Router" innerhalb des LAN und ist Bestandteil jedes BRRP-Advertisement-Pakets, das vom aktuellen Master gesendet wird.</p> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 255.</p>
Priorität der virtuellen Schnittstelle	<p>Setzen Sie die gesendete BRRP-Priorität der Schnittstelle für den virtuellen Router fest. Höhere Prioritäten bestimmen die Schnittstellen des Masters in der Initialisierungs-Phase und bei aktivem Pre-Empt-Modus.</p> <p>Mögliche Werte sind 1 bis 255.</p>

Feld	Beschreibung
	<p>Der Standardwert ist <i>100</i>.</p> <p>Eine Priorität von 255 wird für Router genutzt, deren IP-Adresse mit der IP-Adresse des virtuellen Routers übereinstimmt.</p>

Im Menü **Erweiterte Einstellungen** müssen Sie alle Parameter für alle virtuellen Router auf allen Geräten, die am Routerverbund teilnehmen, identisch konfigurieren. Wir empfehlen Ihnen, die Voreinstellungen zu belassen.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<p>Sendeintervall für Advertisements</p>	<p>Legen Sie fest, wie oft ein BRRP-Advertisement-Paket gesendet wird, wenn der virtuelle Router als Master definiert ist. Nur der aktuelle Master sendet über Multicast BRRP-Advertisements, welche auch die ID und die Priorität des Masters enthalten.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>1</i> und <i>255</i>. Der Wert wird in Sekunden angegeben, Standardwert ist <i>1</i>.</p> <p>Basierend auf diesem Sendeintervall für Advertisements läuft routerintern ein Advertisement Timer, nach dessen Ablauf ein Advertisement-Paket gesendet wird.</p>
<p>Master down trials</p>	<p>Legen Sie die Anzahl von BRRP Advertisements fest, die fehlschlagen darf, bevor der Backup Router mit der jeweils niedrigeren Priorität annimmt, dass der Master inaktiv ist und er die Rolle des Masters übernimmt.</p> <p>Basierend auf dem Parameter Master down trials läuft routerintern ein Master Down Timer, nach dessen Ablauf vom Backup Router angenommen wird, dass der Master nicht erreichbar ist, falls kein Advertisement empfangen wurde.</p> <p>Das effektive Master Down Intervall entspricht der Zeit errechnet aus der Anzahl erwarteter, aber ausgelassener BRRP Advertisements, dem Advertisement Interval und der sogenannten Skew Time, welche einen minimalen Zeitraum abhängig von der Priorität hinzufügt. Je höher die Priorität, desto kürzer ist die hinzugefügte Zeit, so dass ein Backup-Router mit höherer Priorität früher reagiert als einer mit niedrigerer Priorität).</p>

Feld	Beschreibung
	Mögliche Werte sind ganze Zahlen zwischen 1 und 255, Standardwert ist 10.
Pre-Empt-Modus (zurück in Master-Status)	<p>Legen Sie fest, ob ein Backup-Router mit höherer Priorität Vorrang hat vor einem Master-Router mit niedriger Priorität.</p> <p>Der Pre-Empt-Modus dient dazu, unnötige Umschaltvorgänge zu verhindern.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv. Der Router mit der höheren Priorität hat immer Vorrang. Das heißt, bei Wiedererreichbarkeit des eigentlichen Master-Routers wird dieser auch immer aktiv. Wenn die Funktion nicht aktiv ist, bleibt der aktuell aktive Backup-Router auch nach Wiedererreichbarkeit des eigentlichen Master-Routers weiterhin aktiv, obwohl die Priorität des Master-Routers höher ist als die Priorität des derzeit aktivierten Backup-Routers.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Beachten Sie eine Ausnahme: Wird als Priorität der virtuellen Schnittstelle 255 ausgewählt, erhält das Gateway mit dieser Priorität auf jeden Fall die Masterrolle, d.h. die Einstellung in Pre-Empt-Modus (zurück in Master-Status) wird nicht berücksichtigt. Wählen Sie daher zur Nutzung von Pre-Empt-Modus eine Priorität der virtuellen Schnittstelle kleiner 255.</p>
Authentisierung aktivieren	<p>Aktivieren oder deaktivieren Sie die Authentisierung.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Wenn die Funktion aktiv ist, wird ein Eingabefeld angezeigt. Hier geben Sie den Authentisierungsschlüssel ein.</p> <p>Hinweis: Beachten Sie, dass der Authentisierungsschlüssel für alle am Routerverbund teilnehmenden virtuellen Router gleich sein muss.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

20.11.2 VR-Synchronisation

Im Menü **Lokale Dienste->BRRP->VR-Synchronisation** wird der Watchdog Daemon konfiguriert, d.h. Sie legen fest, wie Statusänderungen gehandhabt werden.

Nach Öffnen des Menüs **Lokale Dienste->BRRP->VR-Synchronisation** wird eine Liste aller Synchronisationen angezeigt. Sie können entweder virtuelle Router untereinander synchronisieren oder Schnittstellen. Neue Synchronisationen können im Menü **Neu** hinzugefügt werden.

Sie können z. B. die beiden virtuellen Router R1 und R2 über BRRP synchronisieren. Dazu müssen Sie zwei Einträge anlegen. Für den ersten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R1 und als **Synchronisations-VR/Schnittstelle** R2 verwenden. Für den zweiten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R2 und als **Synchronisations-VR/Schnittstelle** R1 konfigurieren.

20.11.2.1 Neu

Wählen Sie die Schaltfläche **Neu** um neue Synchronisationen hinzuzufügen.

Abb. 175: **Lokale Dienste->BRRP->VR-Synchronisation->Neu**

Das Menü **Lokale Dienste->BRRP->VR-Synchronisation->Neu** besteht aus folgenden Feldern:

Felder im Menü **Monitoring-VR/Schnittstelle**

Feld	Beschreibung
Monitoring-Modus	<p>Zeigt an, welcher Mechanismus für die Überwachung eines virtuellen Routers angewendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>BRRP</i> : Die BRRP-spezifischen Status-Advertisements werden zur Statusermittlung des Masters verwendet. (Der Master sendet Advertisements gemäß seiner Konfiguration im Menü Lokale Dienste->BRRP->Virtuelle Router->Neu->Erweiterte Einstellungen.)

Feld	Beschreibung
ID des virtuellen Routers	Wählen Sie einen virtuellen Router über die ID des virtuellen Routers und legen Sie durch die Auswahl fest, welche Schnittstelle kontrolliert werden soll. Wählbar sind die vorher definierten IDs (siehe ID des virtuellen Routers im Menü Lokale Dienste->BRRP->Virtueller Router->Neu im Bereich BRRP Überwachte Schnittstelle). Der Watchdog Daemon fragt die in Virtuelle Router festgelegten Detailinformationen ab.

Felder im Menü Synchronisations-VR/Schnittstelle

Feld	Beschreibung
Synchronisationsmodus	Zeigt an, mit welchem Mechanismus virtuelle Router bzw. Schnittstellen synchronisiert werden: Mögliche Werte: <ul style="list-style-type: none"> • <i>BRRP</i> : BRRP wird für die Synchronisierung der virtuellen Router verwendet.
ID des virtuellen Routers	Wählen Sie die ID des virtuellen Routers, der synchronisiert werden soll. Über die Synchronisation des virtuellen Routers wird implizit die mit dem virtuellen Router verbundene virtuelle Schnittstelle synchronisiert.

20.11.3 Optionen

Im Menü **Lokale Dienste->BRRP->Optionen** können Sie die Funktion BRRP ein- oder ausschalten.

The screenshot shows a configuration window with three tabs: 'Virtuelle Router', 'VR-Synchronisation', and 'Optionen'. The 'Optionen' tab is active. Inside the window, there is a section titled 'Basisparameter' containing a checkbox labeled 'BRRP aktivieren' which is currently unchecked. At the bottom of the window, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 176: **Lokale Dienste->BRRP->Optionen**

Das Menü **Lokale Dienste->BRRP->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
BRRP aktivieren	Aktivieren oder deaktivieren Sie die Funktion BRRP. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Kapitel 21 Wartung

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

21.1 Diagnose

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

21.1.1 Ping-Test

The screenshot shows a web interface for the 'Ping-Test' function. At the top, there are three tabs: 'Ping-Test' (selected), 'DNS-Test', and 'Traceroute-Test'. Below the tabs is a form with the following elements:

- A header bar labeled 'Ping-Test'.
- A 'Test-Ping-Modus' section with two radio buttons: 'IPv4' (selected) and 'IPv6'.
- A 'Ping-Befehl testweise an Adresse senden' section with a text input field.
- An 'Ausgabe' section with a large, empty text area for displaying results.
- A 'Los' button at the bottom center.

Abb. 177: **Wartung**->**Diagnose**->**Ping-Test**

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

Felder im Menü Ping-Test

Feld	Beschreibung
Test-Ping-Modus	Wählen Sie die für den Ping-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i>
Ping-Befehl testweise an Adresse senden	Geben Sie die zu testende IP-Adresse ein.
Zu verwendende Schnittstelle	Nur für Test-Ping-Modus = <i>IPv6</i> Wählen Sie für Link-Local-Adressen die Schnittstelle, die für den Ping-Test verwendet werden soll. Für globale Adressen kann <i>Standard</i> verwendet werden.

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

21.1.2 DNS-Test

The screenshot shows a web interface for network diagnostics. At the top, there are three tabs: 'Ping-Test', 'DNS-Test', and 'Traceroute-Test'. The 'DNS-Test' tab is currently selected. Below the tabs, the interface is divided into sections. The 'DNS-Test' section contains a label 'DNS-Adresse' followed by an empty text input field. Below this is a section labeled 'Ausgabe' which contains a large, empty rectangular area for displaying test results. At the bottom center of the interface is a button labeled 'Los'.

Abb. 178: **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 Domännennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

21.1.3 Traceroute-Test

Abb. 179: **Wartung->Diagnose->Traceroute-Test**

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

Felder im Menü Traceroute-Test

Feld	Beschreibung
Traceroute-Modus	Wählen Sie die für den Traceroute-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i>
Traceroute-Adresse	Geben Sie die zu testende IP-Adresse ein.

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

21.2 Software & Konfiguration

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

21.2.1 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.teldat.de. 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 Teldat 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.

Optionen

Aktuell installierte Software	
BOSS	V.9.1 Rev. 2 IPsec from 2012/03/23 00:00:00
Systemlogik	1.0
ADSL-Logik	2.1.4.7.0.2
Optionen zu Software und Konfiguration	
Aktion	Keine Aktion <input type="button" value="v"/>

Abb. 180: **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.

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	<p>Wählen Sie die Aktion aus, die Sie ausführen möchten.</p> <p>Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine Aktion</i> (Standardwert): • <i>Konfiguration exportieren</i>: 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. • <i>Konfiguration importieren</i>: Wählen Sie in Dateiname eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken auf Los wird die Datei zunächst unter dem Namen <i>boot</i> in den Flash-Speicher des Geräts geladen. Zum Aktivieren müssen Sie das Gerät neu starten. <p>Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben!</p> <ul style="list-style-type: none"> • <i>Konfiguration kopieren</i>: Die Konfigurationsdatei im Feld Name der Quelldatei wird als Name der Zieldatei gespeichert. • <i>Konfiguration löschen</i>: Die Konfiguration im Feld Datei auswählen wird gelöscht. • <i>Konfiguration umbenennen</i>: Die Konfigurationsdatei im Feld Datei auswählen wird zu Neuer Dateiname umbenannt. • <i>Konfiguration umbenennen</i>: Nur, wenn unter Konfigura-

Feld	Beschreibung
	<p>tion speichern mit der Einstellung <i>Konfiguration speichern</i> und <i>vorhergehende Boot-Konfiguration sichern</i> die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen.</p> <ul style="list-style-type: none"> • <i>Software/Firmware löschen</i>: Die Datei im Feld Datei auswählen wird gelöscht. • <i>Sprache importieren</i>: Sie können weitere Sprachversionen des GUI auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von www.teldat.de auf Ihren PC herunterladen und von dort aus in Ihr Gerät einspielen. • <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware, der ADSL-Logik und des BOOTmonitors initiieren. • <i>Konfiguration mit Statusinformationen exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die Los-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.
Aktueller Dateiname im Flash	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.</p>
Zertifikate und Schlüssel einschließen	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Verschlüsselung der Konfiguration	<p>Nur für Aktion = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p>

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Password eingeben.</p>
Dateiname	<p>Nur für Aktion = <i>Konfiguration importieren, Sprache importieren, Systemsoftware aktualisieren</i></p> <p>Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.</p>
Name der Quelldatei	<p>Nur für Aktion = <i>Konfiguration kopieren</i></p> <p>Wählen Sie die Quelldatei aus, die kopiert werden soll.</p>
Name der Zieldatei	<p>Nur für Aktion = <i>Konfiguration kopieren</i></p> <p>Geben Sie den Namen der Kopie ein.</p>
Datei auswählen	<p>Nur für Aktion = <i>Konfiguration löschen, Konfiguration umbenennen</i> oder <i>Software/Firmware löschen</i></p> <p>Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.</p>
Neuer Dateiname	<p>Nur für Aktion = <i>Konfiguration umbenennen</i></p> <p>Geben Sie den neuen Namen der Konfigurationsdatei ein.</p>
Quelle	<p>Nur für Aktion = <i>Systemsoftware aktualisieren</i></p> <p>Wählen Sie die Quelle der Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokale Datei</i> (Standardwert): Die Systemsoftware-Datei ist lokal auf Ihrem PC gespeichert. • <i>HTTP-Server</i>: Die Datei ist auf dem entfernten Server gespeichert, der in der URL angegeben wird. • <i>Aktuelle Software vom Teldat-Server</i>: Die Datei liegt auf dem offiziellen Teldat-Update-Server.

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

21.3 Neustart

21.3.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **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.

Systemneustart

Möchten Sie das System jetzt wirklich neu starten?

OK

Abb. 181: **Wartung->Neustart->Systemneustart**

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

Kapitel 22 Externe Berichterstellung

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

22.1 Systemprotokoll

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

Zusätzlich zu den intern auf Ihrem Gerät protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf Ihrem Gerät intern gespeicherte Systemprotokoll-Nachrichten gehen bei einem Neustart verloren.



Warnung

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

Syslog-Daemon

Die Erfassung der Systemprotokoll-Nachrichten wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (abrufbar im Download-Bereich unter www.teldat.de).

22.1.1 Syslog-Server

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

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

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

22.1.1.1 Neu

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

Syslog-Server

Basisparameter	
IP-Adresse	<input type="text"/>
Level	Informationen ▼
Facility	local0 ▼
Zeitstempel	<input checked="" type="radio"/> Keiner <input type="radio"/> Zeit <input type="radio"/> Datum & Uhrzeit
Protokoll	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Nachrichtentyp	<input type="radio"/> System <input type="radio"/> Accounting <input checked="" type="radio"/> System & Accounting
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 182: **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	<p>Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Benachrichtigung</i> • <i>Informationen</i> (Standardwert) • <i>Debug</i> (niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden an den Host gesendet, d. h. dass beim Syslog-Level <i>Debug</i> sämtliche erzeugten Meldungen an den Host weitergeleitet werden.</p>
Facility	<p>Geben Sie die Syslog Facility auf dem Host an.</p> <p>Dieses ist nur erforderlich, wenn der Log Host ein Unix-Rechner ist.</p> <p>Mögliche Werte: <i>local0</i> - 7 .</p> <p>Standardwert <i>local0</i>.</p>
Zeitstempel	<p>Wählen Sie das Format des Zeitstempels im Systemprotokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Keine Systemzeitangabe. • <i>Zeit</i>: Systemzeit ohne Datum. • <i>Datum & Uhrzeit</i>: Systemzeit mit Datum.
Protokoll	<p>Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>UDP</i> (Standardwert) • <i>TCP</i>
Nachrichtentyp	<p>Wählen Sie den Nachrichtentyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System & Accounting</i> (Standardwert) • <i>System</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> Accounting

22.2 IP-Accounting

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

Aber auch nicht-kommerzielle Zwecke sprechen für ein detailliertes 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.

22.2.1 Schnittstellen

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



Abb. 183: Externe Berichterstellung ->IP-Accounting->Schnittstellen

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

22.2.2 Optionen

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

Abb. 184: 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
%l	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]
```

22.3 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.

22.3.1 Benachrichtigungsempfänger

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

22.3.1.1 Neu

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

Benachrichtigungsempfänger
Benachrichtigungseinstellungen

Benachrichtigungsempfänger hinzufügen/bearbeiten	
Benachrichtigungsdienst	E-Mail
Empfänger	<input style="width: 90%;" type="text"/>
Nachrichtenkomprimierung	<input checked="" type="checkbox"/> Aktiviert
Betreff	<input style="width: 90%;" type="text"/>
Ereignis	Systemmeldung enthält Zeichenfolge ▼
Enthaltene Zeichenfolge	<input style="width: 90%;" type="text"/> (Wildcards zulässig)
Schweregrad	Notfall ▼
Überwachte Subsysteme	<div style="border: 1px solid gray; padding: 2px; display: inline-block;">Subsystem</div> <div style="border: 1px solid gray; padding: 2px; display: inline-block; margin-top: 2px;">Hinzufügen</div>
Timeout für Nachrichten	<input style="width: 50%;" type="text" value="60"/>
Anzahl Nachrichten	<input style="width: 50%;" type="text" value="1"/>

OK
Abbrechen

Abb. 185: 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.
Empfänger	Geben Sie die E-Mail-Adresse des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Nachrichtenkomprimierung	<p>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.</p> <p>Aktivieren oder deaktivieren Sie das Feld.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Betreff	Sie können einen Betreff eingeben.
Ereignis	<p>Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Systemmeldung enthält Zeichenfolge</i> (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. • <i>Neuer Neighbor-AP gefunden</i>: Ein neuer benachbarter AP wurde gefunden. • <i>Neuer Rogue-AP gefunden</i>: Ein neuer Rogue AP wurde gefunden, d. h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • <i>Neuer Slave-AP (WTP) gefunden</i>: Eine neuer unkonfiguriertes AP hat sich beim WLAN Controller gemeldet. • <i>Verwalteter AP offline</i>: Ein managed AP ist nicht mehr erreichbar.
Enthaltene Zeichenfolge	<p>Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms.</p> <p>Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "**") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichen-</p>

Feld	Beschreibung
	<p>folge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.</p>
<p>Schweregrad</p>	<p>Wählen Sie den Schweregrad aus, auf dem der im Feld Enthaltene Zeichenfolge konfigurierte String vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird.</p> <p>Mögliche Werte:</p> <p><i>Notfall (Standardwert), Alarm, Kritisch, Fehler, Warnung, Benachrichtigung, Informationen, Debug</i></p>
<p>Überwachte Subsysteme</p>	<p>Wählen Sie die Subsysteme aus, die überwacht werden sollen.</p> <p>Fügen Sie mit Hinzufügen neue Subsysteme hinzu.</p>
<p>Timeout für Nachrichten</p>	<p>Geben Sie ein, wie lange der Router nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Benachrichtigungsmails erzwungen wird.</p> <p>Zur Verfügung stehen Werte von 0 bis 86400. Ein Wert von 0 deaktiviert den Timeout.</p>
<p>Anzahl Nachrichten</p>	<p>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.</p> <p>Zur Verfügung stehen Werte von 0 bis 99, Standardwert ist 1.</p>

22.3.2 Benachrichtigungseinstellungen

Benachrichtigungsempfänger
Benachrichtigungseinstellungen

Basisparameter	
Benachrichtigungsdienst	<input checked="" type="checkbox"/> Aktiviert
Maximale Nachrichtenzahl pro Minute	6 <small>▼</small>
E-Mail-Parameter	
E-Mail-Adresse	<input type="text"/>
SMTP-Server	<input type="text"/>
SMTP-Authentifizierung	<input checked="" type="radio"/> Keine <input type="radio"/> ESMTP <input type="radio"/> SMTP after POP

Abb. 186: 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 <i>Aktiviert</i> 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	<p>Authentifizierung, die der SMTP-Server erwartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung. • <i>ESMTP</i>: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt. • <i>SMTP after POP</i>: 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	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.</p>
Passwort	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie das Passwort dieses Benutzers an.</p>
POP3-Server	<p>Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i></p> <p>Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.</p>
POP3-Timeout	<p>Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i></p> <p>Geben Sie ein, wie lange der Router nach dem POP3-Abruf maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird.</p> <p>Standardwert ist <i>600</i> Sekunden.</p>

22.4 SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll in der IP-Protokollfamilie für den Transport von Managementinformationen über Netzwerkkomponenten.

Zu den Bestandteilen eines jeden SNMP-Managementsystems zählt u. a. eine MIB. Über SNMP sind verschiedene Netzwerkkomponenten von einem System aus zu konfigurieren, zu kontrollieren und zu überwachen. Mit Ihrem Gerät haben Sie ein solches SNMP-Werkzeug erhalten, den Konfigurationsmanager. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HPOpenView verwenden.

Weitergehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

22.4.1 SNMP-Trap-Optionen

Zur Überwachung des Systems wird im Fehlerfall unaufgefordert eine Nachricht gesendet, ein sogenanntes Trap-Paket.

Im Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Optionen** können Sie das Senden von Traps konfigurieren.

SNMP-Trap-Optionen SNMP-Trap-Hosts

Basisparameter	
SNMP Trap Broadcasting	<input checked="" type="checkbox"/> Aktiviert
SNMP-Trap-UDP-Port	162
SNMP-Trap-Community	snmp-Trap

OK Abbrechen

Abb. 187: 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	<p>Wählen Sie aus, ob die Übertragung von SNMP-Traps aktiviert werden soll.</p> <p>Ihr Gerät sendet SNMP-Traps dann an die Broadcast-Adresse des LANs.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
SNMP-Trap-UDP-Port	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p> <p>Geben Sie die Nummer des UDP-Ports ein, zu dem Ihr Gerät SNMP-Traps senden soll.</p> <p>Möglich ist jeder ganzzahlige Wert.</p> <p>Standardwert ist <i>162</i>.</p>
SNMP-Trap-Community	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p> <p>Geben Sie eine SNMP-Kennung ein. Diese muss vom SNMP-Manager mit jeder SNMP-Anforderung übergeben werden, damit sie von Ihrem Gerät akzeptiert wird.</p> <p>Möglich ist eine Zeichenkette mit <i>0</i> bis <i>255</i> Zeichen.</p> <p>Standardwert ist <i>SNMP-Trap</i>.</p>

22.4.2 SNMP-Trap-Hosts

In diesem Menü geben Sie an, an welche IP-Adressen Ihr Gerät die SNMP-Traps schicken soll.

Im Menü **Externe Berichterstellung** -> **SNMP** -> **SNMP-Trap-Hosts** wird eine Liste aller konfigurierten SNMP-Trap-Hosts angezeigt.

22.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

The image shows a software dialog box with two tabs: "SNMP-Trap-Optionen" (highlighted) and "SNMP-Trap-Hosts". The "SNMP-Trap-Optionen" tab contains a "Basisparameter" section with an "IP-Adresse" input field. At the bottom of the dialog are "OK" and "Abbrechen" buttons.

Abb. 188: **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 23 Monitoring

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

23.1 Internes Protokoll

23.1.1 Systemmeldungen

Im Menü **Monitoring->Internes Protokoll->Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die 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.

Systemmeldungen

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden <input type="button" value="Übernehmen"/>					
Maximale Anzahl der Syslog-Protokolleinträge					50
Maximales Nachrichtenlevel von Systemprotokolleinträgen					Informationen
Ansicht <input type="text" value="20"/> pro Seite <input type="button" value="«"/> <input type="button" value="»"/> Filtern in <input type="text" value="Keiner"/> <input type="button" value="gleich"/> <input type="button" value="Los"/>					
Nr.	Datum	Zeit	Level	Subsystem	Nachricht
1	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
2	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
3	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
4	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
5	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas5Ghz not found
6	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas5Ghz
7	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanVSSTable
8	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanIFTable
9	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
10	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
11	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
12	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
13	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas5Ghz not found
14	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas5Ghz
15	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanVSSTable
16	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanIFTable
17	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
18	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
19	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
20	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.Jnci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
Seite: 1, Objekte: 1 - 20, Summe der Objekte: 43					

Abb. 189: 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 Aufzeichnung an.
Zeit	Zeigt die Uhrzeit der Aufzeichnung an.
Level	Zeigt die hierarchische Einstufung der Meldung an.
Subsystem	Zeigt an, welches Subsystem Ihres Geräts die Meldung generiert hat.
Nachricht	Zeigt den Meldungstext an.

23.2 IPsec

23.2.1 IPSec-Tunnel

Im Menü **Monitoring->IPSec->IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.

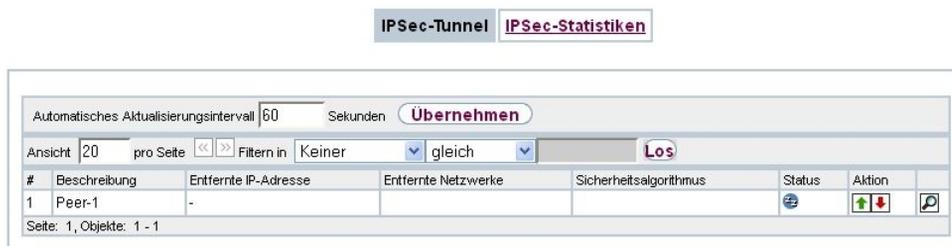


Abb. 190: **Monitoring->IPSec->IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

Durch Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der IPSec-Verbindung geändert.

Durch Drücken der -Schaltfläche wird eine ausführliche Statistik zu der jeweiligen IPSec-Verbindung angezeigt.

IPSec-Tunnel		IPSec-Statistiken	
Automatisches Aktualisierungsintervall		60	Sekunden Übernehmen
Allgemein			
Beschreibung	Peer-1		
Lokale IP-Adresse	0.0.0.0		
Entfernte IP-Adresse	0.0.0.0		
Lokale ID			
Entfernte ID			
Aushandlungsmodus			
Authentifizierungsmethode			
MTU	1418		
Erreichbarkeitsprüfung			
Statistik	Eingehend	Ausgehend	
Pakete	0	0	
Bytes	0	0	
Fehler	0	0	
Nachrichten (0)			

Abb. 191: 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.

23.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

IPSec-Tunnel IPSec-Statistiken

Automatisches Aktualisierungsintervall		60	Sekunden		Übernehmen
Lizenzen			In Verwendung	Maximal	
IPSec-Tunnel			0	110	
Peers	Aktiv	Aktivieren	Blockiert	Ruhend	Konfiguriert
Status	0	0	0	1	1
SAs		Hergestellt	Gesamt		
IKE (Phase-1)		0	0		
IPSec (Phase-2)		0	0		
Paketstatistiken		Eingehend	Ausgehend		
Gesamt		59	136		
Weitergeleitet		59	136		
Verworfen		0	0		
Verschlüsselt		0	0		
Fehler		0	0		

Abb. 192: **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	<p>Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an.</p> <ul style="list-style-type: none"> • 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.

23.3 ISDN/Modem

23.3.1 Aktuelle Anrufe

Im Menü **Monitoring->ISDN/Modem->Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.



Abb. 193: **Monitoring->ISDN/Modem->Aktuelle Anrufe**

Werte in der Liste Aktuelle Anrufe

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden ist: <i>PPP, IPSec, X.25, POTS.</i>
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: <i>Eingehend, Ausgehend.</i>
Kosten	Zeigt die Kosten der laufenden Verbindung an.
Dauer	Zeigt die Dauer der laufenden Verbindung an.
Stack	Zeigt den zugehörigen ISDN-Port (STACK) an.
Kanal	Zeigt die Nummer des ISDN-B-Kanals an.
Status	Zeigt den Status der Verbindung an: <i>null, c-initiated, ovl-send, oc-procd, c-deliverd, c-present, c-recvd, ic-procd, aktiv, discon-req, discon-ind, suspd-req, resum-req, ovl-recv.</i>

23.3.2 Anrufliste

Im Menü **Monitoring->ISDN/Modem->Anrufliste** wird eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

Aktuelle Anrufe
Anrufliste

Automatisches Aktualisierungsintervall Sekunden
 Übernehmen

Ansicht pro Seite

 Filtern in

#	Dienst	Entfernte Nummer	Schnittstelle	Richtung	Kosten	Startzeit	Dauer
Seite: 1							

Abb. 194: Monitoring->ISDN/Modem->Anrufliste

Werte in der Liste Anrufliste

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden war: <i>PPP, IPsec, X.25, POTS.</i>
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: <i>Eingehend, Ausgehend.</i>
Kosten	Zeigt die Kosten der Verbindung an.
Startzeit	Zeigt die Uhrzeit an, zu welcher der Ruf aus- bzw. einging.
Dauer	Zeigt die Dauer der Verbindung an.

23.4 Schnittstellen

23.4.1 Statistik

Im Menü **Monitoring->Schnittstellen->Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. In der Anzeige **Transferdurchsatz** werden die Werte pro Sekunde angezeigt.

Statistik

Anzeigen <input type="text" value="Gesamttransfer"/> Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden <input type="button" value="Übernehmen"/>											
Ansicht <input type="text" value="20"/> pro Seite <input type="button" value="Filtern in"/> <input type="text" value="Keiner"/> <input type="text" value="gleich"/> <input type="button" value="Los"/>											
Nr.	Beschreibung	Typ	Tx-Pakete	Tx-Bytes	Tx-Fehler	Rx-Pakete	Rx-Bytes	Rx-Fehler	Status	Nicht geändert seit	Aktion
1	en1-4	Ethernet	0	0	0	0	0	0		6d 22h 42m 24s	
2	en1-0	Ethernet	3.87K	3.75M	0	2.80K	483.09K	0		1d 0h 57m 51s	
3	Peer-1	Tunnel	0	0	0	0	0	0		0d 0h 4m 25s	

Seite: 1, Objekte: 1 - 3

Abb. 195: **Monitoring->Schnittstellen->Statistik**

Durch Drücken der -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 zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

Statistik

Anzeigen	Gesamttransfer	<input checked="" type="checkbox"/> Automatisches Aktualisierungsintervall	300	Sekunden	Übernehmen
Beschreibung	en1-0				
MAC-Adresse	00:a0:f9:21:ef:16				
IP-Adresse / Netzmaske	0.0.0.0 / 0.0.0.0				
NAT	Deaktiviert				
Tx-Pakete	5.658				
Tx-Bytes	5.840.808				
Rx-Pakete	252.517				
Rx-Bytes	147.957.968				
TCP-Verbindungen					
Status	Lokale Adresse	Lokaler Port	Remote-Adresse	Entfernter Port	

Abb. 196: Monitoring->Schnittstelle->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.
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.

23.5 Bridges

23.5.1 br<x>

Im Menü **Monitoring->Bridges->br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

br0

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen	
MAC-Adresse	Port
00:a0:f9:0b:08:98	en1-0

Abb. 197: **Monitoring->Bridges**

Werte in der Liste br<x>

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adressen der assoziierten Bridges an.
Port	Zeigt den Port an, auf dem die Bridge aktiv ist.

23.6 Hotspot-Gateway

23.6.1 Hotspot-Gateway

Im Menü **Monitoring->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

Hotspot-Gateway

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen				
Authentifizierter Hotspot-Benutzer				
Benutzername	IP-Adresse	Physische Adresse	Anmeldung	Schnittstelle

Abb. 198: **Monitoring->Hotspot-Gateway->Hotspot-Gateway**

Werte in der Liste Hotspot-Gateway

Feld	Beschreibung
Benutzername	Zeigt den Namen des Benutzers an.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Physische Adresse	Zeigt die Physische Adresse des Benutzers an.
Anmeldung	Zeigt den Zeitpunkt der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

23.7 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

23.7.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

QoS

QoS				
Schnittstelle	QoS-Queue	Senden	Verworfen	Queued

Abb. 199: **Monitoring->QoS->QoS**

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

23.8 OSPF

Im Menü **Monitoring->OSPF** werden Informationen zu OSPF überwacht. Der OSPF-Monitor ist horizontal in drei Bereiche gegliedert und zeigt Informationen zu OSPF-Schnittstellen, den erkannten Nachbarn sowie die Link State Database Einträge.

23.8.1 Status

Im Menü **Monitoring->OSPF->Status** wird eine Liste aller Schnittstellen angezeigt, für die OSPF konfiguriert wurde.

Abb. 200: **Monitoring->OSPF->Status**

Werte in der Liste Status

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: <i>Alle, OSPF-Schnittstellen, OSPF-Nachbarn und OSPF Link State Database</i>

Im Bereich **OSPF-Schnittstellen** sind alle aktivierten OSPF-Interfaces aufgelistet:

Werte in der Liste OSPF-Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die OSPF konfiguriert wurde.
Designated Router (DR)	<p>Zeigt die IP-Adresse des Designated Routers an.</p> <p>Der Designated Router generiert Network Links und verteilt diese an alle Gateways innerhalb des BMA-Netzwerkes (BMA = Broadcast Multi Access Network, z.B. Ethernet, FDDI, Tokenring).</p> <p>Ein Designated Router wird bei None BMA-Netzwerken, z.B. X.25, Frame Relay, ATM, nicht angezeigt.</p>
Backup Designated Router (BDR)	Zeigt die IP-Adresse des Backup Designated Routers an.
Admin-Status	Zeigt den OSPF-Admin-Status (<i>Aktiviert</i> oder <i>Deaktiviert</i>) der Schnittstelle an.
Status	<p>Der hier angezeigte OSPF-Status der Schnittstelle kann folgende Werte annehmen:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>: OSPF läuft nicht auf dieser Schnittstelle. • <i>Wartend</i>: Die Initialphase des OSPF, in der DR und BDR bestimmt werden. • <i>Punkt-zu-Punkt</i>: Die Schnittstelle ist eine Point-To-Point-Schnittstelle. DR oder BDR werden nicht angezeigt. • <i>Designated Router</i>: Das Gateway ist der Designated Router innerhalb des BMA-Netzwerkes. • <i>Designated Router Backup</i>: Das Gateway ist der Backup Designated Router innerhalb des BMA-Netzwerkes. • <i>Anderer Designated Router</i>: Ein anderes Gateway ist Designated Router oder Backup Designated Router innerhalb des BMA-Netzwerkes.

Im Bereich **Nachbar** werden die Nachbar-Gateways aufgelistet, die über das HELLO Protokoll identifiziert wurden:

Werte in der Liste OSPF-Nachbarn

Feld	Beschreibung
Nachbar	Zeigt die IP-Adresse des Nachbar-Gateways an.
Router-ID	Zeigt die systemweite Router-ID des Nachbar-Gateways an.
Schnittstelle	Zeigt die Schnittstelle an, über das dieses Nachbar-Gateway identifiziert wurde.

Feld	Beschreibung
Status	<p>Der OSPF-Status mit diesem Nachbar-Gateway kann folgende Werte annehmen:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>: Die Verbindung zu diesem OSPF-Nachbarn ist inaktiv. • <i>Init</i>: Die Initialphase. Ein HELLO Paket wird vom Nachbarn empfangen. • <i>Bidirectional</i>: Bidirektionale Kommunikation mit dem Nachbarn. Die übermittelten HELLO Pakete sind vom Nachbar-Gateway angenommen worden (mit korrekten Parametern). • <i>Austausch starten</i>: Der Austausch von Database Description Paketen zwischen den Gateways hat begonnen. • <i>Austausch</i>: Aktiver Austausch von Database Description Paketen mit dem Nachbarn. • <i>Laden</i>: Das Gateway tauscht nun Link State Advertisements mit dem Nachbarn aus. • <i>Fertig</i>: Die Link State Datenbanken des Gateways und seines Nachbarn sind nun synchronisiert.

Im Bereich für die Link State Database werden die Header aller Link State Advertisements (LSA) aufgelistet.

Werte in der Liste OSPF Link State Database

Feld	Beschreibung
Bereich	Zeigt die Bereichsdatenbank an, der das LSA zugeordnet ist.
Typ	Zeigt den LSA-Typ an. Es gibt fünf LSA-Typen: Router Link, Network Link, Summary Link, Summary ASBR, und AS External.
Link-Status-ID	Zeigt die Link State ID des LSA an. Die Bedeutung der Link State ID hängt vom Typ des Advertisements ab.
Router-ID	Identifiziert das Gateway, das dieses LSA generiert hat.
Sequence Age	Zeigt das Alter des LSA (in Sekunden) an.

23.8.2 Statistik

Im Menü **Monitoring+OSPF+Statistik** werden die aktuellen Werte und Aktivitäten angezeigt.

Status Statistik

Empfangene Hello Nachrichten	0
Gesendete Hello Nachrichten	0
Empfangene Database Description Pakets	0
Gesendete Database Description Pakets	0
Empfangene Link State Acknowledge Pakets	0
Gesendete Link State Acknowledge Pakets	0
Empfangene Link State Request Pakets	0
Gesendete Link State Request Pakets	0
Empfangene Link State Update Pakets	0
Gesendete Link State Update Pakets	0
Aktualisierung der Routing-Tabelle aufgrund von Summary Link Advertisements	0
Updates der Routing-Tabelle aufgrund von External Advertisements	0

Abb. 201: Monitoring+OSPF+Statistik

Werte in der Liste Statistik

Feld	Beschreibung
Empfangene Hello Nachrichten	Zeigt die Anzahl der empfangenen Hello-Pakete an.
Gesendete Hello Nachrichten	Zeigt die Anzahl der gesendeten Hello-Pakete an.
Empfangene Database Description Pakets	Zeigt die Anzahl der empfangenen Datenbankeinträge.
Gesendete Database Description Pakets	Zeigt die Anzahl der gesendeten Datenbankeinträge.
Empfangene Link State Acknowledge Pakets	Zeigt die Anzahl der empfangenen Link State Acknowledge Pakete.
Gesendete Link State Acknowledge Pakets	Zeigt die Anzahl der gesendeten Link State Acknowledge Pakete.
Empfangene Link State Request Pakets	Zeigt die Anzahl der empfangenen Link State Request Pakete.
Gesendete Link State Request Pakets	Zeigt die Anzahl der gesendeten Link State Request Pakete.
Empfangene Link State Update Pakets	Zeigt die Anzahl der empfangenen Link State Update Pakete.
Gesendete Link State Update Pakets	Zeigt die Anzahl der gesendeten Link State Update Pakete.

Feld	Beschreibung
Aktualisierung der Routing-Tabelle aufgrund von Summary Link Advertisements	Zeigt die Anzahl der inkrementellen Routing-Tabellen-Updates an, die durchgeführt wurden, wenn neue Summary Link Advertisements empfangen wurden.
Updates der Routing-Tabelle aufgrund von External Advertisements	Zeigt die Anzahl der inkrementellen Routing-Tabellen-Updates an, die durchgeführt wurden, wenn neue externe Advertisements empfangen wurden.

23.9 PIM

23.9.1 Allgemeine Statusangaben

Im Menü **Monitoring+PIM+Allgemeine Statusangaben** wird der Status aller konfigurierbaren PIM Komponenten angezeigt.

[Allgemeine Statusangaben](#)
[Nicht-schnittstellen-spezifischer Status](#)
[Schnittstellenspezifische Zustände](#)

The screenshot shows the 'Allgemeine Statusangaben' page with three main sections:

- PIM-Schnittstellen:** Table with columns: Schnittstelle, IP-Adresse, Designated Router (DR). Filter: Keiner, gleich. Los button.
- PIM-Nachbarn:** Table with columns: Schnittstelle, Generation ID, IP-Adresse, Uptime, Expiry Timer. Filter: Keiner, gleich. Los button.
- Zuordnung Multicast-Gruppen zu RPs:** Table with columns: Multicast-Gruppen-Adresse, Präfixlänge der Multicast-Gruppe, IP-Adresse des Rendezvous Points. Filter: Keiner, gleich. Los button.

Abb. 202: Monitoring+PIM+Allgemeine Statusangaben

Werte in der Liste Allgemeine Statusangaben

Feld	Beschreibung
Ansicht	<p>Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus.</p> <p>Zur Auswahl stehen: <i>Alle, PIM-Schnittstellen, PIM-</i></p>

Feld	Beschreibung
	<i>Nachbarn und Zuordnung Multicast-Gruppen zu RPs</i>

Werte in der Liste PIM-Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der PIM-Schnittstelle an.
IP-Adresse	Zeigt die primäre IP-Adresse der PIM-Schnittstelle an.
Designated Router (DR)	Zeigt die primäre IP-Adresse des Designated Routers auf dieser PIM-Schnittstelle an.

Werte in der Liste PIM-Nachbarn

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, über die der PIM Neighbor erreicht wird.
Generation ID	Zeigt die ID des Nachbar-Gateways an.
IP-Adresse	Zeigt die primäre IP-Adresse des PIM Neighbors an.
Uptime	Zeigt an, wie lange der letzte PIM Neighbor ein Nachbar des lokalen Routers ist.
Expiry Timer	Zeigt an, wann der PIM Neighbor nicht mehr als Nachbar eingetragen ist. Wird der Wert 0 angezeigt, bleibt der PIM Neighbor immer als Nachbar eingetragen.

Werte in der Liste Zuordnung Multicast-Gruppen zu RPs

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Präfixlänge der Multicast-Gruppe	Zeigt die dazugehörige Präfixlänge an.
IP-Adresse des Rendezvous Points	Zeigt die IP-Adresse des Rendezvous Points an.

23.9.2 Nicht-schnittstellen-spezifischer Status

Das Menü **Monitoring+PIM+Nicht-schnittstellen-spezifischer Status** enthält Status-Angaben für alle PIM-Schnittstellen.

Allgemeine Statusangaben
Nicht-schnittstellen-spezifischer Status
Schnittstellenspezifische Zustände

Ansicht: Alle

(*,*,RP) Status

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los

IP-Adresse des Rendezvous Point Upstream Join State Upstream Nachbar-IP-Adresse Uptime Upstream Join Timer

Seite: 1

(*,G) Status

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los

Multicast-Gruppen-Adresse Upstream Nachbar-IP-Adresse Reverse-Path-Forwarding (RPF) Upstream Join State Uptime Upstream Join Timer

Seite: 1

(S,G) Status

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los

Multicast-Gruppen-Adresse Quell-IP-Adresse Upstream Nachbar-IP-Adresse Upstream Join State Uptime Upstream Join Timer Shortest Path Tree

Seite: 1

(S,G,RPT) Status

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los

Multicast-Gruppen-Adresse Quell-IP-Adresse Reverse-Path-Forwarding (RPF) Uptime Upstream Override Timer

Seite: 1

Abb. 203: **Monitoring+PIM+Nicht-schnittstellen-spezifischer Status**

Werte in der Liste Nicht-schnittstellen-spezifischer Status

Feld	Beschreibung
Ansicht	<p>Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus.</p> <p>Zur Auswahl stehen: <i>Alle, (*,*,RP) Status, (*,G) Status, (S,G) Status</i> und <i>(S,G,RPT) Status</i></p>

Werte in der Liste (*,*,RP) Status

Feld	Beschreibung
IP-Adresse des Rendezvous Point	Zeigt die IP-Adresse des Rendezvous Point (RP) der Gruppe an.
Upstream Join State	Der Upstream (*,*,RP) Join/Prune Status gibt den Status der Upstream (*,*,RP) State Machine in der PIM-SM Spezifikation wieder.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Upstream Neighbors, oder unknown(0), wenn die Upstream Neighbor IP-Adresse nicht bekannt ist oder es sich nicht um einen PIM Neighbor handelt.
Uptime	Zeigt den Zeitraum an, wie lange der RP besteht.

Feld	Beschreibung
Upstream Join Timer	Der Join/Prune Timer wird verwendet, um periodisch Join(*,*,RP) Nachrichten zu senden, und um Prune(*,*,RP) Nachrichten von Peers auf einer Upstream LAN Schnittstelle zu korrigieren.

Werte in der Liste (*,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Upstream Nachbar-IP-Adresse	Zeit die primäre IP-Adresse des Neighbors auf pimStarGRPFIIndex an, zu der der lokale Router periodisch (*,G) Join Nachrichten schickt. Der InetAddressTyp ist durch das Objekt pimStarGUpstreamNeighborType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF(*,G) genannt.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der Next Hop nicht bekannt ist.
Upstream Join State	Zeigt an, ob der lokale Router dem RP Tree der Gruppe beitreten soll. Dieses entspricht dem Status der Upstream (*,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (*,G) Join Nachricht auf pimStarGRPFIIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Upstream Join Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimSGAddressType definiert.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Neighbors auf pimSGRPFIIndex an, zu dem der Router periodisch (S,G) Join Nachrichten schickt. Der Wert ist 0, wenn der RPF Next Hop nicht bekannt oder kein PIM Neighbor ist. InetAddressType wird im Objekt pimSGAddressType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF(S,G) genannt.

Feld	Beschreibung
Upstream Join State	Zeigt an, ob der lokale Router den Shortest-Path-Tree für die Quelle und die Gruppe, die durch diesen Eintrag dargestellt wird, beitreten soll. Dieses entspricht dem Status der Upstream (S,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (S,G) Join Nachricht auf pimSGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Upstream Join Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.
Shortest Path Tree	Zeigt an, ob das Shortest Path Tree Bit gesetzt ist, d.h. ob das Forwarding über den Shortest Path Tree stattfinden soll.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der RPF Next Hop nicht bekannt ist.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Override Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste Triggered (S,G,rpt) Join Nachricht auf pimStarGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Upstream Override Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

23.9.3 Schnittstellenspezifische Zustände

Das Menü **Monitoring+PIM+Schnittstellenspezifische Zustände** enthält schnittstellenspezifische Status-Angaben.

Allgemeine Statusangaben	Nicht-schnittstellen-spezifischer Status	Schnittstellenspezifische Zustände
Ansicht: -Alle-		
(*,G,I) Status		
Ansicht: 20	pro Seite: << >>	Filtern in: Keiner
		gleich
Multicast-Gruppen-Adresse	Schnittstelle	Join/Prune-Status
		Uptime
		Expiry Timer
		Assert-Status
		IP-Adresse des Assert Winner
Seite: 1		
(S,G,I) Status		
Ansicht: 20	pro Seite: << >>	Filtern in: Keiner
		gleich
Multicast-Gruppen-Adresse	Quell-IP-Adresse	Schnittstelle
		Join/Prune-Status
		Uptime
		Expiry Timer
		Assert-Status
		IP-Adresse des Assert Winner
Seite: 1		
(S,G,Rpt,I) Status		
Ansicht: 20	pro Seite: << >>	Filtern in: Keiner
		gleich
Multicast-Gruppen-Adresse	Quell-IP-Adresse	Schnittstelle
		Uptime
		Join/Prune-Status
		Expiry Timer
Seite: 1		

Abb. 204: Monitoring+PIM+Schnittstellenspezifische Zustände

Werte in der Liste Schnittstellenspezifische Zustände

Feld	Beschreibung
Ansicht	<p>Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus.</p> <p>Zur Auswahl stehen: <i>Alle</i>, <i>(*,G,I) Status</i>, <i>(S,G,I) Status</i> und <i>(S,G,RPT) Status</i></p>

Werte in der Liste (*,G,I) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (*,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden. Dieses entspricht dem Status der Downstream Per-Interface (*,G) State Machine in the PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (*,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Join Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFF'h steht für unendlich.

Feld	Beschreibung
Assert-Status	Zeigt den (*,G) Assert State für diese Schnittstelle. Dieser entspricht dem Status der Per-Interface (*,G) Assert State Machine in der PIM-SM Spezifikation. Wenn pimStarGPimMode 'bidir' ist, muss dieses Objekt 'holInfo' lauten.
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner an, wenn pimStarGIAssertState 'iAmAssertLoser' lautet. InetAddressType wird durch das Objekt pimStarGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (S,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden. Dieser entspricht dem Status der Downstream Per-Interface (S,G) State Machine in der PIM-SM und PIM-DM Spezifikation.
Uptime	Zeigt die Zeit an, die verbleibt, bevor der lokale Router auf eine (S,G) Prune Nachricht reagiert, die auf dieser Schnittstelle empfangen wird. Der Router wartet diese Zeit, um zu prüfen, ob ein anderer Downstream Router die Prune Nachricht korrigiert. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Prune-Pending Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Join Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation (S,G) Prune Timer genannt.
Assert-Status	Zeigt den (S,G) Assert State für diese Schnittstelle an. Dieser entspricht dem Status der Per-Interface (S,G) Assert State Machine in der PIM-SM Spezifikation Siehe "I-D.ietf-pim-sm-v2-new section 4.6.1"
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner, wenn pimSGIAssertState 'iAmAssertLoser lautet. InetAddressType wird durch das Objekt pimSGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Join/Prune-Status	Zeigt an, ob der lokale Router die Quelle des RP Tree abschneiden soll. Dieses entspricht in der PIM-SM Spezifikation dem Status der Upstream (S,G,rpt) State Machine für Triggered Messages.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G,rpt) Prune State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Prune Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation(S,G) Prune Timer genannt.

Glossar

100Base-T	Twisted-Pair-Anschluss, Fast Ethernet. Netzwerkanschluss für 100-MBit-Netze.
10Base-2	Thin-Ethernet-Anschluss. Netzwerkanschluss für 10-MBit-Netze mit dem Steckertyp BNC. Zum Anschluss von Geräten mit BNC-Buchsen werden T-Verbindungsstücke eingesetzt.
10Base-T	Twisted-Pair-Anschluss. Netzwerkanschluss für 10-MBit-Netze mit dem Steckertyp RJ45.
1TR6	Im deutschen ISDN verwendetes D-Kanal-Protokoll. Heute gängigeres Protokoll ist das DSS1.
3DES (Triple DES)	Siehe DES.
802.11a/g	Spezifiziert Datenraten von 54, 48, 36, 24, 18, 12, 9 und 6 Mbit/s und eine Arbeitsfrequenz im Bereich von 5 GHz (bei IEEE802.11a) bzw. 2,4 GHz (bei IEEE802.11g). IEEE802.11 g kann so konfiguriert werden, dass es zusätzlich zu 11b oder 11b und 11 kompatibel betrieben wird.
802.11b/g	Einer der IEEE Standards für drahtlose Netzwerk-Hardware. Produkte, die dem gleichen IEEE Standard entsprechen, können miteinander kommunizieren, selbst wenn sie von verschiedenen Hardware-Herstellern stammen. Der IEEE802.11b Standard spezifiziert Datenraten von 1, 2, 5,5 und 11 Mbit/s, eine Arbeitsfrequenz im Bereich von 2,4 bis 2,4835GHz und WEP Verschlüsselung. IEEE802.11 Funknetze werden auch Wi-Fi Netzwerke genannt.
A-Teilnehmer	Der A-Teilnehmer ist der Anrufer.
A-Telefonnummer unterdrücken (CLIR)	CLIP/CLIR: Calling Line Identification Presentation/Calling Line Identification Restriction
a/b-Schnittstelle	Zum Anschluss eines analogen Endgerätes. Bei einem ISDN-Endgerät (Terminaladapter) mit a/b-Schnittstelle wird ein angeschlossenes analoges Endgerät in die Lage versetzt, die unterstützten T-ISDN Leistungsmerkmale zu nutzen.
AAA	Authentication, Authorization, Accounting
Access List	Eine Regel, die eine Anzahl von Datenpaketen definiert, die vom Gateway übertragen bzw. nicht übertragen werden sollen.

Access Point	Eine aktive Komponente eines Netzwerks, das aus funkbasierten und optional zusätzlich aus kabelgebundenen Bestandteilen besteht. An einem Access Point (AP) können sich viele WLAN-Clients (Endgeräte) einbuchen und gegenseitig über den AP Daten austauschen. Bei optionalem Anschluss eines kabelgebundenen Ethernet, werden die Signale zwischen den beiden physikalischen Medien, dem funkbasierten Interface und dem kabelgebundenen Interface überbrückt (Bridging).
Accounting	Aufzeichnen von Verbindungsdaten, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.
Active Probing	Active Probing macht sich den Umstand zu Nutze, dass Access Points dem Standard nach auf Anfragen eines Clients antworten sollen. Clients versenden so genannte Probe-Requests auf allen Kanälen und warten auf Antworten eines in der Nähe befindlichen Access Points. Im Antwortpaket steht dann die SSID des Funk-LANs und ob WEP-Verschlüsselung verwendet wird.
Ad Hoc Netzwerk	Ein Ad Hoc Netzwerk bezeichnet eine Anzahl von Computern, die jeweils mit einem Wireless Adapter ein unabhängiges 802.11 WLAN bilden. Ad Hoc Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer Basis. Der Ad Hoc Modus wird auch als IBSS Modus bezeichnet (Independent Basic Service Set) und ist in kleinsten Netzen sinnvoll, z. B. wenn zwei Notebooks ohne Access Point miteinander vernetzt werden sollen.
ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
Alphanumerisches Display	Anzeigeeinheit z. B. beim Systemtelefon T-Concept PX722, die außer Ziffern auch Buchstaben und weitere Zeichen darstellen kann.
Amtsberechtigung	Telefonanlagen unterscheiden die folgenden "Amtsberechtigungen". Diese können in der Konfiguration für jeden Teilnehmer individuell eingerichtet werden.
Analoge Anschlüsse	Zum Anschluss analoger Endgeräte wie Telefon, Telefax und Anrufbeantworter.
Analoge Endgeräte	Endgeräte, die Sprache oder andere Informationen analog übertragen, sind z. B. Telefon, Faxgerät, Anrufbeantworter und Modem.
Analoge Sprach-	Für die Übermittlung von Sprache über das Telefon werden akusti-

übertragung	sche Schwingungen in kontinuierliche elektrische Signale umgewandelt, die über ein Leitungsnetz übertragen werden (digitale Sprachübertragung).
Anklopfen	Mit dem Leistungsmerkmal "Anklopfen" sind Sie auch während eines Telefonats für andere erreichbar. Ruft Sie ein weiterer Teilnehmer an, während Sie telefonieren, hören Sie den Anklopftön im Hörer Ihres Telefons. Sie können dann entscheiden, ob Sie Ihr bisheriges Gespräch fortführen oder mit dem Anklopfenden sprechen wollen.
Anklopfsperr	Soll das Leistungsmerkmal Anklopfen nicht genutzt werden, schalten Sie den Anklopferschutz ein. Während Sie ein Telefongespräch führen, wird dann einem weiteren Anrufer der Besetztton übermittelt.
Anlagenanschluss	Point-to-Point (Punkt-zu-Punkt)
Anlagenrufnummer	Zu einem Anlagenanschluss gehören eine Anlagenrufnummer und ein Rufnummernband. Mit Hilfe der Anlagenrufnummer erreichen Sie die TK-Anlage. Über eine Rufnummer des Rufnummernbands wird dann ein bestimmtes Endgerät der TK-Anlage ausgewählt.
Anruf auf einen besetzten Teilnehmer	Busy on busy = Besetzt bei Besetzt
Anruf heranzholen	Leistungsmerkmal von Telefonanlagen. Anrufe können an einem internen Endgerät entgegengenommen werden, das sich nicht in der aktiven Rufverteilung befindet.
Anrufbeantworter	Einen analogen Anrufbeantworter konfigurieren Sie unter "Endgerädetyp".
Anruferliste	Komfortable Telefone wie das Systemtelefon T-Concept PX722 bieten die Möglichkeit, Anrufwünsche während der Abwesenheit zu speichern.
Anruffilter	Leistungsmerkmal, z. B. vom Systemtelefon T-Concept PX722, von Komforttelefonen oder Anrufbeantwortern. Die Rufsignalisierung erfolgt nur bei bestimmten, vorher festgelegten Telefonnummern.
Anrufschutz	Ausschalten der akustischen Anrufsignalisierung: Ruhe vor dem Telefon.
Anrufvariante Tag / Nacht	Möglichkeit bei Telefonanlagen, die Rufverteilung über einen Kalender zu ändern. Nach Büroschluss ankommende Telefonanrufe werden zu einem personell noch besetzten Telefon oder zum Anrufbeantworter, Telefax weitergeleitet.

Anrufweitschaltung in der Telefonanlage	Die Telefonanlage gibt Ihnen mit dem Leistungsmerkmal der Anrufweitschaltung (AWS) die Möglichkeit, erreichbar zu bleiben, auch wenn Sie nicht in der Nähe Ihres Telefons sind. Dieses erreichen Sie durch automatisches Weiterleiten von Anrufen an die gewünschte interne oder externe Telefonnummer. Mit dem Konfigurationsprogramm können Sie festlegen, ob die Anrufweitschaltung in der Telefonanlage oder in der Vermittlungsstelle erfolgen soll. Die Anrufweitschaltung in der Vermittlungsstelle können Sie nutzen, wenn bestimmte Leistungen für Ihren Anschluss aktiviert sind. Auskunft darüber erhalten Sie bei Ihrem Berater der T-Com.
Anrufweitschaltung in der Vermittlungsstelle	Die Möglichkeiten der Anrufweitschaltung in der Vermittlungsstelle können Sie nur über Keypad nutzen, wenn bestimmte Leistungen für Ihren Anschluss aktiviert sind. Auskunft darüber erhalten Sie beim Berater der T-Com. Die Vermittlungsstelle verbindet den anrufenden Teilnehmer mit einem von Ihnen festgelegten externen Teilnehmer.
Anschluss analoger Endgeräte	Die Leistungsmerkmale für analoge Endgeräte lassen sich nur mit Endgeräten nutzen, die mit dem MFV -Wahlverfahren wählen und eine R- bzw. eine Flash-Taste besitzen.
Anschluss von ISDN-Endgeräten	In die am internen ISDN-Bus angeschlossenen ISDN-Endgeräte muss die interne Telefonnummer des jeweiligen Anschlusses als MSN eingetragen werden und nicht die externe Telefonnummer (Mehrfachrufnummer). Siehe in der Bedienungsanleitung für die ISDN-Endgeräte: MSN eintragen. Beachten Sie bitte, dass nicht alle im Handel angebotenen ISDN-Endgeräte die von der Telefonanlage bereitgestellten Leistungsmerkmale über ihre Tastenoberfläche nutzen können.
Anzeige der Telefonnummer des Anrufers	Voraussetzung für diese Leistung ist ein geeignetes Telefon. Die Übermittlung der Telefonnummer muss vom Anrufer freigeschaltet sein.
Anzeige und Ausgabe der Verbindungsdaten	Die Speicherung der Datensätze lässt sich über die Konfiguration für bestimmte oder auch alle Endgeräte festlegen. In der Werkseinstellung werden alle kommenden externen Verbindungen und alle von Ihnen eingeleiteten externe Gespräche gespeichert.
AOC-D	Anzeige während und am Ende der Verbindung.
AOC-D/E	Advice of Charge-During/End.
AOC-E	Anzeige nur am Ende der Verbindung.

ARP	Address Resolution Protocol
asynchron	Übertragungsverfahren, bei dem die Zeitabstände zwischen übertragenen Zeichen unterschiedlich lang sein können. Dadurch können Geräte miteinander kommunizieren, die nicht in gleichen Zeittakten arbeiten. Anfang und Ende der übertragenen Zeichen müssen durch Start- und Stop-Bits gekennzeichnet sein – im Gegensatz zu synchron.
ATM	Asynchronous Transfer Mode
Aufmerksamkeitston	Einblenden eines akustischen Signals in laufende Telefongespräche z. B. beim Anklopfen.
Aufschalten	Möglichkeit bei Telefonanlagen, sich in eine bestehende Gesprächsverbindung einzublenden. Dies wird akustisch durch einen Aufmerksamkeitston signalisiert.
Authentication	Überprüfung der Identität des Nutzers (Authentisierung).
Authorization	Auf der Basis der Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
Auto Attendant	System für die automatische Weiterleitung eingehender Anrufe.
Automatische Amtsholung	Nach Abheben des Hörers an eines Telefons kann die Telefonnummer des Externteilnehmers sofort gewählt werden.
Automatische Wahlwiederholung	Leistungsmerkmal von Endgeräten. Im Besetztfall erfolgen automatisch mehrere Anwahlversuche.
Automatischer Abbau der Internetverbindung (ShortHold)	Sie haben die Möglichkeit, ShortHold einzuschalten. Dabei legen Sie eine Zeitspanne fest, nach der eine bestehende Verbindung getrennt wird, wenn kein Datentransfer mehr stattfindet. Wenn Sie hier die Zeitspanne 0 eintragen ist ShortHold ausgeschaltet.
Automatischer Rückruf	Komfortleistung bei Telefonen: Per Tastendruck oder Kennziffer fordert der Anrufer von einem besetzten Endgerät einen Rückruf an. Ist der gewünschte Teilnehmer nicht an seinem Platz oder kann er das Gespräch nicht annehmen, wird er automatisch mit dem Anrufer verbunden, sobald er sein Telefon das nächste Mal benutzt hat und den Hörer wieder auflegt.
Automatischer Rückruf bei Besetzt	Diese Funktion ist nur mit Telefonen nutzbar, die Nachwahl erlauben! Ein automatischer Rückruf ist aus einer Rückfrageverbindung nicht möglich.

Automatischer Rückruf bei Besetzt (CCBS)	Sie müssen dringend Ihren Geschäftspartner oder einen internen Teilnehmer erreichen. Bei einem Anruf auf dessen Anschluss hören Sie jedoch immer den Besetztton. Wenn Sie eine Mitteilung erhielten, dass der gewünschte Teilnehmer das Gespräch beendet hat, wären Ihre Chance, ihn zu erreichen sehr gut. Mit dem "Rückruf bei Besetzt" können Sie den besetzten Gesprächspartner sofort erreichen, wenn dieser am Ende seines Gespräches den Hörer auflegt. Ihr Telefon klingelt dann. Wenn Sie jetzt den Hörer abheben, wird automatisch eine Verbindung zum gewünschten Teilnehmer aufgebaut. Ein interner "Rückruf bei Besetzt" wird automatisch nach 30 Minuten gelöscht. Der externe "Rückruf bei Besetzt" wird nach einer von der Vermittlungsstelle vorgegebenen Zeit gelöscht (ca. 45 Minuten). Manuelles Löschen vor Ablauf der Zeit ist ebenfalls möglich.
Automatischer Rückruf bei Nichtmelden (CCNR)	Sie müssen dringend Ihren Geschäftspartner oder einen internen Teilnehmer erreichen. Bei einem Anruf auf dessen Anschluss hören Sie zwar immer den Freiton, Ihr Partner ist jedoch nicht in der Nähe seines Telefons und hebt nicht ab. Mit dem "Rückruf bei Nichtmelden" können Sie den Teilnehmer sofort erreichen, wenn dieser ein Gespräch beendet hat oder den Hörer seines Telefons abhebt und wieder auflegt. Ihr Telefon klingelt dann. Wenn Sie jetzt den Hörer abheben, wird automatisch eine Verbindung zum gewünschten Teilnehmer aufgebaut.
AUX	Auxiliary
B-Kanal	Basiskanal eines ISDN-Basisanschlusses bzw. Primärmultiplex-Anschlusses zur Übertragung von Nutzinformationen (Sprache, Daten). Ein ISDN-Basisanschluss besitzt zwei B-Kanäle und einen D-Kanal. Ein B-Kanal hat eine Datenübertragungsrate von 64 kBit/s. Durch Kanalbündelung kann mit Ihrem Gateway die Datenübertragungsrate bei einem ISDN-Basisanschluss auf bis zu 128 kBit/s gesteigert werden.
B-Telefonnummer unterdrücken (COLR)	COLP/COLR: Connected Line Identification Presentation/Connected Line Identification Restriction = Übermittlung der Telefonnummer des Anrufenden zum Angerufenen einschalten/unterdrücken. Mit diesem Leistungsmerkmal wird das Anzeigen der Telefonnummer des angerufenen Teilnehmers unterdrückt. Wird die Anzeige der B-Telefonnummer unterdrückt, wird nach Annahme eines Anrufes Ihre eigene Telefonnummer nicht zum Anrufenden übermittelt.
Back Route Verify	Überprüfung der Rückroute
BACP/BAP	Bandwidth Allocation Control Protocol (BACP/BAP nach RFC 2125)

Basisanschluss	ISDN-Anschluss, der zwei Nutzkanäle (B-Kanäle) von je 64 KBit/s und einen Steuerkanal (D-Kanal) mit 16 KBit/s umfasst. Die beiden Nutzkanäle können unabhängig voneinander für jeden im T-ISDN angebotenen Dienst genutzt werden. Man kann also z. B. telefonieren und zur gleichen Zeit faxen. Die T-Com bietet den Basisanschluss als Mehrgeräte- oder als Anlagenanschluss an.
Bedienerführung	Elektronische Bedienungsanleitung, die den Anwender per Display Schritt für Schritt zu gewünschten Funktionen eines Endgeräts wie z. B. Telefon, Anrufbeantworter oder Faxgerät führt (menügeführte Bedienung).
Bit	Binary Digit. Kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.
Block Cipher Modes	Blockorientierter Verschlüsselungsalgorithmus
Blowfish	Ein von Bruce Schneier entwickelter Algorithmus. Es handelt sich um eine Block Cipher mit einer Blockgröße von 64 Bit und einem Schlüssel mit variabler Länge (bis 448 Bit).
Bluetooth	Bluetooth ist eine drahtlose Übertragungstechnik, die verschiedene Geräte miteinander verbinden kann. Bluetooth ist dabei ein Kabelersatz zum Anschluss verschiedener Geräte, z. B. Notebook, PC, PDA, etc.. Diese Geräte können dank Bluetooth ohne eine feste Verbindung miteinander Daten austauschen. Zum Beispiel können PCs, Notebooks oder PDA Zugang zum Internet oder einem lokalen Netzwerk erlangen. Die Termine eines PDA können mit den Terminen auf dem PC synchronisiert werden, ohne dass hierfür eine Kabelverbindung erforderlich ist. Aufgrund der vielfältigen Anwendungsmöglichkeiten der Bluetooth-Technik werden die einzelnen Verbindungsarten zwischen den Geräten in Profiles unterteilt. Durch ein Profile wird der Dienst (die Funktion) festgelegt, den die einzelnen Bluetooth-Clients untereinander nutzen können.
BOD	Bandwith on Demand
BootP	Bootstrap Protocol
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Basic Rate Interface
Bridge	Netzwerkkomponente zum Verbinden gleichartiger Netze. Im Gegensatz zu einem Gateway arbeiten Bridges auf Schicht 2 des OSI-Modells, sind von höheren Protokollen unabhängig und übertragen

	Datenpakete anhand von MAC-Adressen. Die Datenübertragung ist transparent, d. h. die Informationen der Datenpakete werden nicht interpretiert.
Broadcast	Broadcasts sind Rundrufe (Datenpakete), die an alle im Netz angeschlossenen Geräte gesendet werden, um Informationen im Netz auszutauschen. Normalerweise gibt es im Netz eine bestimmte Adresse (Broadcast-Adresse), die es allen Geräten ermöglicht, eine Nachricht als Broadcast zu interpretieren.
Browser	Programm zur Darstellung von Inhalten im Internet bzw. WorldWide-Web.
Bündel	Die externen Anschlüsse größerer Telefonanlagen können zu Bündeln zusammengefasst werden. Bei der Einleitung eines externen Gespräches durch die Amtskennziffer oder bei automatischer Amtsholung wird beim Verbindungsaufbau ein für den Teilnehmer freigegebenes Bündel benutzt. Ist ein Teilnehmer für mehrere Bündel berechtigt, wird die Verbindung über das erste freigegebene Bündel aufgebaut. Ist ein Bündel belegt, wird das nächste freigegebene Bündel benutzt. Sind alle freigegebenen Bündel belegt, hört der Teilnehmer den Besetztton.
Bus	Ein Medium zur Datenübertragung für alle Geräte im Netz. Die Daten werden über den gesamten Bus verbreitet und von allen Geräten am Bus empfangen.
Busy On Busy	Anruf auf einen besetzten Team-Teilnehmer. Hat ein Teilnehmer eines Teams den Hörer abgehoben oder führt ein Gespräch, können Sie entscheiden, ob weitere Anrufe für dieses Team signalisiert werden sollen. Die Erreichbarkeit eines Teilnehmers kann zwischen "Standard" und "Busy On Busy" (Besetzt bei Besetzt) umgeschaltet werden. In der Grundeinstellung steht sie auf Standard. Ist Busy on Busy für ein Team eingerichtet, so erhalten weitere Anrufer Besetzt signalisiert.
CA	Certificate Authority
Call Through	Unter Call Through versteht man die Einwahl über einen externen Anschluss in die Telefonanlage und die Weiterwahl aus der Telefonanlage über einen anderen externen Anschluss.
Called Party's Number	Nummer des Angerufenen.
Calling Party's Num-	Nummer des Anrufers.

ber

CAPI Common ISDN Application Programming Interface

CAST Ein 128-bit Verschlüsselungsalgorithmus mit ähnlicher Funktionalität wie DES. Siehe Block Cipher Modes.

CBC Cipher Block Chaining

CCITT Commite Consultatif International Telegraphique et Telephonique

CD (Call Deflection) Weiterleiten von Anrufen. Mit diesem Leistungsmerkmal haben Sie die Möglichkeit, einen Anruf weiterzuleiten, ohne diesen selbst annehmen zu müssen. Leiten Sie einen Anruf zu einem externen Teilnehmer weiter, tragen Sie die anfallenden Verbindungskosten von Ihrem Anschluss zu dem Ziel der Anrufweiterleitung. Sie können dieses Leistungsmerkmal vom Systemtelefon nutzen, oder von ISDN-Telefonen, die diese Funktion unterstützen (siehe Bedienungsanleitung der Endgeräte). Weitere Hinweise zur Ausführung dieses Leistungsmerkmal mit dem Telefon entnehmen Sie bitte der Bedienungsanleitung.

Certificate Zertifikat

CHAP Challenge Handshake Authentication Protocol

CLID Calling Line Identification (Rufnummernüberprüfung)

Client Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.

CLIP Abkürzung für Calling Line Identification Presentation. Telefonnummernanzeige des Anrufenden.

CLIR Abkürzung für Calling Line Identification Restriction. Zeitweise Unterdrückung der Übermittlung der Telefonnummer des Anrufenden.

COLR Connected Line Identification Restriction (B-Telefonnummer unterdrücken). Mit diesem Leistungsmerkmal wird das Anzeigen der Telefonnummer des angerufenen Teilnehmers ermöglicht oder unterdrückt. Ist die Anzeige der B-Telefonnummer unterdrückt, wird nach Annahme eines Anrufes Ihre eigene Telefonnummer nicht zum Anrufenden übermittelt. Beispiel: Sie haben eine Rufumleitung zu einem anderen Endgerät eingerichtet. Hat dieses Endgerät das Unterdrücken der B-Telefonnummer eingeschaltet, sieht der Anrufende keine Telefonnummer im Display seines Endgerätes.

Configuration Manager	Windows-Applikation (ähnlich dem Windows-Explorer), die SNMP-Kommandos benutzt, um die Einstellungen Ihres Gateways abzufragen und vorzunehmen. Die Applikation wurde vor der BRICKware, Version 5.1.3, als DIME Browser bezeichnet.
CRC	Cyclic Redundancy Check
CRL	Zertifikatssperrliste, ermöglicht es festzustellen, ob ein Zertifikat gesperrt oder widerrufen wurde und warum.
CTI	Computer-Telephony Integration. Begriff für die Verbindung zwischen Telefonanlage und Server. Durch CTI können Funktionen der Telefonanlage von einem PC gesteuert bzw. ausgewertet werden.
D-Kanal	Steuerkanal eines ISDN-Basisanschlusses bzw. Primärmultiplexanschlusses. Der D-Kanal hat eine Datenübertragungsrate von 16 kBit/s. Außer dem D-Kanal besitzt jeder ISDN-Basisanschluss zwei B-Kanäle.
Daemon	Programm das im Hintergrund abläuft.
Datagramm	Ein in sich abgeschlossenes Datenpaket, das mit einem Minimum an Protokoll-Overhead im Netz weitergeleitet wird – ohne Quittierungsmechanismus.
Datenkompression	Methode, um übertragene Datenmengen zu verringern. Bei gleicher Übertragungsdauer kann so der Durchsatz erhöht werden. Bekannte Verfahren sind z. B. STAC, VJHC, MPPC.
Datenpaket	Ein Datenpaket dient der Übermittlung von Informationen. Jedes Datenpaket enthält eine vorgeschriebene Anzahl von Zeichen (Informationen und Steuerzeichen).
Datenübertragungsrates	Die Datenübertragungsrate gibt die Anzahl der Informationseinheiten pro Zeitabschnitt an, die zwischen Sender und Empfänger übertragen werden.
Datex-J	Abkürzung für Data Exchange Jedermann. Die Zugangsplattform zu T-Online. Lokale Einwahlknoten in jedem Ortsnetz. In einigen deutschen Großstädten gibt es zusätzliche Hochgeschwindigkeitszugänge über T-Net/T-Net-ISDN.
DCE	Data Circuit-Terminating Equipment
DECT	Digital European Cordless Telecommunication. Europäischer Standard für schnurlose Telefone und schnurlose Telefonanlagen. Zwischen mehreren Handgeräten können kostenfreie interne Gespräche

	<p>che geführt werden. Ein weiterer Vorteil ist die erhöhte Abhörsicherheit (GAP).</p>
Default Gateway	<p>Bezeichnet die Adresse des Routers, an den sämtlicher Verkehr gesendet wird, der nicht für das eigene Netzwerk bestimmt ist.</p>
Denial-Of-Service Attack	<p>Ein Denial-of-Service (DoS) Angriff ist ein Versuch, ein Gateway oder einen Host in einem LAN mit gefälschten Requests zu überfluten, so dass diese völlig überlastet sind. Das bedeutet: das System oder ein bestimmter Dienst kann nicht mehr betrieben werden.</p>
DES	<p>Data Encryption Standard</p>
DFÜ	<p>Datenfernübertragung</p>
DHCP	<p>Dynamic Host Configuration Protocol</p>
Dienste	<p>Im Euro-ISDN gibt es so genannte Dienste-Indikatoren, deren Namen festgelegt sind. Teilweise haben diese nur noch historische Bedeutung. Generell sollte man für "echte" Telefonate den Dienst "Fernsprechen" auswählen. Falls diese Auswahl nicht funktioniert (Netzbetreiberabhängig), kann man es mit "speech", "audio 3k1Hz" oder "telephony 3k1Hz" weiterversuchen. Das Gleiche gilt für den Faxbetrieb. Auch hier gibt es den Sammelbegriff Fax sowie einige Spezialunterscheidungen. Rein technisch sind die Dienste Bits in einem Datenwort, die über eine Maske ausgewertet werden. Wenn man in der Maske mehrere Bits einschaltet, werden alle diese Dienste zur Weiterschaltung zugelassen. Bei einem Bit entsprechend nur der eine ausgewählte Dienst.</p>
Digitale Sprachübertragung	<p>Durch die international genormte Puls Code Modulation (PCM) werden analoge Sprachsignale in einen digitalen Impulsstrom von 64 KBit/s umgewandelt. Vorteile: bessere Sprachqualität und geringere Störanfälligkeit als bei analoger Sprachübertragung.</p>
Digitale Vermittlungsstelle	<p>Ermöglicht durch computergesteuerte Koppelfelder den schnellen Verbindungsaufbau und die Aktivierung von Komfortleistungen wie Rückfragen, Anklopfen, Dreierkonferenz und Anrufweiterschaltung. Seit Januar 1998 sind alle Vermittlungsstellen der T-Com digitalisiert.</p>
DIME	<p>Desktop Internetworking Management Environment</p>
DIME Browser	<p>Alte Bezeichnung für Configuration Manager.</p>
Direktruf	<p>Sie befinden sich außer Haus. Es gibt jedoch jemanden bei Ihnen zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefo-</p>

nisch erreichen soll (z. B. Kinder oder Großeltern). Da Sie für ein Telefon oder für mehrere Telefone die Funktion Direktruf einrichten können, braucht lediglich der Hörer des entsprechenden Telefons abgehoben zu werden. Nach fünf Sekunden wählt die Telefonanlage automatisch die festgelegte Direktrufnummer, sofern Sie vorher nicht mit der Wahl einer anderen Nummer beginnen. Sie können in der Konfiguration des Direktrufs bis zu 12 Zielrufnummern eintragen. Eine Direktrufnummer ist jeweils nur von einem Teilnehmer nutzbar. Möchten Sie eine eingegebene Direktrufnummer ändern, können Sie die neue Direktrufnummer einfach eingeben, ohne die alte Direktrufnummer löschen zu müssen. Sie wird bei der Übertragung der geänderten Konfiguration zur Telefonanlage automatisch überschrieben.

DISA	Direct Inward System Access
DLCI	In einem Frame Relay Netzwerk bezeichnet ein DLCI eine virtuelle Verbindung eindeutig. Beachten Sie, dass ein DLCI nur für das lokale Ende der Punkt-zu-Punkt-Verbindung von Bedeutung ist.
DMZ	DeMilitarized Zone
DNS	Domain Name System
DOI	Domain Of Interpretation
Domäne	Ein Domäne ist ein logischer Zusammenschluss von Geräten in einem Netzwerk. Im Internet Teil einer Namenshierarchie (z. B. bintec.de).
Dotted Decimal Notation	Die syntaktische Repräsentation für eine 32-Bit-Ganzzahl, die in vier 8-Bit-Zahlen in dezimaler Schreibweise geschrieben ist und durch Punkt unterteilt ist. Sie wird zur Darstellung von IP-Adressen im Internet verwendet, z. B. 192.67.67.20
Download	Datentransfer bei Online-Verbindungen, wobei Dateien von einem PC oder einem Datennetz-Server in den eigenen PC, die Telefonanlage oder das Endgerät "geladen" werden, um sie dort weiterzuverwenden.
Downstream	Datenübertragungsrate vom ISP zum Kunden.
Dreierkonferenz	Telefonieren zu dritt. Leistungsmerkmal im T-Net, im T-ISDN und in Ihrer Telefonanlage.
DSA (DSS)	Digital Signature Algorithm (Digital Signature Standard).

DSL- und ISDN-Verbindungen	Der Datentransfer zwischen dem Internet und Ihrer Telefonanlage erfolgt über ISDN- oder T-DSL. Die Telefonanlage ermittelt, zu welcher Gegenstelle ein Datenpaket geschickt werden soll. Damit eine Verbindung ausgewählt und aufgebaut werden kann, müssen Parameter für alle notwendigen Verbindungen festgelegt werden. Diese Parameter sind in Listen abgelegt, deren Zusammenspiel den Aufbau der richtigen Verbindung gestattet. Beim ISDN-Zugang wird von der Telefonanlage das PPP (Point-to-Point-Protocol) benutzt, beim Zugang über T-DSL das PPPoE (Point-to-Point-Protocol over Ethernet). Der Datenverkehr auf diesen beiden Internet-Verbindungen wird von der Telefonanlage getrennt überwacht.
DSL-Modem	Spezielles Modem für die Datenübertragung mit Hilfe der DSL-Zugangstechnologie.
DSL-Splitter	Eine Breitbandanschlusseinheit (BBAE), umgangssprachlich Splitter, ist ein Gerät, das die Daten beziehungsweise Frequenzen verschiedener Anwendungen, die über eine Teilnehmeranschlussleitung oder einen Abschlusspunkt Linientechnik laufen, aufteilt und über getrennte Anschlüsse zur Verfügung stellt.
DSL/xDSL	Digital Subscriber Line
DSS1	Digital Subscriber Signalling System
DSSS	Direct Sequence Spread Spectrum ist eine Funktechnologie, die ursprünglich für den militärischen Bereich entwickelt wurde und eine hohe Störsicherheit bietet, weil das Nutzsignal auf einen breiten Bereich gespreizt wird. Das Signal wird mittels einer Spreizsequenz oder Chipping Code, bestehend aus 11 Chips auf 22 MHz Breite gespreizt. Selbst wenn ein oder mehr Chips in der Übertragung gestört sind, kann aus den restlichen Chips die Information zuverlässig zurückgewonnen werden.
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi Frequency (Tonfrequenzwahlsystem)
Durchsage	Sie möchten Ihre Mitarbeiter oder Ihre Familienmitglieder zu einer Besprechung oder zum Essen zusammenrufen? Sie könnten jeden einzelnen anrufen oder einfach die Durchsage-Funktion nutzen. Mit nur einem Anruf erreichen Sie alle durchsageberechtigten Telefone, ohne dass Ihre Gesprächspartner den Hörer der Telefone abheben müssen.
Durchsagefunktion	Leistungsmerkmal von Telefonanlagen. An geeigneten Telefonen (z.

	B. Systemtelefonen) lassen sich wie bei einer Sprechanlage Durchsagen tätigen.
Durchwahl	Leistungsmerkmal von größeren Telefonanlagen am Anlagenanschluss: Die Nebenstellen können gezielt von Extern angerufen werden.
Durchwahlbereich	Siehe Rufnummernband
Durchwahlnummer	Eine Durchwahlnummer (Extension) ist eine interne Rufnummer für ein Endgerät oder ein Subsystem. Bei Anlagenanschlüssen ist die Durchwahlnummer in der Regel eine Rufnummer aus dem vom Telefonanbieter zugeteilten Rufnummernband. Bei Mehrgeräteeanschlüssen kann es die MSN oder ein Teil der MSN sein.
Dynamische IP Adresse	Im Gegensatz zu einer statischen IP Adresse wird die dynamische IP Adresse temporär per DHCP zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
E-Mail	Electronic Mail
E1/T1	E1: Europäische Variante des ISDN-Primärmultiplexanschlusses mit 2,048 MBit/s, die auch als E1-System bezeichnet wird.
EAZ	Endgeräteauswahlziffer
ECB	Electronic Code Book mode
ECT	Explizit Call Transfer = Externes Vermitteln. Mit diesem Leistungsmerkmal können zwei externe Verbindungen vermittelt werden, ohne die beiden B-Kanäle des Amtsanschlusses zu blockieren.
Eigene Telefonnummer für das nächste Gespräch festlegen	Falls Sie z. B. am späten Abend aus Ihrem privaten Bereich - vielleicht dem Wohnzimmer - noch geschäftlich telefonieren wollen, können Sie Ihre geschäftliche Telefonnummer für dieses Gespräch als gehende Mehrfachrufnummer (MSN) definieren. Der Vorteil liegt zum einen darin, dass die Verbindung unter der ausgewählten MSN kostenmäßig erfasst wird und zum anderen kann Ihr Gesprächspartner Sie an der übermittelten MSN erkennen. Bevor Sie eine externe Wahl beginnen, können Sie festlegen, welche Ihrer Telefonnummern zur Vermittlungsstelle und zum externen Gesprächspartner mitgesendet werden soll. Die Auswahl erfolgt über den Telefonnummern-Index.
Eigene Telefonnummer	Temporäres Ausschalten der Übermittlung der eigenen Telefonnummer

mer unterdrücken	mer.
Einstellungen zurücksetzen (Reset)	Ein Reset der Geräte ermöglicht es Ihnen, Ihre Anlage wieder in einen definierten Ausgangszustand zu bringen. Dieses kann nötig sein, wenn unerwünschte Konfigurationen zurückgenommen oder das Gerät neu programmiert werden soll.
Einwahlparameter	Legen Sie die Einwahlparameter fest, d.h. Sie geben die Einwahlrufnummer des Providers ein und legen weitere Parameter wie z. B. den Benutzernamen und das Passwort fest.
Empfangsabruf	Funktion von Faxgeräten, um bei anderen Faxgeräten oder von Faxdatenbanken bereitgestellte Dokumente "abzuholen".
Encapsulation	Enkapsulierung von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete über ein Netzwerk zu übertragen, das den ursprünglichen Protokolltyp nicht direkt unterstützt (z. B. NetBIOS über TCP/IP).
Encryption	Bezeichnet die Verschlüsselung von Daten, z. B. MPPE.
Erfassen der externen Verbindungsdaten	In der Werkseinstellung werden alle, sowohl gehende als auch kommende über Ihre Telefonanlage geführten externen Verbindungen erfasst und in Form von Verbindungsdatensätzen gespeichert.
Erweiterte Wahlwiederholung	Eine gewählte Telefonnummer wird in einem Speicher des Telefons "geparkt". Sie kann später wieder gewählt werden, auch wenn zwischendurch mit anderen Telefonnummern telefoniert worden ist.
ESP	Encapsulating Security Payload
ESS	Der Extended Service Set bezeichnet mehrere BSS (mehrere Access Points) die ein einzelnes logisches Funknetz bilden.
Ethernet	Ein lokales Netzwerk, das alle Geräte im Netz (Rechner, Drucker, etc.) über ein Twisted-Pair- oder Koaxialkabel verbindet.
Ethernet-Anschlüsse	Die vier Anschlüsse sind gleichberechtigt über einen internen Switch herausgeführt. An die Anschlussbuchsen können Netzwerkclients direkt angeschlossen werden. Die Ports sind als 100/BaseT voll-duplex, autosensing, auto MDIX abwärtskompatibel zu 10/Base T realisiert. Hier können IP-Softclients mit SIP-Standard auf PCs mit Netzwerkkarte oder bis zu vier SIP-Telefone direkt angeschlossen werden.
Eumex Recovery	Sollte während des Ladens einer neuen Firmware die Stromversorgung der Telefonanlage unterbrochen werden, sind alle Funktionen

der Telefonanlage gelöscht.

- Euro-ISDN** Harmonisiertes, in Europa standardisiertes ISDN, beruhend auf dem Signalisierungsprotokoll DSS1, zu dessen Einführung sich Netzbetreiber in über 20 europäischen Staaten verpflichtet haben. In Deutschland ist das Euro-ISDN - nach dem nationalen Vorläufersystem 1 TR6 - inzwischen eingeführt.
- Eurofile-Transfer** Kommunikationsprotokoll für den Austausch von Dateien zwischen zwei PCs über ISDN mittels ISDN-Karte (File-Transfer) oder über dafür vorbereitete Telefone oder Telefonanlagen.
- Fallback: Priorität der Internet-Provider-Einträge** Die Priorität der Internet-Provider-Einträge wird nach der Reihenfolge festgelegt, in der sie in die Liste eingetragen werden. Der erste Eintrag einer DSL-Verbindung ist der Standardzugang. Sollte über den Standardzugang nach einer vorgegebenen Anzahl von Versuchen kein Verbindungsaufbau möglich sein, wird die Verbindung über den zweiten Eintrag und die folgenden Einträge versucht. Wenn auch der letzte Eintrag auf der Liste nicht zu einem erfolgreichen Verbindungsaufbau führt, wird der Vorgang bis zu einer erneuten Anfrage abgebrochen. Wenn der Fallback eintritt, und alle übrigen ISP's nur durch Wahlverbindungen zu erreichen sind, können beide B-Kanäle belegt sein. Im Falle einer Kanalbündelung sind Sie dann für die Dauer dieser Verbindung nicht zu erreichen.
- Fax** Kurzform für Telefax.
- Fernabfrage** Anrufbeantworterfunktion. Aus der Ferne Nachrichten abhören, meist in Verbindung mit Möglichkeiten wie Nachrichten löschen oder Ansagen ändern.
- Ferndiagnose/Fernwartung** Einige Endgeräte und Telefonanlagen werden komfortabel von T-Service Stützpunkten aus über die Telefonleitung betreut bzw. gewartet. Spart in vielen Fällen den Einsatz eines Servicetechnikers vor Ort.
- Feststation** Zentraleinheit von schnurlosen Telefongeräten. Es gibt zwei verschiedene Ausführungen: Die einfache Feststation dient zum Aufladen der Handgeräte. Bei den so genannten Komforttelefonen ist die Feststation gleichzeitig als Telefon nutzbar, die Handgeräte werden über separate Ladestationen aufgeladen.
- Feststellen böswilliger Anrufer (Fangen)** Dieses Leistungsmerkmal müssen Sie bei der T-Com beauftragen. Dort wird man Sie auch über die weitere Vorgehensweise informieren. Wenn Sie während eines Gespräches oder nach Beendigung des Gespräches durch den Anrufer (Sie hören den Besetzt-Ton aus

der Vermittlungsstelle) die Kennziffer 77 wählen, wird die Telefonnummer des Anrufers in der Vermittlungsstelle gespeichert. ISDN-Telefone können für dieses Leistungsmerkmal auch eigene Funktionen nutzen. Weitere Hinweise zur Ausführung dieser Funktion entnehmen Sie bitte der Bedienungsanleitung.

Festverbindung	Standleitung (leased line)
FHSS, Frequency Hopping Spread Spectrum	Frequenzspreizung wird in einem FHSS System durch ständig nach bestimmten Sprungmustern wechselnde Frequenzen erreicht. Im Gegensatz zu DSSS Systemen gibt es hier keine fest eingestellte Frequenz, sondern einstellbare Sprungmuster (hopping patterns). Die Frequenz wird innerhalb einer Sekunde sehr häufig gewechselt.
File-Transfer	Datenübertragung von einem Computer zu einem anderen, z. B. nach dem Eurofile-Transfer-Standard.
Filter	Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Anhand dieser Kriterien wird ein Paket aus dem Datenstrom ausgesondert. Mit einem so bestimmten Paket kann dann in spezifischer Weise verfahren werden. Zu diesem Zweck wird mit dem Filter eine bestimmte Aktion verbunden. Dadurch entsteht eine Filterregel.
Firewall	Bezeichnet die Summe der Schutzmechanismen für das lokale Netzwerk gegen Zugriffe von außen. Mit Ihrem Gateway stehen Schutzmechanismen wie NAT, CLID, PAP/CHAP, Access-Listen etc. zur Verfügung.
Firmware	Software Code, der alle Funktionen eines Gerätes beinhaltet. Dieser Code wird in einen PROM (Programmable Read Only Memory) geschrieben und bleibt dort auch nach Abschalten des Gerätes erhalten. Firmware kann durch den Benutzer erneuert werden, wenn eine neue Software Version verfügbar ist (Firmware Upgrade).
First-Level Domain	Englische Bezeichnung für den letzten Teil eines Namens im Internet. Bei www.t-com.de lautet die First-Level Domain de und bezeichnet in diesem Fall Deutschland.
Flash-Taste	Die Flash-Taste bei Telefonen entspricht der R-Taste. R ist die Abkürzung für Rückfrage. Die Taste unterbricht die Leitung für einen kurzen Moment, um bestimmte Funktionen wie z. B. Rückfrage über die Telefonanlage einzuleiten.
Follow-me	Leistungsmerkmal von Telefonanlagen zur Rufumleitung von Gesprächen am Zieltelefon.

Fragmentierung	Prozess, durch den ein IP-Datagramm in kleiner Teile getrennt wird, um die Bedingungen eines physikalischen Netzes zu erfüllen. Der umgekehrte Prozess wird Reassembly genannt.
Frame	Einheit der Information, die über eine Datenverbindung gesendet wird.
Frame Relay	Eine Packet Switching Methode, die kleinere Pakete und weniger Fehlerprüfung beinhaltet als das traditionelle Packet Switching wie X.25. Aufgrund seiner Eigenschaften wird Frame Relay für schnelle WAN-Verbindungen mit dichtem Traffic verwendet.
Freecall	Telefonnummer. Bisher Service 0130. Seit dem 1. Januar 1998 werden diese Telefonnummern auf freecall 0800 umgestellt.
Freisprechen	Ermöglicht freihändiges Telefonieren bei Telefonen mit eingebautem Mikrofon und Lautsprecher. Weitere Personen im Raum können so am Gespräch teilnehmen.
FTP	File Transfer Protocol
Full Duplex	Betriebsart, bei der beide Kommunikationspartner gleichzeitig bidirektional kommunizieren können.
Funktionstasten	Mit Telefonnummern oder Netzfunktionen belegbare Tasten an Telefonen.
G.991.1	Datenübertragungsempfehlung für HDSL
G.991.2	Datenübertragungsempfehlung für SHDSL
G.992.1	Datenübertragungsempfehlung für ADSL. Siehe auch G.992.1 Annex A und G.992.1 Annex B.
G.992.1 Annex A	Datenübertragungsempfehlung für ADSL: ITU-T G.992.1 Annex A
G.992.1 Annex B	Datenübertragungsempfehlung für ADSL: ITU-T G.992.1 Annex B
G.SHDSL	Siehe G.991.2.
Gateway	Aus-/Einfahrt, Übergangspunkt
Gehende Durchwahlsignalisierung	Die "gehende Durchwahlsignalisierung" ist für interne Anschlüsse am Anlagenanschluss vorgesehen, denen keine explizite Durchwahl zugeordnet wurde. Bei einem Anruf nach extern wird die unter gehende Durchwahlsignalisierung eingetragene Durchwahlnummer mit gesendet.

Gehende Telefonnummer	Sofern Sie die Übermittlung Ihrer Telefonnummer nicht unterdrückt haben und das Telefon Ihres Gesprächspartners die CLIP-Funktion unterstützt, kann Ihr Gesprächspartner die Telefonnummer des Anschlusses, von dem aus Sie telefonieren, im Display seines Telefons sehen. Diese bei einem Ruf nach extern übermittelte Telefonnummer wird als gehende Telefonnummer bezeichnet.
Gesprächskostenkonto	Sie können hier für einen Teilnehmer ein "Gesprächskostenkonto" einrichten. Jedem Teilnehmer kann damit auf seinem persönlichen "Gesprächskostenkonto" eine maximal zur Verfügung stehende Anzahl von Einheiten in Form eines Limits zugeteilt werden. Damit Einheiten abgebucht werden, ist "Kostenlimit" aktiv zu schalten. Sind die Einheiten verbraucht, sind keine Gespräche nach extern mehr möglich. Interne Gespräche können jederzeit weiter geführt werden. Die Abbuchung des Kontos erfolgt jeweils nach Beendigung eines Gespräches.
GRE	Generic Routing Encapsulation
Half Duplex	Bidirektionale Kommunikationmethode, bei der zu einem Zeitpunkt nur gesendet oder empfangen werden kann. Wird auch Simplex genannt.
Halten einer Verbindung	Ein Telefongespräch auf Wartestellung schalten, ohne die Verbindung zu verlieren (Rückfragen/Makeln).
Halten in der Telefonanlage	Bei den Leistungsmerkmalen "Während eines Gespräches einen weiteren Gesprächspartner anrufen" und "Mit zwei Gesprächspartnern abwechselnd sprechen" (Makeln) werden beide B-Kanäle des ISDN-Anschlusses benötigt. Über den zweiten B-Kanal Ihrer Telefonanlage sind Sie dann von extern nicht erreichbar und können selbst nicht extern telefonieren. In dieser Einstellung hört ein gehaltener externer Gesprächspartner die Wartemusik der Telefonanlage.
Handgerät	Mobile Komponente bei schnurlosen Telefonen. Bei digitaler Übertragung kann auch zwischen den Handgeräten telefoniert werden (DECT).
hashing	Der Vorgang des Ableitens einer Nummer, Hash genannt, von einer Zeichenfolge. Ein Hash ist im allgemeinen viel kürzer als der Textfluss, von dem er abgeleitet wurde. Der Hashing-Algorithmus ist so gestaltet, dass mit ziemlich geringer Wahrscheinlichkeit ein Hash generiert wird, der mit einem anderen Hash übereinstimmt, der aus einer Textfolge mit unterschiedlicher Bedeutung generiert wurde. Verschlüsselungsvorrichtungen benutzen Hashing, um sicherzustellen, dass Eindringlinge übermittelte Nachrichten nicht verändern

	können.
HDLC	High Level Data Link Control
HDSL	High Bit Rate DSL
HDSL2	High Bit Rate DSL, Version 2
Headset	Kombination aus Kopfhörer und Mikrofon als nützliche Hilfe für alle, die viel telefonieren müssen und dabei die Hände für Notizen frei haben wollen.
Heranholen von Rufen (Pick up)	Ein externer Anruf wird nur bei Ihrem Kollegen signalisiert. Da Sie sich in verschiedenen Teams befinden, ist das nicht verwunderlich. Sie können nun verschiedene Gruppen von Teilnehmern bilden, in denen das Heranholen von Rufen möglich ist. Ein Ruf kann nur von Teilnehmern/Endgeräten der gleichen Pick up Gruppe herangeholt werden. Das Zuordnen der Teilnehmer in Pick up Gruppen ist unabhängig von den jeweiligen Einstellungen in der Team-Anrufzuordnung Tag und Nacht.
HMAC	Hashed Message Authentication Code
HMAC-MD5	Hashed Message Authentication Code - benutzt den Message - Digest-Algorithmus Version 5.
HMAC-SHA1	Hashed Message Authentication Code - benutzt den Secure-Hash-Algorithmus Version 1.
Hook-Flash	Die Nutzung der Komfortleistungen Rückfragen, Makeln, Dreierkonferenz im T-Net und bestimmter Leistungsmerkmale einiger Telefonanlagen sind nur mit der Hook-Flash-Funktion (langer Flash) der Signaltaste am Telefon möglich. Bei modernen Telefonen ist diese Taste mit "R" bezeichnet.
Hörerlautstärke	Regelung der Lautstärke im Telefonhörer.
Host	Computer, der Dienste in einem Rechnernetz zur Verfügung stellt.
Host-Name	Bezeichnet in IP-Netzen einen Namen, der anstelle einer zugehörigen Adresse benutzt wird. Ein Host-Name besteht aus einer ASCII-Zeichenfolge, die den Host eindeutig kennzeichnet.
Host-Route	Route zu einem einzelnen Host.
HSDPA	High Speed Downlink Packet Access (Datenübertragungsverfahren des Mobilfunkstandards UMTS).

HTTP	HyperText Transfer Protocol
Hub	Netzwerkkomponente, mit der mehrere Netzwerkkomponenten zu einem lokalen Netz zusammengeschlossen werden (sternförmig).
IAE	ISDN-Anschlusseinheit, ISDN-Anschlussdosen.
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEEE	Das Institute of Electrical and Electronics Engineers (IEEE). Ein großer weltweiter Zusammenschluss von Ingenieuren. Arbeitet ständig an Standards und Normen, um das Zusammenspiel verschiedenster Geräte zu gewährleisten.
IETF	Internet Engineering Task Force
IGMP	Internet-Group-Management-Protokoll, dient zur Organisation von Multicast-Gruppen.
IKE	Internet-Key-Exchange-Protokoll dient der automatischen Schlüsselverwaltung für IPSec.
Index	Der Index von 0...9 ist fest vorgegeben. Jede eingetragene externe Mehrfachrufnummer wird einem Index zugeordnet. Diesen Index benötigen Sie beim Einrichten von Leistungsmerkmalen über die Kennziffern eines Telefons, z. B. Einrichten einer "Anrufweitzerschaltung in der Vermittlungsstelle" oder "Telefonnummer für das nächste externe Gespräch festlegen".
Infrastruktur Modus	Ein Netzwerk im Infrastruktur Modus ist ein Netzwerk, das mindestens einen Access Point als zentrale Kommunikations- und Steuerstelle beinhaltet. In einem Netz im Infrastruktur Modus kommunizieren alle Clients ausschließlich über Access Points miteinander. Es läuft keine Kommunikation zwischen den einzelnen Clients direkt ab. Ein solches Netzwerk wird auch BSS (Basic Service Set) genannt, ein Netzwerk, das aus mehreren BSS besteht wird ESS (Extended Service Set) genannt. Die meisten Funknetze arbeiten im Infrastruktur Modus, um Verbindung mit dem verkabelten Netz herzustellen.
Interne Telefonnummern	Ihre Telefonanlage verfügt über einen festen internen Telefonnummernplan.
Internet	Das Internet besteht aus einer Reihe von regionalen, lokalen und Universitätsnetzen. Für Datenübertragung im Internet wird das Pro-

	tokoll IP verwendet.
Internet Time Sharing	Ermöglicht mehreren Nutzern gleichzeitig über eine ISDN-Verbindung im Internet zu surfen. Die Informationen werden zeitversetzt von den einzelnen Computern abgefragt.
Interngespräche	Kostenfreie Verbindung zwischen Endgeräten einer Telefonanlage.
Internkennziffer übertragen	Erhalten Sie bei Abwesenheit an Ihrem Anschluss einen internen Anruf z. B. vom Teilnehmer mit der internen Telefonnummer 22, wird seine interne Telefonnummer in der Anruferliste Ihres Telefons gespeichert. Da Ihr Anschluss aber werkseitig auf automatische Amtsholung eingestellt ist, müssten Sie für einen Rückruf zunächst ** wählen, um den internen Wählton zu erhalten, und dann die 22. Ist "Internkennziffer übertragen" aktiv, wird ** vor die 22 gesetzt und der Rückruf kann automatisch aus der Anruferliste heraus erfolgen.
Internrufton	Besondere Signalisierung an Telefonanlagen zur Unterscheidung von Intern- und Externanrufen.
Intranet	Lokales, unternehmensinternes Computernetz auf der Basis von Internettechnologien, das die gleichen Internetdienste bereitstellt, wie z. B. E-Mail-Versand und Homepages.
IP	Internet Protocol
IP-Adresse	In einem IP-Netzwerk der erste Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 192.168.1.254. Siehe auch Netzmaske.
IPComP	IP payload compression
IPCONFIG	Ein Hilfsmittel, das unter Windows Computern verwendet wird, um die eigenen IP-Einstellungen zu überprüfen oder zu ändern.
IPoA	IP over ATM
ISDN	Integrated Services Digital Network
ISDN-Adresse	Die Adresse eines ISDN-Gerätes, welche aus einer ISDN-Nummer besteht gefolgt von weiteren Ziffern, die sich auf ein spezifisches Endgerät beziehen, z. B. 47117.
ISDN-Basisanschluss	Teilnehmeranschluss beim ISDN. Der Basisanschluss besteht aus zwei B-Kanälen und einem D-Kanal. Außer dem Basisanschluss gibt es noch den Primärmultiplexanschluss. Die Schnittstelle zum Teilnehmer wird über den sogenannten So-Bus geschaffen.

ISDN-BRI	ISDN Basic Rate Interface
ISDN-Dynamic	Dieses Leistungsmerkmal setzt die Installation des T-ISDN Speedmanagers voraus! Wenn Sie gerade im Internet surfen, und zum Download zwei B-Kanäle nutzen, sind Sie telefonisch von Extern nicht mehr erreichbar. Da die Signalisierung eines weiteren Anrufes über den D-Kanal erfolgt, hat Ihre Telefonanlage, je nach Einstellung, die Möglichkeit, einen B-Kanal gezielt abzuschalten und Sie können das Gespräch annehmen.
ISDN-Intern/-Extern	Alternative Bezeichnung für den S0-Bus.
ISDN-Karte	Adapter für den Anschluss eines PCs an den ISDN-Basisanschluss. Technisch unterscheidet man aktive und passive Karten. Aktive ISDN-Karten verfügen über einen eigenen Prozessor, der Kommunikationsvorgänge unabhängig vom PC-Prozessor abwickelt und somit keine Ressourcen benötigt. Eine passive ISDN-Karte hingegen nutzt Ressourcen des PCs.
ISDN-Login	Funktion Ihres Gateways. Über ISDN-Login ist Ihr Gateway fernkonfigurier- und wartbar. ISDN-Login funktioniert bereits bei Gateways im Auslieferungszustand, sobald sie mit einem ISDN-Anschluss verbunden und so über eine Rufnummer erreichbar sind.
ISDN-Nummer	Die Netzwerkadresse der ISDN-Schnittstelle, z. B. 4711.
ISDN-PRI	ISDN Primary Rate Interface
ISDN-Router	Ein Router, der nicht über Netzwerkanschlüsse verfügt, aber gleiche Funktionen zwischen PC, ISDN und dem Internet bereitstellt.
ISO	International Standardization Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union
IWV	Abkürzung für Impulswahlverfahren. Herkömmliches Wahlverfahren im Telefonnetz. Wählziffern werden durch eine definierte Anzahl von Gleichstromimpulsen dargestellt. Das Impulswahlverfahren wird durch das Mehrfrequenzwahlverfahren (MFV) abgelöst.
Kalender	Mit der Zuweisung eines Kalenders erfolgt die Umschaltung zwischen den Anrufzuordnungen Tag und Nacht. Für jeden Wochentag kann eine beliebige Tag-/Nachtumschaltzeit gewählt werden. Ein Kalender verfügt über jeweils vier Schaltzeiten, die jedem einzelnen Wochentag gezielt zugewiesen werden können.

Kanalbündelung	Channel Bundling
Key Escrow	Hinterlegte Schlüssel können von der Regierung eingesehen werden. Besonders die U.S.-Regierung schreibt Schlüsselhinterlegung vor, um zu verhindern, dass Verbrechen durch Datenverschlüsselung getarnt werden.
Kombigerät	Ist ein analoger Endgeräteanschluss der Telefonanlage als „Multifunktionsport“ für Kombigeräte eingerichtet, werden alle Anrufe unabhängig vom Dienst angenommen. Bei einer Amtsholung über Kennziffern können unabhängig von der Konfigurierung des analogen Anschlusses die Dienstkennungen „analoge Telefonie“ oder „Telefax Gruppe 3“ mit gesendet werden. Bei Wahl der 0 wird die Dienstkennung „analoge Telefonie“ mit gesendet.
Komfortanschluss	T-ISDN Basisanschluss mit umfangreichem Leistungsangebot: An-klopfen, Anrufweitschaltung, Dreierkonferenz, Gesprächskosten-anzeige am Ende der Verbindung, Rückfragen/Makeln, Telefonnum-mernübermittlung. Im Komfortanschluss sind als Standard drei Mehrfachrufnummern enthalten.
Komfortleistungen	Leistungsmerkmale der Netze T-Net und T-ISDN wie Anzeige der Telefonnummer des Anrufers, Rückruf bei Besetzt, Anrufweiter-schaltung, veränderbare Anschluss-Sperre, veränderbare Telefon-nummernsperre, Verbindung ohne Wahl und Übermittlung von Tarif-informationen. Die Verfügbarkeit ist abhängig vom Standard der an-geschlossenen Endgeräte.
Konferenzschaltung	Leistungsmerkmal von Telefonanlagen: Mehrere interne Gesprächs-teilnehmer können gleichzeitig telefonieren. Es sind auch mit exter-nen Gesprächspartnern Dreierkonferenzen möglich.
Konfiguration der Telefonanlage mit dem PC	Eine wichtige Voraussetzung für die erfolgreiche Übertragung Ihrer Konfiguration zur Telefonanlage ist, dass Sie eine Verbindung zwis-chen PC und Telefonanlage eingerichtet haben. Sie haben diese Möglichkeit über die Ethernet-Verbindung LAN.
Konfiguration der Telefonanlage mit dem Telefon	Sie können Ihre Telefonanlage - allerdings eingeschränkt - auch mit einem Telefon programmieren. Hinweise zur Programmierung Ihrer Telefonanlage mit dem Telefon entnehmen Sie bitte der beiliegen-den Bedienungsanleitung.
Kurzwahl	Jeder der bis zu 300 Telefonnummern des Telefonbuches kann ein Kurzwahl-Index (000...299) zugeordnet werden. Diesen Kurzwahl-In-dex wählen Sie dann anstelle der langen Telefonnummer. Beachten Sie, dass über die Kurzwahl gewählte Telefonnummern ebenfalls

	der Wahlregel unterliegen.
L2TP	Ermöglicht das Tunneln von PPP-Verbindungen.
LAN	Local Area Network (Lokales Netzwerk)
LAPB	Link Access Procedure Balanced
Lauthören	Funktion bei Telefonen mit eingebauten Lautsprechern: Per Tastendruck können im Raum anwesende Personen ein Telefongespräch mithören.
Layer 1	Schicht 1 des ISO-OSI-Modells, die Bitübertragungsschicht.
LCD	Liquid-Crystal Display (Flüssigkristallbildschirm), ist ein Bildschirm, bei dem spezielle Flüssigkristalle zur Bilddarstellung genutzt werden.
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
Lease Time	Unter "Lease Time" versteht man die Zeit, in der ein Rechner seine ihm zugewiesene IP-Adresse behält, ohne mit dem DHCP-Server "Rücksprache" halten zu müssen.
Leased Line	Standleitung, eine permanente (stehende) Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetzwerk.
Letzter Zugriff	Der letzte Zugriff durch den T-Service wird gespeichert und in der Konfigurierung angezeigt.
LLC	Link Layer Control
MAC-Adresse	Jedes Gerät im Netz ist über eine feste Hardware-Adresse (MAC-Adresse) definiert. Die Netzwerkkarte eines Geräts bestimmt diese weltweit eindeutige Adresse.
Makeln	Makeln erlaubt es, zwischen zwei externen bzw. internen Gesprächspartnern hin- und her zu schalten, ohne dass der wartende Teilnehmer mithören kann.
Man-in-the-Middle Attack	Die Verschlüsselung mittels öffentlicher Schlüssel setzt den Austausch der öffentlichen Schlüssel voraus. Während des Austausches kann der ungeschützte Schlüssel leicht abgefangen werden und eröffnet so die Möglichkeit eines "man-in-the-middle"-Angriffs. Der Angreifer kann seinen eigenen Schlüssel setzen, so dass ein

	Schlüssel, der dem "man-in-the-middle" bekannt ist, anstelle des gewünschten Schlüssels des beabsichtigten Kommunikationspartners verwendet wird.
MD5	Siehe HMAC-MD5
Mehrfachrufnummer (MSN)	Multiple Subscriber Number
Mehrgeräteanschluss	Point-to-Multipoint (Punkt-zu-Mehrpunkt)
Mehrgeräteanschluss	Basisanschluss im T-ISDN mit standardmäßig drei Telefonnummern und zwei Leitungen. Der Anschluss der ISDN-Endgeräte erfolgt direkt am Netzabschluss (NTBA) oder am ISDN-Internanschluss einer Telefonanlage.
Mehrgeräteanschluss für die Telefonanlage	Ihre von der T-Com mit der Auftragsbestätigung erhaltenen Mehrfachrufnummern tragen Sie in der Konfiguration in die dort vorgesehenen Tabellenfelder ein. In der Regel erhalten Sie drei Mehrfachrufnummern, können jedoch bis zu zehn Telefonnummern je Anschluss beantragen. Mit der Eintragung der Telefonnummern erfolgt neben der Zuordnung zu einem "Index" gleichzeitig die Zuordnung zu einem Team. Beachten Sie bitte, dass alle Telefonnummern zunächst dem Team 00 zugeordnet werden. In das Team 00 wiederum sind werkseitig die internen Telefonnummern 10, 11 und 20 eingetragen. Anrufe von extern werden somit an den in Team 00 eingetragenen Anschlüssen mit den internen Telefonnummern 10, 11 und 20 signalisiert.
MFV	Mehrfrequenzwahlverfahren
MIB	Management Information Base
Mikrofonstumm-schaltung	Taste zum Abschalten des Mikrofons. Der Gesprächspartner am Telefon kann dann die im Raum geführten Rückfragen nicht mithören.
Mitschneiden von Telefongesprächen	Leistungsmerkmal eines Anrufbeantworters. Erlaubt die Aufnahme eines Gespräches auch während des Telefonats.
Mixed Mode	Der Access Point akzeptiert WPA sowie WPA2.
MLPPP	Multilink-PPP
Modem	Modulator/Demodulator
MPDU	MAC Protocol Data Unit - jedes Informationspaket, das auf dem

	Funkmedium ausgetauscht wird inclusive Management-Frames und fragmentierten MSDUs.
MPPC	Microsoft Point-to-Point Compression
MPPE	Microsoft Point-to-Point Encryption
MSDU	MAC Service Data Unit - ein Datenpaket, ohne Berücksichtigung von Fragmentierung im WLAN.
MSN	Multiple Subscriber Number
MSSID	Siehe SSID
MTU	Maximum Transmission Unit
Multicast	Eine spezifische Form des Broadcasts, bei dem gleichzeitig eine Nachricht an eine definierte Benutzergruppe übertragen wird.
Multiprotokollgateway	Gateway, das mehrere Protokolle routen kann, z. B. IP, X.25 etc.
Music On Hold (MOH, Wartemusik)	Ihre Telefonanlage verfügt über zwei interne Wartemusik-Melodien. Bei Auslieferung ist die interne Melodie 1 aktiv. Sie können zwischen den Melodien 1 und 2 wählen oder die Wartemusik inaktiv schalten.
MWI	Übermittlung einer vorliegenden Sprachnachricht aus einer Nachrichtenbox, z. B. T-NetBox oder MailBox an ein entsprechendes Endgerät. Der Nachrichteneingang am Endgerät wird z. B. durch eine Leuchtdiode signalisiert.
NAT	Network Address Translation
NDIS WAN	NDIS WAN ist eine Microsoft-Erweiterung dieses Standards in Bezug auf Wide Area Networking (WAN). Der NDIS WAN CAPI-Treiber erlaubt die Nutzung des ISDN-Controllers als WAN-Karte. Der NDIS WAN Treiber ermöglicht die Nutzung eines DFÜ-Netzwerkes unter Windows. NDIS ist die Abkürzung für Network Device Interface Specification und stellt einen Standard für die Anbindung von Netzwerkkarten (Hardware) an Netzprotokolle (Software) dar.
Nebenstelle	Bezeichnet bei Telefonanlagen das mit der Anlage verbundene Endgerät (z. B. Telefon). Jede Nebenstelle kann auf die Anlagenleistungen zugreifen und mit anderen Nebenstellen kommunizieren.
NetBIOS	Network Basic Input Output System

Netsurfen	"Entdeckungsreise" auf der Suche nach interessanten Angeboten in weit verzweigten Datennetzen wie T-Online. Vor allem bekannt aus der Welt des Internets.
Netz-Direkt (Keypad-Funktionen)	Mit Hilfe der Funktion "Netz-Direkt" (Keypad) können Sie durch die Eingabe einer Tastenfolge auch von Ihrem ISDN- oder analogen Telefon aus aktuelle T-ISDN Funktionen nutzen. Fragen Sie hierzu beim Kundenberater der T-Com nach und lassen Sie sich die entsprechenden Kennziffern geben (z. B. Anrufweiserschaltung in der Vermittlungsstelle).
Netzabschluss (NTBA)	Mit Netzabschluss bezeichnet man in der Telekommunikation den Punkt, an dem einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt wird.
Netzadresse	Eine Netzadresse bezeichnet die Adresse eines gesamten lokalen Netzwerks.
Netzmaske	In einem IP-Netzwerk der zweite Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 255.255.255.0. Siehe auch IP-Adresse.
NMS	Network Management Station
Notizbuchfunktion	Während eines Telefonats kann eine Telefonnummer in den Zwischenspeicher des Telefons eingegeben werden, um sie später anzuwählen.
Notrufnummern	Der Fall der Fälle tritt ein und Sie müssen dringend Polizei, Feuerwehr oder eine andere Telefonnummer erreichen. Zu allem Überfluss sind alle Anschlüsse belegt. Sie haben jedoch Ihrer Telefonanlage die Telefonnummern mitgeteilt, die im Notfall erreichbar sein müssen. Wählen Sie nun eine dieser Notrufnummern, wird dies von der Telefonanlage erkannt und automatisch ein B-Kanal des T-ISDN für Ihren Notruf freigeschaltet. Notrufe unterliegen keinen Einschränkungen durch Konfigurationen. Ist für einen Anschluss "Telefonieren mit Vorwahlziffer eingestellt", wird der interne Anschluss belegt. Wählen Sie, um nach extern telefonieren zu können, vorab die 0 und dann die gewünschte Notrufnummer.
NT	Network Termination
NTBA	Network Termination for Basic Access
NTP	Network Time Protocol
Nutzkanal	Entspricht einer Telefonleitung im T-Net. Beim T-ISDN sind im Ba-

	sisanschluss zwei Nutzkanäle mit je 64 KBit/s Datenübertragungsrate enthalten.
OAM	Operations and Maintenance
Offline	Vom englischen "off-line" (ohne Verbindung). Verbindungsloser Betriebszustand, z. B. des PCs.
Online	Vom englischen "on-line" (in Verbindung). Zum Beispiel der Zustand der Verbindung eines PCs mit Datennetzen oder beim Datenaustausch von PC zu PC.
Online Pass	Teil der Zertifizierungsdienste der T-Com für das Internet. Digitaler Ausweis für das Internet. Mit dem OnlinePass kann sich ein Internetsnutzer als Kunde bei einem Unternehmen ausweisen.
Online-Banking	Begriff für die elektronische Kontoführung, z. B. über T-Online.
Online-Dienste	Leistungen, die über Kommunikationsdienste wie T-Online und Internet rund um die Uhr verfügbar sind.
Ortsvermittlungsstelle (OVst)	Vermittlungsknoten eines öffentlichen Telefon-Ortsnetzes, der den Anschluss von Endsystemen unterstützt.
OSI-Modell	OSI = Open System Interconnection (offene Kommunikationssysteme)
OSPF	Open Shortest Path First
PABX	Private Automatic Branch Exchange (Nebenstellenanlage)
Paketvermittlung	Packet Switching
PAP	Password Authentication Protocol
Parken	Das Gespräch wird in der Vermittlungsstelle vorübergehend gehalten. Prinzipieller Unterschied zum Halten: Das Gespräch wird unterbrochen, der Hörer kann z. B. aufgelegt werden. Anwendbar für Makeln. Möglich im T-Net, im T-ISDN und bei Telefonanlagen. Das Endgerät muss mit MFV und R-Taste ausgestattet sein.
PBX	Private Branch Exchange
PCMCIA	Die PCMCIA (Personal Computer Memory Card International Association) ist eine 1989 gegründete Industrievereinigung, die Kreditkartengroße I/O Karten vertritt, wie z. B. WLAN Karten.
Peer	Endpunkt einer Kommunikation in einem Computernetzwerk.

PGP	Pretty Good Privacy
PH	Packet Handler
PIN	Persönliche Identifikationsnummer
Ping	Packet Internet Groper
PKCS	Public-Key Cryptography Standards
Port	Ein-/Ausgang
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPP-Authentisierung	Sicherheitsmechanismus; Authentisierung durch ein Passwort im PPP.
PPPoA	Point to Point Protocol over ATM
PPPoE	Point to Point Protocol over Ethernet
PRI	Primary Rate Interface
Primärmultiplexanschluss	Teilnehmeranschluss beim ISDN. Der Primärmultiplexanschluss besteht aus einem D-Kanal und 30 B-Kanälen (Europa). (In Amerika: 23 B-Kanäle und ein D-Kanal.) Außer dem Primärmultiplexanschluss gibt es noch den ISDN-Basisanschluss.
Protokoll	Protokolle werden verwendet, um Art und Weise eines Informationsaustausches zwischen zwei Systemen zu definieren. Protokolle steuern und regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen (Decodierung, Adressierung, Wegwahl im Netz, Kontrollmechanismen, etc.).
Proxy ARP	ARP = Address Resolution Protocol
Prüfsummenfeld	Frame Check Sequence (FCS)
PSN	Packet Switched Network
PSTN	Public Switched Telephone Network
Punkt-zu-Mehrpunkt	Point-to-Multipoint
Punkt-zu-Punkt	Point-to-Point

PVID	Port VLAN ID
QoS	Quality of Service ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen.
R-Taste	Telefone, die mit der R-Taste (Rückfragetaste) ausgestattet sind, eignen sich auch für den Anschluss an Telefonanlagen. Bei modernen Telefonen löst die R-Taste die Hook-Flash-Funktion aus. Sie ist für die Nutzung der Leistungsmerkmale im T-Net wie Rückfragen/Makeln und Dreierkonferenz erforderlich.
RADIUS	Remote Authentication Dial-In User Service
RADSL	Rate-adaptive Digital Subscriber Line
RAS	Remote Access Service
Raumüberwachung (akustisch)	Um das Leistungsmerkmal "Raumüberwachung" nutzen zu können, muss in dem zu überwachenden Raum das Telefon über eine Kennziffer zur Raumüberwachung freigegeben und der Hörer abgehoben oder Freisprechen eingeschaltet sein. Legen Sie den Hörer des Telefons im zu überwachenden Raum auf oder schalten Sie das Freisprechen aus, ist die Raumüberwachung beendet und das Leistungsmerkmal wieder ausgeschaltet.
Raumüberwachung von externen Telefonen	Mit dieser Funktion kann eine Raumüberwachung von einem externen Telefon aus erfolgen.
Raumüberwachung von internen Telefonen	Sie können von einem internen Telefon Ihrer Telefonanlage einen Raum akustisch überwachen. Die Einrichtung erfolgt mit den in der Bedienungsanleitung beschriebenen Telefonprozeduren. Lesen Sie bitte zu den hier beschriebenen Funktionen auch die entsprechenden Hinweise in der Bedienungsanleitung.
Real Time Clock (RTC)	Hardware-Uhr mit Pufferbatterie
Real Time Jitter Control	Hier können Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert werden, damit die Sprachpakete nicht blockiert werden.
Remote	Entfernt, nicht lokal.
Remote Access	Nicht lokaler Zugriff, siehe Remote.
Remote-CAPI	bintec-eigene Schnittstelle für CAPI.

Repeater	Ein Gerät, das elektrische Signale von einer Kabelverbindung zur anderen überträgt, ohne Routing-Entscheidungen zu treffen oder Paketfilterung vorzunehmen. Vergleiche Bridge und Router.
RFC	Spezifikationen, Vorschläge, Ideen und Richtlinien, das Internet betreffend, werden in Form von so genannten RFCs (Request For Comments) veröffentlicht.
Rijndael (AES)	Rijndael (AES) wurde als AES ausgewählt aufgrund der schnellen Schlüsselgenerierung, der niedrigen Speicheranforderungen und der hohen Sicherheit gegenüber Angriffen. Weitere Informationen zu AES, siehe http://csrc.nist.gov/encryption/aes .
RIP	Routing Information Protocol
RipeMD 160	RipeMD 160 ist eine kryptographische Hash-Funktion mit 160 Bit. Sie gilt als sichererer Ersatz für MD5 und RipeMD.
RJ45	Stecker bzw. Buchse für maximal acht Adern. Anschluss für digitale Endgeräte.
Roaming	In einem mehrzelligen WLAN können sich Clients frei bewegen und sich bei der Bewegung durch Funkzellen von einem Access Point abmelden und neu auf einem anderen Access Point anmelden, ohne dass der Benutzer dies bemerkt. Diese Fähigkeit wird Roaming genannt.
Round-Robin	Rundlauf-Verfahren
Router	Geräte, die unterschiedliche Netze auf der Schicht 3 des OSI-Modells verbinden und Informationen von einem Netz in das andere weiterleiten (routen).
Routing	Bezeichnet das Festlegen von Wegen bei der Nachrichtenübermittlung.
RSA	Der RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) basiert auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Daher benötigt man eine sehr hohe Datenverarbeitungskapazität und viel Zeit, um einen RSA Schlüssel abzuleiten.
RTSP	Real-Time Streaming Protocol
Rückfrage	Bietet die Möglichkeit, nach dem Anklopfen das erste Gespräch zu halten und ein neues Gespräch entgegenzunehmen.
Rückruf bei Besetzt	Leistungsmerkmal im T-ISDN, in Telefonanlagen und im T-Net. Eine

	<p>Verbindung wird automatisch hergestellt, sobald der Besetztstatus am Zielanschluss aufgehoben ist. Nach Freiwerden des Anschlusses erfolgt die Signalisierung beim Anrufer. Sobald dieser dann seinen Hörer abhebt, wird die Verbindung automatisch hergestellt. Zuvor muss jedoch der Rückruf vom Anrufer an seinem Endgerät aktiviert werden.</p>
Rückruf bei Nichtmelden	<p>Sie rufen bei einem gewünschten Gesprächspartner an und der Angerufene meldet sich nicht. Mit "Rückruf bei Nichtmelden" ist das für Sie in Zukunft kein Problem. Denn durch diese Komfortleistung stellen Sie die Verbindung jetzt ohne erneute Wahl her. Immer, wenn Sie nicht selbst telefonieren, erfolgt ein erneuter Verbindungsaufbau zum gewünschten Gesprächspartner - maximal 180 Minuten lang.</p>
Rufnummernband	<p>(Durchwahlbereich)</p>
Rufumleitung	<p>Auch: Anrufweiterleitung oder Anrufweiserschaltung. Ein ankommender Anruf wird an einen vorgegebenen Telefon-, Internet- oder Mobilfunkanschluss weitergeleitet.</p>
Rufverteilung	<p>Rufverteilung bei Telefonanlagen bedeutet, dass Anrufe bestimmten Endgeräten zugeordnet werden.</p>
Rufzustellung bei Besetzt	<p>Ablehnen</p>
Ruhe vor dem Telefon	<p>Anrufschutz</p>
S0-Anschluss	<p>Siehe ISDN-Basisanschluss.</p>
S0-Bus	<p>Sämtliche ISDN-Anschlussdosen und der NTBA beim ISDN-Mehrgeräteanschluss. Jeder So-Bus besteht aus einem vieradrigen Kabel. Die Leitungen/ Kabel übertragen die digitalen ISDN-Signale. Hinter der letzten ISDN-Anschlussdose wird der So-Bus mit einem Abschlusswiderstand terminiert. Der So beginnt beim NTBA und kann bis zu 150 m lang sein. Es lassen sich beliebige ISDN-Geräte daran betreiben. Gleichzeitig können allerdings immer nur zwei Geräte den So verwenden, da nur zwei B-Kanäle zur Verfügung stehen.</p>
S0-Schnittstelle	<p>International standardisierte Schnittstelle für ISDN-Einrichtungen. Diese Schnittstelle wird netzseitig vom NTBA bereitgestellt. Nutzerseitig ist die Schnittstelle sowohl für den Anschluss einer Telefonanlage (Anlagenanschluss) als auch für den Anschluss von bis zu acht ISDN-Endgeräten (Mehrgeräteanschluss) vorgesehen.</p>

S2M-Anschluss	Siehe Primärmultiplexanschluss.
SAD	Die SAD (=Security Association Database) enthält Informationen über die Sicherheitsvereinbarungen, wie z. B. AH oder ESP Algorithmen und Schlüssel, Sequenznummern, Protokollmodi und SA-Lebensdauer. Für ausgehende IPSec-Verbindungen weist ein SPD-Eintrag auf einen Eintrag im SAD hin, d.h. die SPD legt fest, welche SA angewendet werden muss. Für eingehende IPSec-Verbindungen wird in der SAD abgerufen, wie das Paket weiterverarbeitet werden soll.
Scheduling	Zeitablaufsteuerung
SDSL	Symmetric Digital Subscriber Line
Server	Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden. Oft versteht man unter Server einen bestimmten Rechner im LAN, z. B. DHCP-Server.
ServerPass	Teil der Zertifizierungsdienste der T-Com für das Internet. Digitaler Ausweis eines Unternehmens. Mit dem ServerPass bestätigt die T-Com, dass ein Server im Internet zu einem bestimmten Unternehmen gehört und dies durch die Vorlage des Handelsregistrauszugs belegt wurde.
Service 0190	Sprachmehrwertdienst der T-Com zur gewerblichen Verbreitung privater Informationsdienstleistungen. Die Leistungen der T-Com beschränken sich auf die Bereitstellung der technischen Infrastruktur und auf die Abwicklung des Inkassos für die Informationsanbieter. Der Zugang zu den bereitgestellten Informationen erfolgt über die bundesweit einheitliche Telefonnummer 0190 und über eine 6-stellige Telefonnummer. Informationsangebote: Unterhaltung, Wetter, Finanzen, Sport, Gesundheit, Support- und Service-Hotlines.
Service 0700	Sprachmehrwertdienst der T-Com. Ermöglicht die Entgegennahme von Anrufen unter einer bundeseinheitlichen, standortunabhängigen Telefonnummer, die mit den Ziffern 0700 beginnt. Kostenfreie Weiterleitung im nationalen Festnetz. Erweiterung mit Vanity möglich.
Service 0900	Sprachmehrwertdienst der T-Com. Löst den Service 0190 ab.
Servicenummer 0180	Sprachmehrwertdienst 0180call der T-Com zur Entgegennahme von Anrufen unter einer bundeseinheitlichen, standortunabhängigen Telefonnummer, beginnend mit den Ziffern 0180.

Setup Tool	Menügesteuertes Tool zur Konfiguration Ihres Gateways. Das Setup Tool kann verwendet werden, sobald ein Zugang zum Gateway (seriell, ISDN-Login, LAN) besteht.
SFP	Small Form-factor Pluggable (kleine Module für Netzwerkverbindungen).
SHA1	Siehe HMAC-SHA.
SHDSL	Single-Pair High-Speed
Shell	Eingabeschnittstelle zwischen Computer und Benutzer.
Shorthold	Bezeichnet die definierte Zeit, nach der eine Verbindung abgebaut wird, wenn keine Daten mehr übertragen werden. Der Shorthold lässt sich statisch (feste Zeit) und dynamisch (in Abhängigkeit von Gebühreninformationen) einrichten.
Sicherungsschicht	Data Link Layer (DLL)
SIF	Stateful Inspection Firewall
Signalisierung	Signalisierung gleichzeitig: Alle zugeordneten Endgeräte werden gleichzeitig gerufen. Ist ein Telefon besetzt, kann angeklopft werden.
SIP	Session Initiation Protocol
SMS	Short Message Service
SMS Server Telefonnummern	An Ihre Telefonanlage können Sie SMS-fähige Telefone anschließen und damit das Leistungsmerkmal SMS im Festnetz der T-Com nutzen. SMS werden über den SMS Server der T-Com an den jeweiligen Empfänger weitergeleitet. Um eine SMS mit einem SMS-fähigen Endgerät versenden zu können, muss die Telefonnummer 0193010 des SMS Servers der Empfängernummer vorangestellt werden. Diese Telefonnummer ist bereits in Ihrer Telefonanlage gespeichert, so dass sich eine manuelle Eingabe der Server Telefonnummer erübrigt bzw. vom Telefon nicht mitgesendet werden muss. Damit Sie SMS an Ihrem SMS-fähigen Festnetztelefon empfangen können, müssen Sie sich einmalig beim SMS Service der Deutschen Telekom registrieren lassen. Das Senden von SMS ist kostenpflichtig. Das Empfangen von SMS ist kostenfrei.
SMS-Empfang	Haben Sie ein SMS-fähiges Endgerät angeschlossen, können Sie entscheiden, ob für den betreffenden Anschluss der SMS-Empfang erlaubt sein soll. Werkseitig ist kein SMS-Empfang eingerichtet. Da-

mit Sie mit Ihrem SMS-fähigen Endgerät SMS empfangen können, müssen Sie sich einmalig beim SMS Service der T-Com registrieren. Die einmalige Registrierung ist kostenfrei. Sie schicken einfach eine SMS mit dem Inhalt ANMELD an die Zielrufnummer 8888. Anschließend erhalten Sie vom SMS-Dienst der T-Com eine kostenlose Bestätigung der Registrierung. Mit einer SMS mit dem Inhalt ABMELD an die Zielrufnummer 8888 können Sie Ihr Gerät bzw. Ihre Telefonnummer auch wieder abmelden. Eingehende SMS werden dann vorgelesen. Welche Telefone SMS-fähig sind, erfahren Sie im nächsten T-Punkt, bei unserer Kundenhotline 0800 330 1000 oder im Internet unter <http://www.t-com.de>.

SNMP	Simple Network Management Protocol
SNMP-Shell	Eingabeebene für SNMP-Kommandos.
SOHO	Small Offices and Home Offices
SPD	Die SPD (=Security Policy Database) definiert die Sicherheitsdienste, die für den IP-Traffic zur Verfügung stehen. Diese Sicherheitsdienste sind abhängig von Parametern wie Quelle und Ziel des Pakets, etc.
Sperrliste (Wahlbereiche)	Sie können für einzelne Teilnehmer eine Einschränkung der externen Wahl festlegen. Die in der Sperrwerk-Tabelle eingetragenen Telefonnummern können von den Endgeräten, die der Wahlkontrolle unterliegen, nicht gewählt werden. z. B. würde der Eintrag 0190 alle Verbindungen zu kostenintensiven Diensteanbietern verhindern.
SPID	Service Profile Identifier
Splitter	Der Splitter trennt am DSL-Anschluss Daten- und Sprachsignale.
Spoofing	Technik zur Reduktion des Datenverkehrs (und damit zur Kostensparnis) insbesondere in WANs.
SSH	Verschlüsselter Zugang zur Shell
SSID	Als Service Set Identifier (SSID) oder auch Network Name bezeichnet man die Kennung eines Funknetzwerkes, das auf IEEE 802.11 basiert.
SSL	Secure Sockets Layer Eine von Netscape entwickelte, heute standardisierte Technologie, die im allgemeinen dazu verwendet wird, HTTP-Traffic zwischen einem Web Browser und einem Web Server zu sichern.

STAC	Datenkomprimierungsverfahren.
Standardanschluss	T-ISDN Basisanschluss mit den Leistungsmerkmalen Dreierkonferenz, Rückfragen/Makeln und Telefonnummernübermittlung. Im Standardanschluss sind drei Mehrfachrufnummern enthalten.
Statische IP-Adresse	Im Gegensatz zu einer dynamischen IP-Adresse eine fest eingestellte IP Adresse.
Subadressierung	Neben der Übertragung der ISDN-Telefonnummer können zusätzliche Informationen im Form einer Subadresse bereits beim Verbindungsaufbau über den D-Kanal vom Anrufer zum Angerufenen übertragen werden. Eine über die reine MSN hinausgehenden Adressierung, mit der z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt für einen Dienst angesprochen werden können. In dem angerufenen Endgerät - z.B einem PC - können auch verschiedene Applikationen angesprochen und ggf. ausgeführt werden. Das Leistungsmerkmal ist kostenpflichtig und muss beim Netzbetreiber gesondert beauftragt werden.
Subnetz	Ein Netzwerkschema, das einzelne logische Netzwerke in kleinere physikalische Einheiten teilt.
Subnetz Maske	Eine Methode um mehrere IP Netze in eine Reihe von Untergruppen oder Subnetze zu teilen. Die Maske ist ein Binärmuster, welches mit den IP-Adressen im Netz zusammenpassen muss. Standardmäßig ist die Subnet Mask 255.255.255.0. In diesem Fall können in einem Subnetz 254 verschiedene IP Adressen auftreten, von x.x.x.1 bis x.x.x.254.
Switch	LAN-Switches sind Netzwerkkomponenten, die der Funktion von Bridges oder sogar von Gateways ähnlich sind. Sie vermitteln Datenpakete zwischen Ein- und Ausgangs-Port. Im Gegensatz zu Bridges haben Switches allerdings mehrere Ein- und Ausgangs-Ports. Dadurch erhöht sich die Bandbreite im Netz. Switches können auch eingesetzt werden, um zwischen verschiedenen schnellen Netzen (z. B. 100MBit- und 10MBit-Netzen) zu übersetzen.
Swyx Ware	Softwarelösung für die IP-Telefonie
synchron	Übertragungsverfahren, bei dem Sender und Empfänger in genau gleichen Zeittakten arbeiten – im Gegensatz zu asynchron. Leerzeichen werden durch eine Pausenkodierung überbrückt.
Syslog	Syslog dient als De-facto-Standard zur Übermittlung von Log-Meldungen in einem IP-Netzwerk. Syslog-Meldungen werden als

unverschlüsselte Textnachricht über den UDP Port 514 gesendet und zentral gesammelt. Sie werden meist zum Überwachen von Computersystemen benutzt.

Systemtelefone	Ein zu modernen Telefonanlagen gehörendes Telefon, das – je nach Telefonanlage – mit einer Reihe von Komfortfunktionen und Sondertasten ausgestattet ist, z. B. das T-Concept PX722.
T-DSL	Produktname der Deutschen Telekom AG für ihre DSL-Dienstleistungen und -Produkte.
T-Fax	Produktbezeichnung für die Telefaxgeräte der T-Com.
T-ISDN	Telefonieren, Faxen, Datenübertragung, Online-Dienste - alles über ein Netz und über einen einzigen Anschluss: T-ISDN erschließt Ihnen faszinierende Leistungen mit vielen Vorteilen. Zum Beispiel mit einem Mehrgeräteanschluss - genau die passende Lösung für Familien oder kleine Firmen. Diese Anschlussvariante, bei der die bereits vorhandenen Telefonkabel genutzt werden können, kostet weniger als zwei Telefonanschlüsse, bringt Ihnen aber viel mehr an Qualität und Komfort: Zwei voneinander unabhängige Leitungen, damit Sie auch dann noch telefonieren, ein Fax empfangen oder im Internet surfen können, wenn gerade ein anderes Familienmitglied etwas länger plaudert. Drei oder mehr Telefonnummern, die Sie individuell Ihren Geräten zuordnen und bei Bedarf durch einfache Programmierung wieder anders verteilen können. Wobei man wissen muss, dass die meisten ISDN-Telefone mehrere Telefonnummern "verwalten" können. So lässt sich z. B. ein "zentrales" Telefon im Haushalt einrichten, damit Sie dort auf die Anrufe unter allen ISDN-Telefonnummern reagieren können. Zusätzlich bekommen Fax und Telefon im Arbeitszimmer je eine Telefonnummer - das Telefon für Tochter oder Sohn nicht zu vergessen. So ist jedes Familienmitglied ganz gezielt erreichbar. Ein feiner Komfort, der bestimmt so manchen "Reibungseffekt" beseitigt! Und was die Kosten betrifft, können Sie auf Wunsch in Ihrer Rechnung getrennt ausweisen lassen, welche Tarifeinheiten sich auf welcher ISDN-Telefonnummer summiert haben.
T-Net	Das digitale Telefonnetz der T-Com zum Anschluss analoger Endgeräte.
T-NetBox	Der Anrufbeantworter im T-Net und im T-ISDN. Die T-NetBox speichert bis zu 30 Nachrichten.
T-NetBox Telefonnummer	Tragen Sie hier die aktuelle T-NetBox-Telefonnummer ein, falls diese von der werkseitig eingetragenen 08003302424 abweicht. So

	bald eine Sprach- oder Faxnachricht in Ihrer T-NetBox eingegangen ist, wird eine Benachrichtigung an Ihre Telefonanlage gesendet.
T-Online	Oberbegriff für die Online-Plattform der T-Com. Mit Leistungen wie E-Mail und Zugang zum Internet.
T-Online Software	Softwaredecoder der T-Com für alle gängigen Computersysteme, der den Zugang zu T-Online ermöglicht. Unterstützt alle Funktionen wie KIT, E-Mail und Internet mit einem Browser. Diese Software erhalten alle T-Online Nutzer kostenlos.
T-Service	Der T-Service führt sämtliche Installationsarbeiten und Konfigurationen der Telefonanlagen im Auftrag des Kunden aus. Durch Instandhaltungs- und Instandsetzungsarbeiten sorgt er jederzeit für eine optimale Gesprächs- und Datenübertragung.
T-Service Zugang	Der T-Service Zugang bietet Ihnen die Möglichkeit, Ihre Telefonanlage vom T-Service konfigurieren zu lassen. Rufen Sie den T-Service an! Lassen Sie sich beraten und geben Sie Ihre Konfigurationswünsche an. Der T-Service konfiguriert dann Ihre Telefonanlage aus der Ferne ohne Ihr weiteres Zutun.
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System
TAE	Telekommunikationsanschlusseinheit
Tag/Nacht/Kalender	Sie legen fest, wie die Umschaltung der Anrufvariante Tag/Nacht erfolgen soll.
TAPI	Telephony Applications Programming Interface
TAPI-Konfiguration	Mit der TAPI-Konfiguration können Sie den TAPI-Treiber dem Programm anpassen, das diesen Treiber nutzt. Sie können überprüfen, welche MSN einem Endgerät zugeordnet ist, können einen neuen Leitungsnamen festlegen und die Wählparameter einstellen. Konfigurieren Sie zuerst Ihre Telefonanlage. Anschließend müssen Sie die TAPI-Schnittstelle konfigurieren. Benutzen Sie das Programm "TAPI-Konfiguration".
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment

TEI	Terminal Endpoint Identifier
Teilnehmer Name	Um Anschlüsse einfacher zu unterscheiden, können Sie für jeden internen Teilnehmer einen Teilnehmer-Namen vergeben.
Telefax	Bezeichnung für Fernkopieren zur originalgetreuen Übertragung von Texten, Grafiken und Dokumenten über das Telefonnetz.
Telefonanlage	Der Leistungsumfang einer Telefonanlage ist herstellerspezifisch und ermöglicht unter anderem den Betrieb von Nebenstellen, kostenlose Interngespräche, Rückruf bei Besetzt und Konferenzschaltungen. Telefonanlagen übernehmen z. B. die Bürokommunikation (Sprach-, Text- und Datenübertragung).
Telefonbuch	Die Telefonanlage verfügt über ein internes Telefonbuch. Sie können bis zu 300 Telefonnummern mit den dazugehörigen Namen speichern. Auf das Telefonbuch der Telefonanlage können Sie mit einem Teldat-Gerät (z. B. CS 410) zugreifen. Über die Konfigurationsoberfläche fügen Sie dem Telefonbuch Einträge hinzu.
Telematik	Telematik bezeichnet eine Kombination aus Telekommunikation und Computertechnik und beschreibt die Datenkommunikation zwischen Systemen und Geräten.
Telnet	Protokoll aus der TCP/IP-Protokollfamilie. Telnet ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk.
Terminaladapter	Gerät zur Schnittstellenanpassung. Hierdurch wird der Anschluss von unterschiedlichem Equipment an das T-ISDN ermöglicht. So dient der Terminaladapter a/b zum Anschluss analoger Endgeräte an die S0-Schnittstelle des ISDN-Basisanschlusses. Bereits vorhandene analoge Endgeräte mit Tonwahl können weiter betrieben werden.
TFE	Türfreisprecheinrichtung. Sie lässt sich an verschiedene Telefonanlagen anschalten. Über ein Telefon kann ein Türgespräch geführt und die Tür geöffnet werden.
TFE am analogen Anschluss	Ein analoger Anschluss kann für die Anschaltung eines Funktionsmoduls M06, zur Anschaltung einer Türfreisprecheinrichtung DoorLine eingerichtet werden.
TFE-Adapter	Das Funktionsmodul kann an einem analogen Anschluss Ihrer Telefonanlage installiert werden. Ist an Ihre Telefonanlage eine TFE (DoorLine) über ein Funktionsmodul angeschaltet, können Sie von jedem berechtigten Telefon aus mit einem Besucher an der Tür

sprechen. Jedem Klingeltaster können Sie bestimmte Telefone zuordnen, die dann beim Betätigen des Klingeltasters klingeln. Die Signalisierung erfolgt bei analogen Telefonen im Takt des Türstellenrufes. Anstelle der internen Telefone kann auch ein externes Telefon für den Klingeltaster als Rufziel konfiguriert werden. Ihre Türsprechstelle kann bis zu 4 Klingeltaster besitzen. Der Türöffner kann während eines Türgesprächs betätigt werden. Eine Betätigung ohne Türgespräch ist nicht möglich.

TFTP	Trivial File Transfer Protocol
Tiger 192	Tiger 192 ist ein relativ neuer und sehr schneller Hash-Algorithmus.
TK-Anlage	Telekommunikationsanlage
TLS	Transport Layer Security
Tonwahl	Mehrfrequenzwahlverfahren (MFV)
Trap	Unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist.
Trap-Paket	Nachricht im Fehlerfall.
Trigger	Auslöseimpuls
Trunk	Bündelung
TTL	TTL bedeutet Time to Live und beschreibt die Zeit, in der ein Datenpaket zwischen den einzelnen Servern hin und her geschickt wird, bevor es verworfen wird.
Twofish	Twofish war ein möglicher Kandidat für AES (Advanced Encryption Standard). Er wird als ebenso sicher wie Rijndael (AES) angesehen, ist jedoch langsamer.
U-ADSL	Universal Asymmetric Digital Subscriber Line
Übertragungsrate	Die Anzahl der Bits pro Sekunde, die im T-Net oder im T-ISDN vom PC oder Faxgerät aus übertragen werden. Faxgeräte erreichen bis zu 14,4 KBit/s, Modems bis zu 56 KBit/s. Im ISDN ist Daten- und Fauxaustausch mit 64 KBit/s möglich. Bei T-DSL können bis zu 8 MBit/s empfangen und bis zu 768 KBit/s gesendet werden.
UDP	User Datagram Protocol
Umschaltbares	Möglichkeit, durch Schalter oder Tasteneingabe an Endgeräten wie

Wahlverfahren	Telefon oder Faxgerät zwischen Impulswahlverfahren und Mehrfrequenzwahlverfahren zu wechseln.
Umstecken am Bus (Parken)	Ermöglicht beim Mehrgeräteanschluss während des Telefongesprächs das Umstecken der Endgeräteverbindung in eine andere ISDN-Anschlussdose.
UMTS	Universal Mobile Telecommunications System (Mobilfunkstandard der dritten Generation, 3G)
Unterdrückung der Telefonnummer	Leistungsmerkmal in Telefonanlagen. Die Anzeige der Telefonnummer lässt sich fallweise ausschalten.
Update	Aktualisierung eines Softwareprogramms (Firmware der Telefonanlage). Ein Update ist die aktualisierte Version eines vorhandenen Softwareproduktes; man erkennt es an der geänderten Versionsnummer.
Upload	Datentransfer bei Online-Verbindungen, wobei Dateien von dem eigenen PC auf einen anderen PC oder zu einem Datennetzserver übertragen werden.
UPnP	Universal Plug and Play
Upstream	Datenübertragungsrate vom Kunden zum ISP.
URL	Universal/Uniform Resource Locator
USB	Universal Serial Bus
UUS1 (User to User Signalling 1)	Diese Funktion ist nur für Systemtelefone und ISDN-Telefone möglich.
V.11	ITU-T-Empfehlung für symmetrische Doppelstrom-Schnittstellenleitungen (bis zu 10 MBit/s).
V.24	CCITT- und ITU-T-Empfehlung, welche die Schnittstelle zwischen einem Computer oder Terminal als Datenendeinrichtung (DTE) und einem Modem als Datenübertragungseinrichtung (DCE) definiert.
V.28	TU-T-Empfehlung für unsymmetrische Doppelstrom-Schnittstellenleitung.
V.35	ITU-T-Empfehlung für Datenübertragung mit 48 kBit/s im Bereich von 60 bis 108 kHz.
V.36	Modem für V.35.

V.42bis	Datenkomprimierungsverfahren.
V.90	ITU-Standard für 56 kBit-Analogmodems. Im Gegensatz zu den älteren V.34-Modems werden mit dem V.90-Standard Daten digital zum Kunden weitergesendet und müssen auf einer Modemseite (Provider) nicht zuerst von digital in analog umgewandelt werden, wie es bei V.34-Modems und älteren Modellen der Fall ist. Dadurch sind höhere Übertragungsraten möglich. Eine maximale Geschwindigkeit von 56 kBit/s kann nur unter optimalen Umständen erreicht werden.
Vanity	Buchstabenwahl
Variante Tag - Nacht	Sie möchten wichtige Anrufe für Ihr Home-Office nach Feierabend automatisch auf einen Anrufbeantworter umleiten, damit Sie nicht gestört werden? Dieses können Sie mit der Anrufzuordnung realisieren. Sie können jedem Teilnehmer zwei verschiedene Rufverteilungen (Anrufzuordnung Tag und Anrufzuordnung Nacht) zuweisen. In den Anrufzuordnungen ist auch eine Anrufweitschaltung zu einem externen Teilnehmer einrichtbar, so dass Sie jederzeit erreichbar sein können. In der Anrufzuordnung Tag und Nacht wird also festgelegt, welche internen Endgeräte bei einem Anruf von extern klingeln sollen. Die Anrufzuordnung Tag und Nacht ist eine Tabelle, in der die ankommenden Rufe internen Teilnehmern zugeordnet werden.
VDSL	Very High Bit Rate Digital Subscriber Line (auch als VADSL oder BDSL bezeichnet)
Vermittlungsstelle	Knotenpunkt im öffentlichen Telekommunikationsnetz. Man unterscheidet zwischen Ortsvermittlungsstellen und Fernvermittlungsstellen.
VID	VLAN ID
VJHC	Van-Jacobsen-Header-Komprimierung
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
VSS	Virtual Service Set
Wahlkontrolle	Sie können in der Konfiguration für bestimmte Endgeräte eine Einschränkung der externen Wahl festlegen.

Wählverbindung	Eine Verbindung wird bei Bedarf durch Wählen einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung.
Wahlvorbereitung	Bei einigen Telefonen mit Display kann man eine Telefonnummer zuerst eingeben, noch einmal kontrollieren und danach wählen.
WAN	Wide Area Network
WAN-Interface	WAN-Schnittstelle.
WAN-Partner	Gegenstelle, die über das WAN, z. B. ISDN, erreicht wird.
Wartemusik (Music On Hold, MOH)	Leistungsmerkmal bei Telefonanlagen. Während der Rückfrage oder des Weiterverbindens wird eine Melodie eingespielt, die der Wartende hört. Ihre Telefonanlage verfügt über zwei interne Melodien zur Auswahl.
Web-Filter	Filter, der das Aufrufen unerwünschter Webseiten unterbindet.
Webmail	Dienst von T-Online, mit dem über einen Browser im Internet weltweit E-Mails versendet und empfangen werden können.
Webserver	Server, der Dokumente im HTML-Format zum Abruf über das Internet bereithält (WWW).
Wechselsprechen (nur ISDN-Teilnehmer)	Dieser Anschluss ist für ein ISDN-Telefon (nur Systemtelefone T-Concept PX722) mit Wechselsprechfunktion nutzbar. Rufen Sie ein ISDN-Telefon mit Wechselsprechfunktion an, schaltet dieses automatisch die Funktion Lauthören ein, damit sofort ein Gespräch erfolgen kann. Bitte beachten Sie die Hinweise in der Bedienungsanleitung des Telefons zur Funktion Wechselsprechen.
WEP	Wired Equivalent Privacy
Westernstecker	(auch RJ-45-Stecker) Für ISDN-Endgeräte verwendeter Stecker mit acht Kontakten. Von der US-Telefongesellschaft Western Bell entwickelt. Westerntelefonstecker für analoge Telefone haben vier oder sechs Kontakte.
WINIPCFG	Ein grafisches Tool unter Windows 95, 98 und Millennium, das die Win32 API verwendet, um die IP- Adresskonfiguration von Rechnern anzusehen und zu konfigurieren.
WLAN	Eine Gruppe von Computern, die drahtlos miteinander vernetzt sind (FunkLAN).
WMM	Wireless Multimedia

WPA	Wi-Fi-Protected Access
WPA - Enterprise	Wendet sich v. a. an die Bedürfnisse von Unternehmen und bietet sichere Verschlüsselung und Authentisierung. Verwendet 802.1x und das Extensible Authentication Protocol (EAP) und bietet damit eine effektive Möglichkeit der Anwender-Authentisierung.
WPA - PSK	Wendet sich an Privat-Anwender oder kleine Unternehmen, die keinen zentralen Authentisierungsserver betreiben. PSK steht für Pre-Shared Key und bedeutet, dass AP und Client eine feste, allen Teilnehmern bekannte, beliebige Zeichenfolge (8 bis 63 Zeichen) als Basis für die Schlüsselberechnung im Funkverkehr verwenden.
WWW	World Wide Web
X.21	Die Empfehlungen aus X.21 definieren die physikalische Schnittstelle zwischen zwei Netzwerkkomponenten in einem Paketvermittlungsnetz (z. B. Datex-P).
X.21bis	Die Empfehlungen aus X.21bis definieren die DTE/DCE-Schnittstelle zu synchronen Modems der V-Serie.
X.25	Protokoll, das die Schnittstelle von Netzwerkkomponenten zu einem Paketvermittlungsnetz definiert.
X.31	ITU-T-Empfehlung zur Integration von X.25-fähigen DTEs in ISDN (D-Kanal).
X.500	ITU-T Standards, die Benutzerverzeichnisdienste abdecken, vergleiche: LDAP. Beispiel: Das Telefonbuch ist das Verzeichnis, in dem man Personen anhand des Namens findet (anhand der Übereinstimmung mit dem Telefonverzeichnis). Das Internet unterstützt mehrere Datenbanken mit Informationen über Anwender, wie z. B. Email-Adressen, Telefonnummern und Postanschrift. Diese Datenbanken können durchsucht werden, um Informationen über einzelne Personen zu erhalten.
X.509	ITU-T Standards, die das Format der Zertifikate und Zertifikatanfragen und deren Verwendung definieren.
XAuth	Extended Authentication (Authentifizierungsmethode)
Zentraler Kurzwahl-speicher	Leistungsmerkmal von Telefonanlagen. Telefonnummern werden in der Telefonanlage gespeichert und können dann mit einer Tastenkombination von jedem angeschlossenen Telefon aus aufgerufen werden.

Zielwahlspeicher	Kurzwahlspeicher
Zugangscodes	PIN oder Passwort
Zugriffsschutz	Über Filter kann verhindert werden, dass Außenstehende auf die Daten der Rechner Ihres LAN zugreifen können. Diese Filter stellen eine Basisfunktion einer Firewall dar.
Zuordnung	Ein externer Anruf kann bei internen Teilnehmern signalisiert werden. Die Einträge in der "Variante Tag" und der "Variante Nacht" können unterschiedlich sein.

Index

171

ISDN-Zeitserver 69
Systemadministrator-Passwort 66

#

#1 #2, #3 102

6

6in4 Relay IPv4-Adresse 294
6to4 Relay Anycast IPv4-Adresse 294

A

Abfrage Intervall 250
ACCESS_ACCEPT 84
ACCESS_REJECT 84
ACCESS_REQUEST 84
ACCOUNTING_START 84
ACCOUNTING_STOP 84
ACL-Modus 166
Admin-Status 200 , 242 , 495
Administrativer Status 306 , 395
Adressbereich 381
Adresse/Präfix 381
Adresse/Subnetz 381
Adressmodus 128
Adresstyp 381
Ähnliches Zertifikat überschreiben
422
Aktion 171 , 224 , 370 , 373 , 422 ,
466 , 485 , 491
aktiv 263
Aktive IPSec-Tunnel 61
Aktive Sitzungen (SIF, RTP, etc...)
61
Aktives Funkmodulprofil 153
Aktiviert 365
Aktualisierung aktivieren 404
Aktualisierung der Routing-Tabelle auf-

grund von Summary Link Advertisements 498

Aktualisierungsintervall 406
Aktualisierungspfad 406
Aktualisierungstimer 236
Aktuelle Ortszeit 68
Aktuelle Geschwindigkeit / Aktueller Modus 109
Aktueller Dateiname im Flash 466
Aktuelles Netzwerk 119
Alle Multicast-Gruppen 255
Allgemeiner Name 100
Als DHCP-Server 394
Als IPCP-Server 394
Alternative Schnittstelle, um DNS-Server zu erhalten 392
Andere Inaktivität 378
Ankommende Rufnummer 319
Anmeldefenster 449
Anmeldung 493
Ansicht 495 , 499 , 501 , 504
Antwort 397
Antwortintervall (Letztes Mitglied) 250
Anzahl Nachrichten 475
Anzahl der Spatial Streams 156
Anzahl der Wählversuche 441
Anzahl erlaubter Verbindungen 314
Anzahl Verwendeter Ports 286
APN (Access Point Name) 119
Arbeitsspeichernutzung 61
ARP Lifetime 228
ARP Processing 163
Art des Datenverkehrs 189
Assert-Status 504 , 505
Auf Client-Anfrage antworten 442
Auf Discard/Refuse-Schnittstelle gebundene Routen propagieren 245
Ausgehende ISDN-Nummer 361
Ausgehende Rufnummer 319
Ausgehende Schnittstelle 214
Ausgehende Nummer 440
Aushandlungsmodus 486
Auswahl 382
Auszuführende Aktion 434

- Authentifizierung 271 , 276 , 282 ,
290 , 350 , 358
- Authentifizierung für PPP-Einwahl 93
- Authentifizierungsmethode 306 , 322 ,
486
- Authentifizierungstyp 85 , 90 , 242
- Authentisierung aktivieren 456
- Automatische Subnetzerstellung 132 ,
185
- Automatische Konfiguration beim
Start 112
- Autonomous Flag 133 , 186
- Autospeichermodus 102 , 422

- B**
- Back-up der Konfiguration auf SD
Karte 60
- Backup Designated Router (BDR)
495
- Bandbreite 156
- Bandbreite angeben 375
- Basierend auf Ethernet-Schnittstelle
127
- Beacon Period 159
- Bedingung des Schnittstellenverkehrs
416
- Bedingung für Ereignisliste 422
- Befehlsmodus 422
- Befehlstyp 422
- Benachrichtigungsdienst 475 , 475 ,
478
- Benachrichtigungseinstellungen 478
- Benachrichtigungsempfänger 475
- Benutzer 336
- Benutzerdefiniert 100
- Benutzerdefinierter Kanalplan 159
- Benutzername 267 , 274 , 280 , 288 ,
294 , 347 , 355 , 404 , 413 , 478 ,
493
- Benutzter Präfix/Länge 183
- Bereich 497
- Bereichs-ID 240 , 242
- Berichtsmethode 226
- Berücksichtigen 195
- Beschreibung 95 , 105 , 152 , 156 ,
180 , 189 , 200 , 204 , 207 , 214 ,
220 , 224 , 267 , 274 , 280 , 288 ,
294 , 298 , 306 , 313 , 322 , 330 ,
336 , 343 , 347 , 355 , 365 , 379 ,
380 , 381 , 382 , 383 , 386 , 395 ,
411 , 416 , 422 , 485 , 486 , 491 ,
492
- Beschreibung - Verbindungsinformation
- Status 61
- Beschreibung des
IP-Zuordnungspools 357
- Betreff 475
- Betreibermodus 85
- Betriebsmodus 153 , 156
- Bevorzugte Gültigkeitsdauer 133
- Bevorzugter Netzwerktyp 119
- Blockieren nach Verbindungsfehler
für 271 , 276 , 282 , 290 , 350 ,
358
- blockiert 263
- Blockzeit 91 , 327
- BOSS 466
- BOSS-Version 60
- BRRP aktivieren 459
- Burst-Größe 214
- Burst-Mode 158
- Bytes 486

- C**
- CA-Name 422
- CA-Zertifikat 98
- CA-Zertifikate 327
- Cache-Größe 392
- Cache-Treffer 401
- Cache-Trefferrate (%) 401
- Callback 361
- Callback-Modus 282
- CAPWAP-Verschlüsselung 152
- Code 383
- COS-Filter (802.1p/Layer 2) 204 , 220
- CPU-Nutzung 61
- CRL verwenden 422
- CRLs senden 341

- CSV-Dateiformat 422
- D**
- Datei auswählen 466
 Dateikodierung 103 , 104
 Dateiname 422 , 466
 Dateiname auf Server 422
 Dateiname in Flash 422
 Datum 484
 Datum einstellen 69
 Dauer 489 , 490
 Demand Circuit Options 242
 Designated Router (DR) 495 , 500
 Designated-Router-Priorität 257
 Details 485
 DH-Gruppe 322
 DHCP Broadcast Flag 134
 DHCP Client an Schnittstelle 228
 DHCP-Hostname 134
 DHCP-MAC-Adresse 134
 DHCP-Modus 135
 DHCP-Optionen 409
 DHCP-Server 148
 Dienst 116 , 190 , 200 , 220 , 370 ,
 373 , 489 , 490
 Dienstmerkmal 116
 DNS-Anfragen 401
 DNS-Aushandlung 271 , 276 , 286 ,
 290 , 351 , 360
 DNS-Hostname 397
 DNS-Server 398
 DNS-Test 462
 Domäne 398
 Domäne am Hotspot-Server 447
 Domänenname 392
 Downstream-Schnittstelle 185
 Drahtloser Modus 158
 Dritter Zeitserver 69
 Dropping-Algorithmus 217
 DSA-Schlüsselstatus 81
 DSCP-/TOS-Wert 176
 DSCP/TOS-Filter (Layer 3) 204 , 220
 DTIM Period 159
 Dynamic LS Update Compression
 245
 Dynamische
 RADIUS-Authentifizierung 340
- E**
- E-Mail 100
 E-Mail-Adresse des Senders 478
 EAP-Vorabauthentifizierung 164
 Eigene IP-Adresse per ISDN/GSM über-
 tragen 319
 Eingehende ISDN-Nummer 361
 Eingehende Nummer 440
 Eingehender Dienstyp 119
 Einstellungen zurücksetzen 18
 Eintrag aktiv 85 , 90
 Einträge 285
 Empfangene DNS-Pakete 401
 Empfangene Database Description Pa-
 kets 498
 Empfangene Hello Nachrichten 498
 Empfangene Link State Acknowledge
 Pakets 498
 Empfangene Link State Request
 Pakets 498
 Empfangene Link State Update
 Pakets 498
 Empfänger 475
 Entfernte GRE-IP-Adresse 365
 Entfernte IP-Adresse 344
 Entfernte IPv6-Adresse 294
 Entfernte PPTP-IP-Adresse 276 , 355
 Entfernte PPTP-IP-AdresseHostname
 355
 Entfernte IP-Adresse 485 , 486
 Entfernte Netzwerke 485
 Entfernte Nummer 489 , 490
 Entfernte ID 486
 Entfernter Hostname 343
 Entfernter Port 492
 Entfernter Port 486
 Entfernter Benutzer (nur Einwahl) 280
 Entferntes IPv6-Netzwerk 294
 Enthaltene Zeichenfolge 475
 Ereignis 475

Ereignisliste 416 , 422
 Ereignistyp 416
 Erfolgreich beantwortete Anfragen
 401
 Erfolgreiche Versuche 434
 Ergebnis der automatischen Konfiguration
 112
 Erlaubte Adressen 166
 Erreichbarkeitsprüfung 87 , 327 , 333
 , 486
 Erster Zeitserver 69
 Erweiterte Route 175
 Ethernet-Schnittstelle 454
 Ethernet-Schnittstellenauswahl 109
 Expiry Timer 500 , 504 , 505 , 506
 Externe Routen importieren 240
 Externer Dateiname 103 , 104

F

Facility 471
 Fallback-Nummer 119
 Fehler 171 , 486 , 488
 Fehlgeschlagene Versuche 434
 Fertig 171
 Filter 207
 Filterregeln 375
 Firewall Status 377
 Fragmentation Threshold 159
 Frames ohne Tag verwerfen 139
 Frequenzband 156
 Für DNS-/WINS-Serverzuordnung zu
 verwendende IP-Adresse 392

G

Garbage Collection Timer 236
 Gateway 175 , 409
 Gateway-Adresse 180 , 183
 Generation ID 500
 Gerät 152
 Gesamt 488
 Geschäftsbedingungen 447
 Gesendete Database Description Pa-
 kets 498

Gesendete Hello Nachrichten 498
 Gesendete Link State Acknowledge Pa-
 kets 498
 Gesendete Link State Request
 Pakets 498
 Gesendete Link State Update Pakets
 498
 Gewichtung 214
 GRE-Window-Anpassung 362
 GRE-Window-Größe 362
 Größe der Zero Cookies 340
 Größe des Protokoll-Headers unterhalb
 Layer 3 211
 Gruppen-ID 434
 Gruppenbeschreibung 85 , 195 , 197 ,
 228
 Gültigkeitsdauer 133

H

Hashing-Algorithmen 80
 Hello Hold Time 257
 Hello-Intervall 257 , 345
 High-Priority-Klasse 207
 Hinzuzufügende/zu bearbeitende MIB/
 SNMP-Variable 422
 Hold Down Timer 237
 Host 398
 Host für mehrere Standorte 450
 Hostname 404
 HTTP 77
 HTTPS 77
 HTTPS-TCP-Port 402

I

ID des virtuellen Routers 455 , 458 ,
 459
 IGMP Proxy 252
 IGMP-Status 253
 IKE (Phase-1) 488
 IKE (Internet Key Exchange) 306
 IKE (Phase-1) SAs 486
 Image bereits vorhanden. 171
 Immer aktiv 267 , 274 , 280 , 288 ,

- 347 , 355
 - Importiere Summary-Routen 240
 - inaktiv 263
 - Indexvariablen 416 , 422
 - Indirekte, statische Routen
 - exportieren 242
 - Initial Contact Message senden 340
 - Intervall 416 , 422 , 434 , 438
 - Intra-cell Repeating 163
 - IP Address Owner 451
 - IP-Accounting 473
 - IP-Adressbereich 148 , 357 , 408
 - IP-Adresse 241 , 397 , 411 , 454 ,
471 , 482 , 493 , 500 , 500
 - IP-Adresse / Netzmaske 128
 - IP-Adresse des Rendezvous Point
501
 - IP-Adresse des Rendezvous Points
500
 - IP-Adresse des Assert Winner 504 ,
505
 - IP-Adresse des virtuellen Routers 455
 - IP-Adresse zur Nachverfolgung 198
 - IP-Adresse/Netzmaske 234 , 492
 - IP-Adressenvergabe 309
 - IP-Adressmodus 269 , 275 , 281 , 289
, 348 , 357
 - IP-Komprimierung 333
 - IP-Poolbereich 292 , 338 , 363
 - IP-Poolname 292 , 338 , 363 , 408
 - IP-Version 382
 - IP-Zuordnungspool 281 , 309
 - IP-Zuordnungspool (IPCP) 348 , 357
 - IPSec (Phase-2) 488
 - IPSec aktivieren 338
 - IPSec (Phase-2) SAs 486
 - IPSec über TCP 340
 - IPSec-Debug-Level 338
 - IPSec-Tunnel 487
 - IPv4 381
 - IPv4-Adresse des Tunnelendpunkts
294
 - IPv6 128 , 270 , 381
 - IPv6-Adresse 128
 - IPv6-Modus 128
 - IPv6-Präfix/Länge 128 , 270
 - ISDN Verwendung Extern 61
 - ISDN-Diebstahlsicherungsdienst 440
 - ISDN-Konfigurationstyp 112
 - ISDN-Login 77
 - ISDN-Port 116
 - ISDN-Switch-Typ 112
- J**
- Join/Prune Hold Time 257
 - Join/Prune-Intervall 257
 - Join/Prune-Status 504 , 505 , 506
- K**
- Kanal 153 , 489
 - Kanalbündelung 285
 - Kanalplan 159
 - Keepalive-Periode 261
 - Kennwort für geschütztes Zertifikat
422
 - Key Hash Payloads senden 341
 - Klassen-ID 207 , 214
 - Klassenplan 207
 - Komprimierung 79 , 299 , 350 , 358
 - Konfiguration verschlüsseln 422
 - Konfiguration enthält Zertifikate/Schlüssel 422
 - Konfigurationsmodus 183 , 309
 - Konfigurationsschnittstelle 75
 - Konfigurierte Geschwindigkeit/konfigurierter Modus 109
 - Kontakt 63
 - Kontrollmodus 211 , 301
 - Kosten 489 , 490
- L**
- Land 100
 - Layer 4-Protokoll 176
 - LCP-Erreichbarkeitsprüfung 271 , 276
, 290 , 299 , 350 , 358
 - LDAP-URL-Pfad 105
 - Lease Time 409

- Lebensdauer 322 , 330
 - Letzte gespeicherte Konfiguration 60
 - Level 471 , 484
 - Link-Präfix 183
 - Link-Präfix aktiv 185
 - Link-Status-ID 497
 - Lizenzschlüssel 73
 - Lizenzseriennummer 73
 - Lokale Adresse 492
 - Lokale GRE-IP-Adresse 365
 - Lokale IP-Adresse 175 , 228 , 269 ,
275 , 281 , 289 , 298 , 309 , 345 ,
348 , 357 , 365
 - Lokale IPv6-Adresse 294
 - Lokale PPTP-IP-Adresse 276
 - Lokale Zertifikatsbeschreibung 103 ,
104 , 422
 - Lokale IP-Adresse 486
 - Lokale ID 306 , 486
 - Lokaler Dateiname 422
 - Lokaler Hostname 343
 - Lokaler ID-Typ 306 , 322
 - Lokaler ID-Wert 322
 - Lokaler Port 492
 - Lokaler Port 486
 - Lokales Zertifikat 322
 - Lokales Zertifikat 402
 - Long Retry Limit 159
 - Loopback aktiv 187
 - Löschen/Editieren aller Routing-Einträge
erlauben 182
- M**
- MAC-Adresse 127 , 411 , 492 , 493
 - Mail-Exchanger (MX) 405
 - Manuelle IP-Adresse des WLAN-
Controller 63
 - Manueller Reset des Gerätes 18
 - Master down trials 456
 - Max. Clients 163
 - Max. Queue-Größe 217
 - Max. Übertragungsrate 158
 - Max. eingehende Kontrollverbindungen
über entfernte IP-Adresse 362
 - Maximale Antwortzeit 250
 - Maximale Anzahl der erneuten Einwähl-
versuche 271 , 276 , 282 , 290
 - Maximale Upload-Geschwindigkeit
211 , 214 , 301
 - Maximale Anzahl der Accounting-
Protokolleinträge 63
 - Maximale Anzahl der Syslog-
Protokolleinträge 63
 - Maximale Gruppen 253
 - Maximale Quellen 253
 - Maximale Anzahl Wiederholungen
345
 - Maximale Anzahl der IGMP-
Statusmeldungen 250
 - Maximale Anzahl der IGMP-
Statusmeldungen 253
 - Maximale E-Mails pro Minute 478
 - Maximale TTL für negative Cacheeinträ-
ge 392
 - Maximale TTL für positive Cacheeinträ-
ge 392
 - Maximale Zeit zwischen Versuchen
345
 - Maximales Nachrichtenlevel von Sy-
stemprotokolleinträgen 63
 - Metrik 175 , 309
 - Metrik (Direkte Routen) 242
 - Metrik-Offset für Inaktive
Schnittstellen 234
 - Metrik-Offset für Aktive Schnittstellen
234
 - Metrikbestimmung 242
 - MIB-Variablen 422
 - Min. Queue-Größe 217
 - Minimale Zeit zwischen Versuchen
345
 - Mitglieder 379 , 380 , 386
 - Mobilfunk-Anbieter 119
 - Modem-Status 119
 - Modus 98 , 176 , 181 , 228 , 250 ,
253 , 286 , 319 , 322 , 336
 - Modus / Bridge-Gruppe 75
 - Modus des D-Kanals 319

Monitoring-Modus 458
 MSN 116
 MSN-Erkennung 116
 MTU 273 , 365 , 486
 Multicast-Gruppen-Adresse 255 , 260
 , 500 , 502 , 502 , 503 , 504 , 505 ,
 506
 Multicast-Gruppenbereich 260
 Multicast-Routing 249

N

Nach Ausführung neu starten 422
 Nachbar 496
 Nachricht 484
 Nachrichten 486
 Nachrichtenkomprimierung 475
 Nachrichtentyp 471
 Name 152 , 336
 Name der Quelldatei 466
 Name der Zieldatei 466
 NAT 492
 NAT aktiv 187
 NAT-Eintrag erstellen 269 , 275 , 281
 , 289 , 348 , 357
 NAT-Erkennung 486
 NAT-Methode 189
 NAT-Traversal 327
 Negativer Cache 392
 Netzmaske 228 , 348
 Netzwerkadresse 228
 Netzwerkkonfiguration 228
 Netzwerkname (SSID) 163
 Netzwerkqualität 119
 Netzwerktyp 175 , 183
 Neue Quell-IP-Adresse/Netzmaske
 176 , 193
 Neue Ziel-IP-Adresse/Netzmaske 193
 Neuer Quell-Port 193
 Neuer Ziel-Port 193
 Neuer Dateiname 466
 Neustart des Geräts nach 422
 Nicht geändert seit 491
 Nicht-Mitglieder verwerfen 139
 Nr. 181 , 484 , 491

Nutzererkennung 294
 Nutzungsart 282

O

On Link Flag 133 , 186
 Organisation 100
 Organisationseinheit 100
 Ort 100
 OSPF-Modus 286 , 299 , 351 , 360
 OSPF-Status 245
 Override Interval 257

P

Pakete 486
 Passwort 98 , 103 , 104 , 267 , 274 ,
 280 , 288 , 294 , 336 , 343 , 347 ,
 355 , 404 , 413 , 422 , 466 , 478
 Passwörter und Schlüssel als Klartext
 anzeigen 66
 Peer-Adresse 306
 Peer-ID 306
 PFS-Gruppe verwenden 330
 Phase-1-Profil 314
 Phase-2-Profil 314
 Physische Adresse 493
 PIM-Modus 257
 PIM-Status 261
 Ping 77
 Ping-Befehl testweise an Adresse sen-
 den 461
 Ping-Test 461
 PMTU propagieren 333
 Poisoned Reverse 235
 Pool-Verwendung 408
 POP3-Server 478
 POP3-Timeout 478
 Port 187 , 406 , 493
 Port-Verwendung 112
 Portname 112
 Positiver Cache 392
 PPPoE-Ethernet-Schnittstelle 267
 PPPoE-Modus 267
 PPPoE-Schnittstelle für Mehrfachlink

- 267
 - PPTP-Adressmodus 276
 - PPTP-Inaktivität 378
 - PPTP-Modus 355
 - PPTP-Passthrough 187
 - PPTP-Schnittstelle 274
 - Präfix 132 , 185
 - Präfix aktiv 183
 - Präfixlänge der Multicast-Gruppe 260
 - Präfixlänge der Multicast-Gruppe 500
 - Präfixmodus 128 , 270
 - Pre-Empt-Modus (zurück in Master-Status) 456
 - Preshared Key 164 , 306
 - Primärer DNS-Server 395
 - Primärer DHCP-Server 412
 - Primary IP Address 451
 - Priorisierungsalgorithmus 211
 - Priorisierungsqueue 214
 - Priorität 85 , 90 , 200 , 214 , 370 , 395
 - Priorität der virtuellen Schnittstelle 455
 - Privaten Schlüssel generieren 98
 - Propagation Delay 257
 - Proposals 322 , 330
 - Protokoll 190 , 200 , 204 , 220 , 313 , 383 , 406 , 422 , 471
 - Protokollformat 474
 - Protokollierte Aktionen 377
 - Protokollierungslevel 79
 - Provider 404
 - Providername 406
 - Proxy ARP 134 , 315
 - Proxy-ARP-Modus 286 , 299 , 351 , 360
 - Proxy-Schnittstelle 252
 - PUK 119
 - PVID 139
- Q**
- QoS anwenden 370
 - QoS-Queue 494
 - Quell-IP-Adresse 416 , 422 , 434 , 438 , 502 , 503 , 505 , 506
 - Quell-IP-Adresse/Netzmaske 190 , 200 , 204 , 220 , 313
 - Quell-Port/Bereich 190 , 200 , 204 , 220
 - Quelladresse/Länge 180
 - Quelle 171 , 370 , 373 , 422 , 466
 - Quellport 176 , 190 , 313
 - Quellportbereich 383
 - Quellschnittstelle 176 , 200 , 255
 - Queued 494
 - Queues/Richtlinien 211
- R**
- RA-Signierungszertifikat 98
 - RA-Verschlüsselungszertifikat 98
 - RADIUS-Dialout 87
 - RADIUS-Passwort 85
 - RADIUS-Server 164
 - RADIUS-Server Gruppen-ID 336
 - Real Time Jitter Control 211
 - Regelkette 224 , 226
 - Region 148
 - Register Suppression Timer 261
 - Remote-Adresse 492
 - Rendezvous Point IP-Adresse 260
 - Reset 18
 - Retransmission Timer 237
 - Reverse-Path-Forwarding (RPF) 502 , 503
 - RFC 2091-Variabler Timer 235
 - RFC 2453-Variabler Timer 235
 - Richtlinie 87 , 91
 - Richtung 207 , 234 , 489 , 490
 - Richtung des Datenverkehrs 416
 - RIP-UDP-Port 235
 - Robustheit 250
 - Rolle 336
 - Rolle bei der Präfixdelegation 128
 - Route aktiv 180
 - Routenankündigung 231
 - Routeneinträge 269 , 275 , 281 , 289 , 298 , 309 , 348 , 357 , 365
 - Routenselektor 198
 - Routentimeout 236

- Routentyp 175 , 180
- Router Advertisement übertragen 128
- Router-Gültigkeitsdauer 135
- Router-ID 496 , 497
- Router-Präferenz 135
- RSA-Schlüsselstatus 81
- RTS Threshold 159
- RTT-Modus (Realtime-Traffic-Modus) 214
- Rufnummer 286
- ruhend 263
- Rx-Bytes 491 , 492
- Rx-Fehler 491
- Rx-Pakete 491 , 492

- S**

- SAs mit dem Status der ISP-Schnittstelle synchronisieren 340
- SCEP-Server-URL 422
- SCEP-URL 98
- Schedule-Intervall 432
- Schlüssel zur Authentisierung 242
- Schlüsselgröße 422
- Schlüsselwert 365
- Schnittstelle 76 , 78 , 139 , 148 , 175 , 181 , 189 , 197 , 211 , 226 , 234 , 250 , 257 , 301 , 375 , 395 , 398 , 404 , 408 , 422 , 437 , 442 , 447 , 489 , 490 , 493 , 494 , 495 , 496 , 500 , 500 , 504 , 505 , 506
- Schnittstelle des virtuellen Routers 455
- Schnittstelle ist UPnP-kontrolliert 442
- Schnittstelle - Verbindungsinformation - Status 61
- Schnittstellen 207
- Schnittstellenaktion 437
- Schnittstellenauswahl 228
- Schnittstellenbeschreibung 75
- Schnittstellenmodus 127 , 395
- Schnittstellenstatus 416
- Schnittstellenstatus festlegen 422
- Schweregrad 475
- Sekundärer DNS-Server 395
- Sekundärer DHCP-Server 412
- Sendintervall für Advertisements 456
- Sendeleistung 153
- Senden 494
- Sequence Age 497
- Sequenznummern der Datenpakete 345
- Seriell-USB-Treiber 25 , 25
- Seriennummer 60
- Server 406
- Server Timeout 87
- Server aktivieren 414
- Server-IP-Adresse 85 , 90
- Server-URL 422
- Serveradresse 422
- Serverfehler 401
- Setze COS Wert (802.1p/Layer 2) 207
- Setze DSCP/TOS Wert (Layer 3) 207
- Short Guard Interval 159
- Short Retry Limit 159
- Shortest Path Tree 502
- Sicherheitsalgorithmus 485
- Sicherheitsmodus 164
- Sicherheitsrichtlinie 128 , 270 , 294
- SIM-Karte verwendet PIN 119
- SIP Port 388
- SIP-Aufrufe priorisieren 388
- SIP-Proxy 388
- Slave-AP-Standort 148
- SMTP-Authentifizierung 478
- SMTP-Server 478
- SNMP 77
- SNMP Read Community 66
- SNMP Trap Broadcasting 480
- SNMP Write Community 66
- SNMP-Listen-UDP-Port 82
- SNMP-Trap-Community 480
- SNMP-Trap-UDP-Port 480
- SNMP-Version 82
- Special Handling Timer 200
- Speicherkarte 61
- Sprache für Anmeldefenster 447

- SSH 77
 - SSH-Dienst aktiv 79
 - Staat/Provinz 100
 - Stack 489
 - Standard-Benutzerpasswort 85
 - Standardmäßige Routenverteilung 235
 - Standardroute 269 , 275 , 281 , 289 , 298 , 309 , 348 , 357 , 365
 - Standardroute für Bereich eintragen (nur ABR) 240
 - Standardroute für AS eintragen 245
 - Standardrouter 128
 - Standort 63 , 152
 - Startmodus 314
 - Startzeit 420 , 490
 - Status 416 , 485 , 488 , 489 , 491 , 492 , 495 , 496
 - Status festlegen 422
 - Status des Auslösers 422
 - Stoppzeit 420
 - Stub Interface Mode 257
 - Subjektname 422
 - Subnetz 132 , 185
 - Subsystem 484
 - Switch-Port 109
 - Synchronisationsmodus 459
 - System als Zeitserver 69
 - Systemadministrator-Passwort bestätigen 66
 - Systemdatum 60
 - Systemlogik 466
 - Systemname 63
- T**
- TACACS+-Passwort 90
 - TCP-ACK-Pakete priorisieren 271 , 276 , 290 , 299 , 350 , 358
 - TCP-Inaktivität 378
 - TCP-Keepalives 79
 - TCP-MSS-Clamping 134
 - TCP-Port 91
 - TCP-Port des CAPI-Servers 414
 - Telnet 77
 - Test-Ping-Modus 461
 - Tickettyp 449
 - Timeout 91 , 441
 - Timeout bei Inaktivität 267 , 274 , 280 , 288 , 347 , 355
 - Timeout für Nachrichten 475
 - Traceroute-Adresse 463
 - Traceroute-Modus 463
 - Traceroute-Test 463
 - Traffic Shaping 211 , 214 , 375
 - Trigger 437
 - Triggered-Hello-Intervall 257
 - TTL 397
 - Tunnel-ID 294
 - Tunnelmodus 294
 - Tunnelprofil 347
 - Tx-Bytes 491 , 492
 - Tx-Fehler 491
 - Tx-Pakete 491 , 492
 - Typ 204 , 220 , 383 , 491 , 497
- U**
- Über Schnittstelle 294
 - Überbuchen zugelassen 214
 - Überprüfung anhand einer Zertifikatsperlliste (CRL) 95
 - Überprüfung der Rückroute 315
 - Überprüfung der Rückroute 181
 - Übertragener Datenverkehr 416
 - Übertragungsmodus 319
 - Übertragungsschlüssel 164
 - Überwachte IP-Adresse 434
 - Überwachte Schnittstelle 416 , 437
 - Überwachte Subsysteme 475
 - Überwachte Variable 416
 - Überwachte Schnittstellen 440
 - Überwachtes Zertifikat 416
 - UDP-Inaktivität 378
 - UDP-Port 87
 - UDP-Quellport 344
 - UDP-Quellportauswahl 353
 - UDP-Zielport 344 , 353
 - UMTS/LTE-Schnittstelle 288
 - UMTS/LTE-Status 119

Ungültige DNS-Pakete 401
 Unveränderliche Parameter 202
 Updates der Routing-Tabelle aufgrund
 von External Advertisements
 498
 UPnP TCP Port 443
 UPnP-Status 443
 Upstream Nachbar-IP-Adresse 501 ,
 502 , 502
 Upstream Join State 501 , 502 , 502
 Upstream Join Timer 501 , 502 , 502
 Upstream Override Timer 503
 Upstream-Präfixe 132
 Upstream-Schnittstelle 132 , 183
 Uptime 60 , 500 , 501 , 502 , 502 ,
 503 , 504 , 505 , 506
 URL 171 , 466

V

Verbindungsstatus 204 , 220
 Verbindungstyp 280 , 347
 Verbleibende Gültigkeitsdauer 416
 Vergleichsbedingung 416
 Vergleichswert 416
 Vermeidung von Datenstau (RED)
 217
 Verschlüsselt 488
 Verschlüsselung 91 , 282 , 350 , 358
 Verschlüsselung der Konfiguration
 466
 Verschlüsselungsalgorithmen 80
 Version in Empfangsrichtung 231
 Version in Senderichtung 231
 Versionsprüfung 422
 Versuche 416 , 422 , 438
 Verteilungsmodus 195
 Verteilungsrichtlinie 195 , 197
 Verteilungsverhältnis 197
 Vertrauenswürdigkeit des Zertifikats er-
 zwingen 95
 Verwaltungs-VID 140
 Verwendeter Kanal 153
 Verwerfen ohne Rückmeldung 226
 Verwerfen ohne Rückmeldung 187

Verworfen 488 , 494
 Virtual Router Backup 451
 Virtual Router Master 451
 Virtueller Router 451
 VLAN 167 , 267
 VLAN Identifier 138
 VLAN aktivieren 140
 VLAN-ID 127 , 167 , 267
 VLAN-Mitglieder 138
 VLAN-Name 138
 Vollständige Filterung 377
 Vollständige IPSec-Konfiguration lö-
 schen 338
 Vom NAT ausnehmen (DMZ) 228
 Vorrang 260
 VRRP Advertisement 451
 VRRP-Router 451

W

Wählnummer 440
 Walled Garden 447
 Walled Garden URL 447
 Walled Network / Netzmaske 447
 Weitergeleitet 488
 Weitergeleitete Anfragen 401
 Weiterleiten 398
 Weiterleiten an 398
 WEP-Schlüssel 1-4 164
 Werkseinstellung 18
 Wiederholungen 87
 Wildcard 405
 WINS-Server 392
 Wird ausgeführt 171
 WLC-SSID 422
 WMM 163
 WPA Cipher 164
 WPA-Modus 164
 WPA2 Cipher 164

X

X.31 TEI-Dienst 114
 X.31 TEI-Wert 114
 X.31 (X.25 im D-Kanal) 114

- XAUTH-Profil 314
- Z**
- Zeit 484
- Zeit einstellen 69
- Zeitaktualisierungsintervall 69
- Zeitaktualisierungsrichtlinie 69
- Zeitbedingung 420
- Zeitstempel 471
- Zeitzone 68
- Zero Cookies verwenden 340
- Zertifikat in Konfiguration schreiben
422
- Zertifikat ist ein CA-Zertifikat 95
- Zertifikate und Schlüssel einschließen
466
- Zertifikatsanforderungs-Payloads nicht
beachten 341
- Zertifikatsanforderungs-Payloads sen-
den 341
- Zertifikatsanforderungsbeschreibung
98 , 422
- Zertifikatsketten senden 341
- Ziel 370 , 373
- Ziel-IP-Adresse 416 , 422 , 438
- Ziel-IP-Adresse/Netzmaske 175 , 190
, 200 , 204 , 220 , 313
- Ziel-Port/Bereich 190 , 200 , 204 ,
220
- Zieladresse/Länge 180
- Zielport 176 , 313
- Zielportbereich 383
- Zielschnittstelle 180 , 255
- Zu verwendende Schnittstelle 461
- Zugewiesene Drahtlosnetzwerke
(VSS) 153
- Zugewiesener IPv6-Präfix/Länge 294
- Zugriff 413
- Zugriffsfiler 224
- Zulässiger Hotspot-Client 449
- Zusammenfassend 100
- Zusätzliche IPv6-Adresskonfiguration
128
- Zusätzliche, frei zugängliche Domänen-
namen 447
- Zusätzlicher Filter des Datenverkehrs
311 , 313
- Zweiter Zeitserver 69