

Benutzerhandbuch bintec RS-Serie

Referenz

Copyright© Version 9.0, 2014 bintec elmeg GmbH

Rechtlicher Hinweis

Ziel und Zweck

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

Haftung

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

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

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

Marken

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

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

Copyright

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

Richtlinien und Normen

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

Wie Sie bintec elmeg GmbH erreichen

bintec elmeg GmbH, Südwestpark 94, D-90449 Nürnberg, Deutschland, Telefon: +49 911 9673 0, Fax: +49 911 688 07 25

Teldat France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradignan, Frankreich, Telefon: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05

Internet: www.teldat.fr

Inhaltsverzeichnis

Kapitel 1	Einleitung	1
Kapitel 2	Zum Handbuch	3
Kapitel 3	Inbetriebnahme	6
3.1	bintec RS120 und bintec RS120wu	6
3.1.1	Aufstellen und Anschließen	6
3.1.2	Anschlüsse	8
3.1.3	Antennenanschlüsse	10
3.1.4	LEDs	10
3.1.5	Lieferumfang	12
3.1.6	Allgemeine Produktmerkmale	12
3.1.7	Reset	14
3.2	bintec RS230a, bintec RS230aw und bintec RS230au+	15
3.2.1	Aufstellen und Anschließen	15
3.2.2	Anschlüsse	18
3.2.3	Antennenanschlüsse	19
3.2.4	LEDs	19
3.2.5	Lieferumfang	21
3.2.6	Allgemeine Produktmerkmale	22
3.2.7	Reset	24
3.3	bintec RS232j, bintec RS232jw und bintec RS232j-4G	24
3.3.1	Aufstellen und Anschließen	25
3.3.2	Anschlüsse	28
3.3.3	Antennenanschlüsse	29
3.3.4	LEDs	29
3.3.5	Lieferumfang	31
3.3.6	Allgemeine Produktmerkmale	32
3.3.7	Reset	34

3.4	Reinigen	35
3.5	Pin-Belegungen	35
3.5.1	Serielle Schnittstelle	35
3.5.2	Ethernet-Schnittstelle	36
3.5.3	ADSL-Schnittstelle	36
3.5.4	ISDN-S0-Schnittstelle	37
3.5.5	USB-Schnittstelle	38
3.6	SIM-Karte einsetzen	38
3.7	Support Information	39
3.8	WEEE-Information	40
Kapitel 4	Grundkonfiguration	41
4.1	Voreinstellungen	41
4.1.1	IP-Konfiguration	41
4.1.2	Software-Update	42
4.2	System-Voraussetzungen	42
4.3	Vorbereitung	42
4.3.1	Daten sammeln	43
4.3.2	PC einrichten	46
4.3.3	Systempasswort ändern	47
4.4	Internetverbindung einrichten.	47
4.4.1	Internetverbindung über das interne ADSL-Modem	47
4.4.2	Internetverbindung über UMTS/LTE	48
4.4.3	Andere Internetverbindungen.	48
4.4.4	Konfiguration prüfen	48
4.5	Wireless LAN einrichten	49
4.6	Softwareaktualisierung	50

Kapitel 5	Zugang und Konfiguration	52
5.1	Zugangsmöglichkeiten	52
5.1.1	Zugang über LAN.	52
5.1.2	Zugang über die serielle Schnittstelle	55
5.1.3	Zugang über ISDN	57
5.2	Anmelden	58
5.2.1	Benutzernamen und Passwörter im Auslieferungszustand	58
5.2.2	Anmelden zur Konfiguration	59
5.3	Konfigurationsmöglichkeiten	60
5.3.1	GUI (Graphical User Interface)	60
5.3.2	SNMP Shell	71
5.4	BOOTmonitor	71
Kapitel 6	Assistenten	73
Kapitel 7	Systemverwaltung	74
7.1	Status.	74
7.2	Globale Einstellungen	77
7.2.1	System	77
7.2.2	Passwörter	80
7.2.3	Datum und Uhrzeit	82
7.2.4	Systemlizenzen	88
7.3	Schnittstellenmodus / Bridge-Gruppen	90
7.3.1	Schnittstellen.	92
7.4	Administrativer Zugriff	96
7.4.1	Zugriff.	96
7.4.2	SSH	97
7.4.3	SNMP.	101

7.5	Remote Authentifizierung	103
7.5.1	RADIUS	103
7.5.2	TACACS+	109
7.5.3	Optionen	113
7.6	Konfigurationszugriff	114
7.6.1	Zugriffsprofile	114
7.6.2	Benutzer	117
7.7	Zertifikate	121
7.7.1	Zertifikatsliste	122
7.7.2	CRLs	131
7.7.3	Zertifikatsserver	132
Kapitel 8	Physikalische Schnittstellen	134
8.1	Ethernet-Ports	134
8.1.1	Portkonfiguration	135
8.2	ISDN-Ports	138
8.2.1	ISDN-Konfiguration	139
8.2.2	MSN-Konfiguration	142
8.3	DSL-Modem	145
8.3.1	DSL-Konfiguration	145
8.4	UMTS/LTE.	148
8.4.1	UMTS/LTE.	148
Kapitel 9	LAN	159
9.1	IP-Konfiguration	159
9.1.1	Schnittstellen	159
9.2	VLAN	163
9.2.1	VLANs	165
9.2.2	Portkonfiguration	166

9.2.3	Verwaltung	167
Kapitel 10	Wireless LAN	168
10.1	WLAN.	169
10.1.1	Einstellungen Funkmodul	169
10.1.2	Drahtlosnetzwerke (VSS)	184
10.1.3	WDS-Links.	191
10.1.4	Client Link	194
10.2	Verwaltung	198
10.2.1	Grundeinstellungen	198
Kapitel 11	Netzwerk	200
11.1	Routen	200
11.1.1	Konfiguration von IPv4-Routen	200
11.1.2	IPv4-Routing-Tabelle	207
11.1.3	Optionen	208
11.2	NAT.	210
11.2.1	NAT-Schnittstellen	210
11.2.2	NAT-Konfiguration	211
11.3	Lastverteilung	218
11.3.1	Lastverteilungsgruppen	218
11.3.2	Special Session Handling	223
11.4	QoS	227
11.4.1	QoS-Filter	227
11.4.2	QoS-Klassifizierung	231
11.4.3	QoS-Schnittstellen/Richtlinien	234
11.5	Zugriffsregeln	242
11.5.1	Zugriffsfilter	243
11.5.2	Regelketten	247
11.5.3	Schnittstellenzuweisung	249

11.6	Drop-In	251
11.6.1	Drop-In-Gruppen	251
Kapitel 12	Routing-Protokolle	254
12.1	RIP	254
12.1.1	RIP-Schnittstellen.	254
12.1.2	RIP-Filter	257
12.1.3	RIP-Optionen	259
Kapitel 13	Multicast.	263
13.1	Allgemein	265
13.1.1	Allgemein	265
13.2	IGMP	265
13.2.1	IGMP	266
13.2.2	Optionen	269
13.3	Weiterleiten	270
13.3.1	Weiterleiten	270
Kapitel 14	WAN.	272
14.1	Internet + Einwählen	272
14.1.1	PPPoE	275
14.1.2	PPTP	280
14.1.3	PPPoA	285
14.1.4	ISDN	290
14.1.5	UMTS/LTE.	299
14.1.6	IP Pools	304
14.2	ATM	305
14.2.1	Profile.	306
14.2.2	Dienstkategorien	311

14.2.3	OAM-Regelung	314
14.3	Real Time Jitter Control	318
14.3.1	Regulierte Schnittstellen	318
Kapitel 15	VPN	320
15.1	IPSec	320
15.1.1	IPSec-Peers	321
15.1.2	Phase-1-Profile	339
15.1.3	Phase-2-Profile	347
15.1.4	XAUTH-Profile	353
15.1.5	IP Pools	355
15.1.6	Optionen	357
15.2	L2TP	361
15.2.1	Tunnelprofile	361
15.2.2	Benutzer	365
15.2.3	Optionen	371
15.3	PPTP	372
15.3.1	PPTP-Tunnel	372
15.3.2	Optionen	380
15.3.3	IP Pools	381
15.4	GRE	382
15.4.1	GRE-Tunnel	382
Kapitel 16	Firewall	385
16.1	Richtlinien	387
16.1.1	Filterregeln	387
16.1.2	QoS	390
16.1.3	Optionen	392
16.2	Schnittstellen	393
16.2.1	Gruppen	393

16.3	Adressen	394
16.3.1	Adressliste.	395
16.3.2	Gruppen.	396
16.4	Dienste	396
16.4.1	Diensteliste	397
16.4.2	Gruppen.	399
Kapitel 17	VoIP	401
17.1	SIP	401
17.1.1	Optionen	401
17.2	RTSP	402
17.2.1	RTSP-Proxy	402
Kapitel 18	Lokale Dienste	404
18.1	DNS	404
18.1.1	Globale Einstellungen	406
18.1.2	DNS-Server	408
18.1.3	Statische Hosts.	410
18.1.4	Domänenweiterleitung.	412
18.1.5	Cache.	414
18.1.6	Statistik	415
18.2	HTTPS	416
18.2.1	HTTPS-Server	416
18.3	DynDNS-Client	417
18.3.1	DynDNS-Aktualisierung	417
18.3.2	DynDNS-Provider.	419
18.4	DHCP-Server	421
18.4.1	IP-Pool-Konfiguration	422
18.4.2	DHCP-Konfiguration	422

18.4.3	IP/MAC-Bindung	427
18.4.4	DHCP-Relay-Einstellungen	428
18.5	Web-Filter	429
18.5.1	Allgemein	429
18.5.2	Filterliste	431
18.5.3	Black / White List	433
18.5.4	Verlauf	434
18.6	CAPI-Server	435
18.6.1	Benutzer	435
18.6.2	Optionen	436
18.7	Scheduling.	437
18.7.1	Auslöser.	438
18.7.2	Aktionen	444
18.7.3	Optionen	457
18.8	Überwachung	457
18.8.1	Hosts	458
18.8.2	Schnittstellen.	460
18.8.3	Ping-Generator.	462
18.9	ISDN-Diebstahlsicherung	463
18.9.1	Optionen	463
18.10	UPnP	465
18.10.1	Schnittstellen.	466
18.10.2	Allgemein	467
18.11	Hotspot-Gateway	468
18.11.1	Hotspot-Gateway	470
18.11.2	Optionen	474
18.12	Wake-On-LAN	475
18.12.1	Wake-on-LAN-Filter.	475
18.12.2	WOL-Regeln	478
18.12.3	Schnittstellenzuweisung	480

18.13	BRRP	481
18.13.1	Virtuelle Router	483
18.13.2	VR-Synchronisation	489
18.13.3	Optionen	490
Kapitel 19	Wartung	492
19.1	Diagnose	492
19.1.1	Ping-Test	492
19.1.2	DNS-Test	493
19.1.3	Traceroute-Test	493
19.2	Software & Konfiguration	494
19.2.1	Optionen	494
19.3	Neustart	499
19.3.1	Systemneustart.	499
Kapitel 20	Externe Berichterstellung.	501
20.1	Systemprotokoll	501
20.1.1	Syslog-Server	502
20.2	IP-Accounting	504
20.2.1	Schnittstellen.	504
20.2.2	Optionen	505
20.3	Benachrichtigungsdienst	506
20.3.1	Benachrichtigungsempfänger	506
20.3.2	Benachrichtigungseinstellungen	509
20.4	SNMP.	511
20.4.1	SNMP-Trap-Optionen	511
20.4.2	SNMP-Trap-Hosts	513
20.5	Activity Monitor	513
20.5.1	Optionen	514

Kapitel 21	Monitoring	516
21.1	Internes Protokoll	516
21.1.1	Systemmeldungen	516
21.2	IPSec	517
21.2.1	IPSec-Tunnel	518
21.2.2	IPSec-Statistiken	520
21.3	ISDN/Modem	521
21.3.1	Aktuelle Anrufe	522
21.3.2	Anrufliste	522
21.4	Schnittstellen.	523
21.4.1	Statistik	523
21.5	WLAN.	526
21.5.1	WLANx	526
21.5.2	VSS	528
21.5.3	Client Links	531
21.6	Bridges	534
21.6.1	br<x>	534
21.7	Hotspot-Gateway	534
21.7.1	Hotspot-Gateway	534
21.8	QoS	535
21.8.1	QoS	535
	Glossar	537
	Index	568

Kapitel 1 Einleitung

Die leistungsstarken Gateways **RS120**, **RS120wu**, **RS230a**, **RS230aw**, **RS230au+**, **RS232j**, **RS232jw** und **RS232j-4G** ermöglichen Ihnen die kostengünstige Verbindung kleiner Netzwerke sowie die Anbindung Ihres Einzelarbeitsplatzes oder kleinen Unternehmens an das Internet und an andere Partnernetze (z. B. eine Firmenzentrale).

Sicherheitshinweise

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

Installation

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

Konfiguration

Wie Sie Ihr Gerät das Laufen lehren, erfahren Sie im Kapitel [Grundkonfiguration](#) auf Seite 41 . Dort zeigen wir Ihnen, wie Sie Ihr Gerät innerhalb weniger Minuten von einem Windows-PC aus mit einem Konfigurationsassistenten in Betrieb nehmen und wie Sie weitere nützliche Hilfsprogramme installieren. Am Ende dieses Kapitels sind Sie in der Lage, im Internet zu surfen, E-Mails zu verschicken und zu empfangen und eine Verbindung mit einem Partnernetz herzustellen, um beispielsweise auf Daten einer Firmenzentrale zuzugreifen.

Passwort

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

Benutzername: *admin*

Passwort: *admin*



Hinweis

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

Alle bintec elmeg-Geräte werden mit gleichem Passwort ausgeliefert. Sie sind daher erst gegen einen unauthorisierten Zugriff geschützt, wenn Sie das Passwort ändern.

Die Vorgehensweise bei der Änderung von Passwörtern ist im Kapitel [Systempasswort ändern](#) auf Seite 47 beschrieben.

Workshops

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

Dime Manager

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

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

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

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

Kapitel 2 Zum Handbuch

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

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

Benutzerhandbuch - Referenz

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

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

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

Symbolübersicht

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

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

Auszeichnungselemente

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

Kapitel 3 Inbetriebnahme



Achtung

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

3.1 bintec RS120 und bintec RS120wu

3.1.1 Aufstellen und Anschließen



Hinweis

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



Achtung

Die Verwendung eines falschen Netzgerätes kann zum Defekt Ihres Geräts führen! Verwenden Sie ausschließlich das mitgelieferte Netzgerät! Falls Sie ausländische Adapter/Netzteile benötigen, wenden Sie sich bitte an unseren bintec elmeg Service.

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

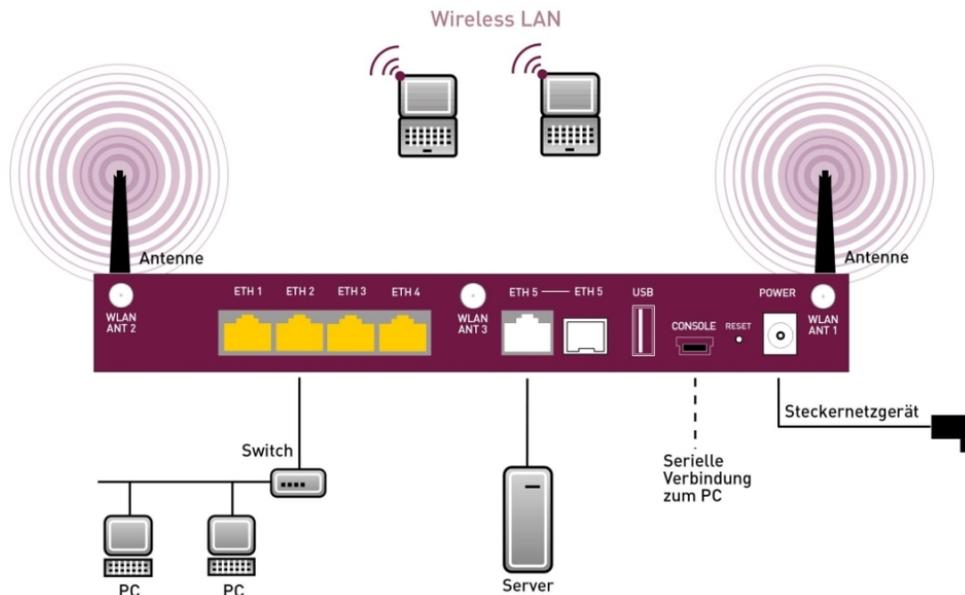


Abb. 2: Anschlussmöglichkeiten am Beispiel **bintec RS120wu**

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

- (1) Antennen

Bei **bintec RS120wu** schrauben Sie die mitgelieferten externen WLAN-Antennen auf die dafür vorgesehenen RSMA-Anschlüsse, und zusätzlich die zwei UMTS-Antennen auf die SMA-Anschlüsse.
- (2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.
- (3) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den ersten Switch-Port (1, gelbe Buchse) Ihres Geräts über das mitgelieferte Ethernet-Kabel (gelbes 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 mit dem mitgelieferten Netzgerät an eine Steckdose an.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- DMZ

Verbinden Sie die WAN-Schnittstelle (**ETH**, weiße Buchse) Ihres Geräts über ein weiteres Ethernet-Kabel mit dem Ethernet-Anschluss Ihrer DMZ.

- USB

Schließen Sie an die USB-Schnittstelle Ihres Geräts einen Mobilfunk-Stick an.

- Weitere LANs/WANs

Schließen Sie beliebige weitere Endgeräte in Ihrem Netzwerk an den verbleibenden Switch-Ports (**2, 3** oder **4**) Ihres Geräts mittels weiterer Ethernet-Kabeln an.

- Serielle Verbindung

Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs mit der seriellen Schnittstelle des Geräts (**Console**). Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen. Ein passendes Kabel ist als Zubehör erhältlich.

Das Gerät ist nun für die Konfiguration mit dem **GUI** vorbereitet. Im Kapitel *Grundkonfiguration* auf Seite 41 finden Sie ausführliche Schritt-für-Schritt-Anleitungen zu den grundlegenden Funktionen Ihres Geräts.

Montage

Die Geräte sind wahlweise durch Laschen im Gehäuse an die Wand, oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

Befestigen Sie die selbstklebenden Gummifüßchen an der Unterseite des Geräts. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wandmontage

Um die Geräte der **bintec RS120x**-Serie an der Wand zu montieren, benutzen Sie die Laschen an der Gehäuserückseite.



Warnung

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

Kensington Lock

Die Geräte bieten die Möglichkeit ein Kensington Lock zu befestigen. Die dazu notwendige Aussparung finden Sie an der rechten Gehäusesseite.

3.1.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts.

bintec RS120 und **bintec RS120wu** verfügen über einen 4-Port Gigabit Switch, über einen Gigabit LAN/WAN-Anschluss sowie über eine serielle Schnittstelle, einen SFP LAN-Anschluss und einen USB-Anschluss. **bintec RS120wu** verfügt über Anschlüsse für 3 externe WLAN Antennen und zusätzlich für 2 externe UMTS Antennen.



Hinweis

Beachten Sie, dass der SFP-Anschluss von **bintec RS120** und **bintec RS120wu** nicht hotswap-fähig ist. Schalten Sie das Gerät vor dem Stecken eines SFP-Moduls aus und starten Sie das Gerät danach neu. Sie können für ETH5 nur entweder den Ethernet- oder den SFP-Anschluss betreiben. Bei einem Wechsel zwischen Ethernet- und SFP-Betrieb müssen Sie das Gerät ebenfalls neu starten, damit der Wechsel korrekt vollzogen wird.

Die Anschlüsse sind folgendermaßen angeordnet:

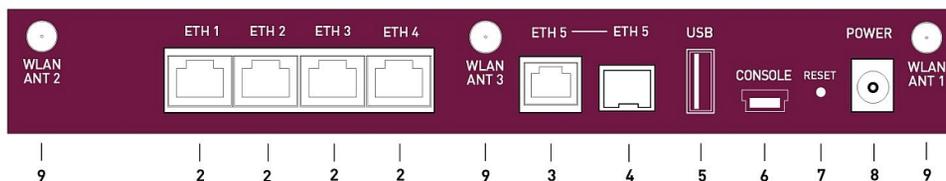


Abb. 3: **bintec RS120wu** Rückseite

Anschlüsse Rückseite

2	ETH1 / ETH2 / ETH3 / ETH4 (gelb)	10/100/1000 Base-T Ethernet-Schnittstelle
3	ETH5 (weiß)	10/100/1000 Base-T Ethernet-Schnittstelle
4	ETH5 (weiß)	SFP Slot für 10/100/1000 Mbit/s Ethernet SFP Module (optional)
5	USB	USB-Anschluss
6	CONSOLE	Serielle Schnittstelle
7	RESET	Reset-Taste
8	POWER	Buchse für Steckernetzteil
9	WLAN ANT1 / ANT2 / ANT3	RSMA-Anschluss (nur bintec RS120wu)
ohne Abb.	UMTS MAIN/AUX	Anschlüsse für UMTS Antennen (nur bintec RS120wu)

3.1.3 Antennenanschlüsse

Die Geräte **bintec RS120wu** haben drei Anschlüsse für die externen WLAN-Antennen und an den Seiten zusätzlich noch zwei Anschlüsse für die externen UMTS-Antennen (SMA-Buchsen). Die Belegung der zwei Antennenanschlüsse können Sie den folgenden Grafiken entnehmen:



Abb. 4: Antennenbelegung der **bintec RS120wu**



Abb. 5: Antennenbelegung der **bintec RS120wu**

3.1.4 LEDs

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

Die LEDs sind folgendermaßen angeordnet:

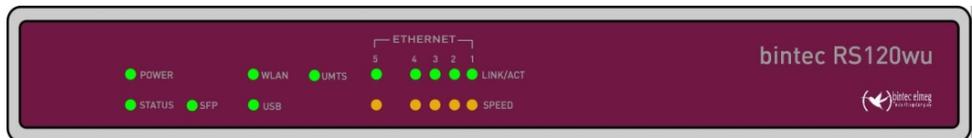


Abb. 6: Anordnung der LEDs

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	Startvorgang

LED	Farbe	Status	Information
	grün	blinkend	Normaler Betrieb
	grün	aus	Fehler
Ethernet 1 bis 4: LINK/ACT	grün	an	Die Verbindung zum LAN ist hergestellt.
	grün	blinkend	Datenverkehr über die LAN-Schnittstelle.
		aus	Kein Anschluss.
Ethernet 1 bis 4: SPEED	grün	an	Das Gerät ist an das LAN angeschlossen mit 1000 Mbit/s.
	orange	an	Das Gerät ist an das LAN angeschlossen mit 100 Mbit/s.
		aus	Das Gerät ist an das LAN angeschlossen mit 10 Mbit/s oder kein Datenverkehr.
Ethernet 5: LINK/ACT	grün	an	Die Verbindung zum WAN ist hergestellt.
	grün	blinkend	Datenverkehr über die WAN-Schnittstelle
		aus	Kein Anschluss.
Ethernet 5: SPEED	grün	an	Das Gerät ist an das WAN angeschlossen mit 1000 Mbit/s.
	orange	an	Das Gerät ist an das WAN angeschlossen mit 100 Mbit/s.
		aus	Das Gerät ist an das LAN angeschlossen mit 10 Mbit/s oder kein Datenverkehr.
SFP	grün	an	SFP-Verbindung ist aktiv.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über die SFP-Schnittstelle.
WLAN (nur bintec RS120wu)	grün	an	Das Funkmodul ist aktiv.
		aus	Kein Anschluss zum Funkmodul.
		blinkend	Datenverkehr über die WLAN-Schnittstelle.
UMTS (nur bintec RS120wu)	grün	an	UMTS/LTE-Verbindung zum Netzwerk über das interne Modem nach erfolgreicher Einwahl.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über das interne UMTS/

LED	Farbe	Status	Information
			LTE-Modem.
USB	grün	an	USB-Gerät ist verbunden.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über USB-Schnittstelle.

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

LED BRRP-Anzeige

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.

3.1.5 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Lieferumfang	bintec RS120	bintec RS120wu
Kabelsätze/Netzteil/Sonstiges	Ethernet-Kabel (gelb) Steckernetzteil	Ethernet-Kabel (gelb) Steckernetzteil
Software	Companion DVD, Dime Manager (auf DVD)	Companion DVD, Dime Manager (auf DVD)
Dokumentation	Kurzanleitung und Sicherheitshinweise (gedruckt)	Kurzanleitung und Sicherheitshinweise (gedruckt)
Online-Dokumentation	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz

3.1.6 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	bintec RS120 und bintec RS120wu
Speicher	64 MB RAM, 16 MB Flash-ROM
Leistungsaufnahme Gerät	4,7 Watt
Spannungsversorgung	12 V DC 800 mA EU PSU
Umweltanforderungen:	
Lagertemperatur	-25 °C bis +70 °C
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 95 % (nichtkondensierend)
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET TM Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec

Weitere Produktmerkmale

Eigenschaft	bintec RS120	bintec RS120wu
Maße und Gewicht:		
Gerätemaße ohne Kabel (B x H x T)	235 mm x 32,6 mm x 147,6 mm	235 mm x 32,6 mm x 147,6 mm
Gewicht	ca. 1000 g	ca. 1100 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1500 g	ca. 1600 g
LEDs	14 (1x Power, 1x Status, 5x2 Ethernet, 2x Funktion)	16 (1x Power, 1x Status, 5x2 Ethernet, 4x Funktion)
Verfügbare Schnittstellen:		
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
Ethernet	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur wisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
SFP LAN Port	SFP Slot für gängige optische 10/100/1000 Mbit/s Ethernet SFP	SFP Slot für gängige optische 10/100/1000 Mbit/s Ethernet SFP

Eigenschaft	bintec RS120	bintec RS120wu
	Module, nicht hotswap-fähig	Module, nicht hotswap-fähig
WLAN-Schnittstelle (Antennen)	-	802.11a/b/g/h mit Antenna Diversity; Datenraten von 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 MBit/s 802.11n; Datenrate bis 300 Mbit/s
UMTS/GPRS	-	Unterstützung von UMTS, HSxPA (HSDPA mit bis zu 7,2 Mbit/s, HSUPA mit bis zu 2,0 Mbit/s), GPRS-, Edge- und GSM, LTE; UMTS/WCDMS Bänder 900/1900/2100 MHz, GSM/GPRS/EDGE Bänder 850/900/1800/1900 MHz,
Vorhandene Buchsen:		
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse	5-polige Mini-USB-Buchse
Ethernet-Schnittstelle (gelb)	RJ45-Buchse	RJ45-Buchse
USB	USB-Anschluss Typ A	USB-Anschluss Typ A
WLAN	-	RSMA-Anschluss
UMTS	-	SMA-Buchsen

3.1.7 Reset

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

Gehen Sie folgendermaßen vor:

- (1) Trennen Sie Ihr Gerät vom Strom.
- (2) Drücken Sie die **Reset**-Taste Ihres Geräts.
- (3) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.
- (4) Lassen Sie nach fünfmaligem Blinken der *Status*-LED die **Reset**-Taste los.

**Hinweis**

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

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 41 beschrieben.

3.2 bintec RS230a, bintec RS230aw und bintec RS230au+

3.2.1 Aufstellen und Anschließen

**Hinweis**

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

**Achtung**

Die Verwendung eines falschen Netzgerätes kann zum Defekt Ihres Geräts führen! Verwenden Sie ausschließlich das mitgelieferte Netzgerät! Falls Sie ausländische Adapter/Netzteile benötigen, wenden Sie sich bitte an unseren bintec elmeg Service.

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

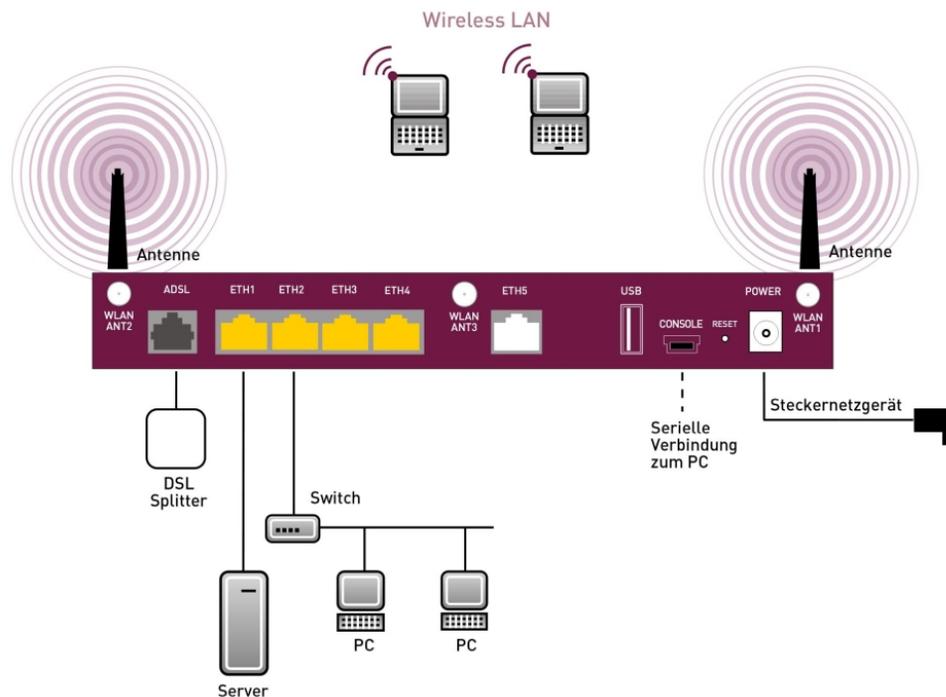


Abb. 7: Anschlussmöglichkeiten am Beispiel **bintec RS230aw**

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

- (1) Antennen

Bei **bintec RS230aw** schrauben Sie die mitgelieferten externen WLAN-Antennen auf die dafür vorgesehenen RSMA-Anschlüsse. Bei **bintec RS230au+** schrauben Sie die zwei UMTS/LTE-Antennen auf die SMA-Anschlüsse.
- (2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.
- (3) LAN

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

Verbinden Sie die ADSL-Schnittstelle (**ADSL**, graue Buchse) Ihres Geräts über das mitgelieferte DSL-Kabel (graues Kabel) mit dem DSL-Ausgang des Splitters.
- (5) Netzanschluss

Schließen Sie das Gerät mit dem mitgelieferten Netzgerät an eine Steckdose an.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- DMZ

Verbinden Sie die WAN-Schnittstelle (**ETH**, weiße Buchse) Ihres Geräts über ein weiteres Ethernet-Kabel mit dem Ethernet-Anschluss Ihrer DMZ.

- Weitere LANs/WANs

Schließen Sie beliebige weitere Endgeräte in Ihrem Netzwerk an den verbleibenden Switch-Ports (**2, 3** oder **4**) Ihres Geräts mittels weiterer Ethernet-Kabeln an.

- USB

Schließen Sie an die USB-Schnittstelle Ihres Geräts einen Mobilfunk-Stick an.

- Serielle Verbindung

Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs mit der seriellen Schnittstelle des Geräts (**Console**). Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen. Ein passendes Kabel ist als Zubehör erhältlich.

Das Gerät ist nun für die Konfiguration mit dem **GUI** vorbereitet. Im Kapitel [Grundkonfiguration](#) auf Seite 41 finden Sie ausführliche Schritt-für-Schritt-Anleitungen zu den grundlegenden Funktionen Ihres Geräts.

Montage

Die Geräte sind wahlweise durch Laschen im Gehäuse an die Wand, oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

Befestigen Sie die selbstklebenden Gummifüßchen an der Unterseite des Geräts. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wandmontage

Um die Geräte der **bintec RS230x**-Serie an der Wand zu montieren, benutzen Sie die Laschen an der Gehäuserückseite.



Warnung

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

Kensington Lock

Die Geräte bieten die Möglichkeit ein Kensington Lock zu befestigen. Die dazu notwendige Aussparung finden Sie an der rechten Gehäuseseite.

3.2.2 Anschlüsse

bintec RS230a , **bintec RS230aw** und **bintec RS230au+** verfügen über einen 4-Port Giga-bit Switch, eine ADSL-Schnittstelle (Annex A), eine serielle Schnittstelle und einen USB-Anschluss. **bintec RS230aw** verfügt über Anschlüsse für 3 externe WLAN Antennen. **bintec RS230au+** verfügt über Anschlüsse für 2 externe UMTS Antennen.

Die Anschlüsse sind folgendermaßen angeordnet:

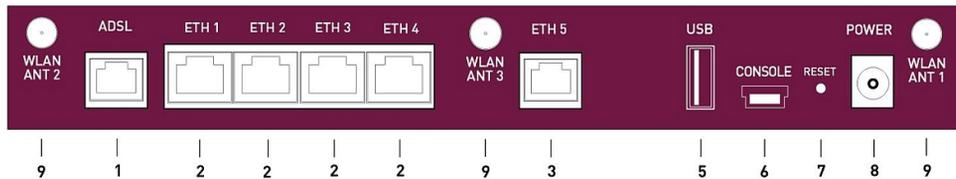


Abb. 8: **bintec RS230aw** Rückseite

Anschlüsse Rückseite

1	ADSL (grau)	ADSL2+-Schnittstelle
2	ETH1 / ETH2 / ETH3 / ETH4 (gelb)	10/100/1000 Base-T Ethernet-Schnittstelle
3	ETH5 (weiß)	10/100/1000 Base-T Ethernet-Schnittstelle
5	USB	USB-Anschluss
6	CONSOLE	Serielle Schnittstelle
7	RESET	Reset-Taste
8	POWER	Buchse für Steckernetzteil
9	WLAN ANT1 / ANT2 / ANT3	RSMA-Anschluss (nur bintec RS230aw)
ohne Abb.	UMTS MAIN/AUX	Anschlüsse für UMTS Antennen (nur bintec RS230au+)

3.2.3 Antennenanschlüsse

Die Geräte **bintec RS230aw** haben drei Anschlüsse für die externen WLAN-Antennen. Die Geräte **bintec RS230au+** haben zwei Anschlüsse für die externe UMTS/LTE-Antennen (SMA-Buchsen). Die Belegung der zwei Antennenanschlüsse können Sie den folgenden Grafiken entnehmen:



Abb. 9: Antennenbelegung der **bintec RS230au+**



Abb. 10: Antennenbelegung der **bintec RS230au+**

3.2.4 LEDs

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

Die LEDs sind folgendermaßen angeordnet:

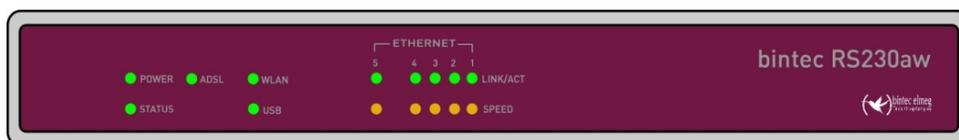


Abb. 11: Anordnung der LEDs

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	Startvorgang

LED	Farbe	Status	Information
	grün	blinkend	Normaler Betrieb
	grün	aus	Fehler
Ethernet 1 bis 4: LINK/ACT	grün	an	Die Verbindung zum LAN ist hergestellt.
	grün	blinkend	Datenverkehr über die LAN-Schnittstelle.
		aus	Kein Anschluss.
Ethernet 1 bis 4: SPEED	grün	an	Das Gerät ist an das LAN angeschlossen mit 1000 Mbit/s.
	orange	an	Das Gerät ist an das LAN angeschlossen mit 100 Mbit/s.
		aus	Das Gerät ist an das LAN angeschlossen mit 10 Mbit/s oder kein Datenverkehr.
Ethernet 5: LINK/ACT	grün	an	Die Verbindung zum WAN ist hergestellt.
	grün	blinkend	Datenverkehr über die WAN-Schnittstelle
		aus	Kein Anschluss.
Ethernet 5: SPEED	grün	an	Das Gerät ist an das WAN angeschlossen mit 1000 Mbit/s.
	orange	an	Das Gerät ist an das WAN angeschlossen mit 100 Mbit/s.
		aus	Das Gerät ist an das LAN angeschlossen mit 10 Mbit/s oder kein Datenverkehr.
ADSL	grün	an	DSL-Verbindung ist aktiv.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über die DSL-Schnittstelle.
WLAN (nur bintec RS230aw)	grün	an	Das Funkmodul ist aktiv.
		aus	Kein Anschluss zum Funkmodul.
		blinkend	Datenverkehr über die WLAN-Schnittstelle.
USB	grün	an	USB-Gerät ist verbunden.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über USB-Schnittstelle.
UMTS (nur bintec	grün	an	UMTS/LTE-Verbindung zum Netzwerk über das interne Modem nach erfolgreicher Ein-

LED	Farbe	Status	Information
RS230au+)			wahl.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über das interne UMTS/ LTE-Modem.

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

LED BRRP-Anzeige

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.

3.2.5 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Lieferumfang	bintec RS230a	bintec RS230aw	bintec RS230au+
Kabelsätze/Netzteil/Sonstiges	Ethernet-Kabel (gelb) ADSL-Kabel für Annex A (grau) Steckernetzteil	Ethernet-Kabel (gelb) ADSL-Kabel für Annex A (grau) Steckernetzteil 3 externe WLAN Antennen	Ethernet-Kabel (gelb) ADSL-Kabel für Annex A (grau) Steckernetzteil 2 externe UMTS Antennen
Software	Companion DVD, Dime Manager (auf DVD)	Companion DVD, Dime Manager (auf DVD)	Companion DVD, Dime Manager (auf DVD)
Dokumentation	Kurzanleitung und Sicherheitshinweise (gedruckt) Release Notes, falls erforderlich	Kurzanleitung und Sicherheitshinweise (gedruckt) Release Notes, falls erforderlich	Kurzanleitung und Sicherheitshinweise (gedruckt) Release Notes, falls erforderlich
Online-Dokumentation	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz	Benutzerhandbuch Workshops MIB-Referenz

3.2.6 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	bintec RS230a , bintec RS230aw und bintec RS230au+
Speicher	64 MB RAM, 16 MB Flash-ROM
Leistungsaufnahme Gerät	4,7 Watt
Spannungsversorgung	12 V DC 500 mA EU PSU
Umweltanforderungen:	
Lagertemperatur	-25 °C bis +70 °C
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec

Weitere Produktmerkmale

Eigenschaft	bintec RS230a	bintec RS230aw	bintec RS230au+
Maße und Gewicht:			
Gerätemaße ohne Kabel (B x H x T) mm	235 mm x 32,6 mm x 147,6 mm	235 mm x 32,6 mm x 147,6 mm	235 mm x 32,6 mm x 147,6 mm
Gewicht	ca. 1000 g	ca. 1100 g	ca. 1000 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1500 g	ca. 1600 g	ca. 1500 g
LEDs	14 (1x Power, 1x Status,	15 (1x Power, 1x Status,	15 (1x Power, 1x Status,

Eigenschaft	bintec RS230a	bintec RS230aw	bintec RS230au+
	5x2 Ethernet, 2x Funktion)	5x2 Ethernet, 3x Funktion)	5x2 Ethernet, 3x Funktion)
Verfügbare Schnittstellen:			
ADSL-Schnittstelle	Internes ADSL2+-Modem für Annex A	Internes ADSL2+-Modem für Annex A	Internes ADSL2+-Modem für Annex A
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
Ethernet	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
WLAN-Schnittstelle (Antennen)	-	802.11a/b/g/h mit Antenna Diversity; Datenraten von 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 MBit/s 802.11n; Datenrate bis 300 Mbit/s	-
UMTS/GPRS/LTE	-	-	Unterstützung von UMTS, HSPA+ (mit bis zu 21,1 Mbit/s downstream und bis zu 5,76 Mbit/s upstream), HSDPA, HSUPA, GPRS-, Edge- und GSM; UMTS/WCDMS Bänder 850/900/1900/2100 MHz, GSM/GPRS/EDGE Bänder 850/900/1800/1900 MHz
Vorhandene Buchsen:			
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse	5-polige Mini-USB-Buchse	5-polige Mini-USB-Buchse

Eigenschaft	bintec RS230a	bintec RS230aw	bintec RS230au+
Ethernet-Schnittstelle (gelb)	RJ45-Buchse	RJ45-Buchse	RJ45-Buchse
ADSL-Schnittstelle (grau)	RJ11-Buchse	RJ11-Buchse	RJ11-Buchse
USB	USB-Anschluss Typ A	USB-Anschluss Typ A	USB-Anschluss Typ A
WLAN	-	RSMA-Anschluss	
UMTS	-	-	SMA-Buchse

3.2.7 Reset

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

Gehen Sie folgendermaßen vor:

- (1) Trennen Sie Ihr Gerät vom Strom.
- (2) Drücken Sie die **Reset**-Taste Ihres Geräts.
- (3) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.
- (4) Lassen Sie nach fünfmaligem Blinken der *Status*-LED die **Reset**-Taste los.



Hinweis

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

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 41 beschrieben.

3.3 bintec RS232j, bintec RS232jw und bintec RS232j-4G

3.3.1 Aufstellen und Anschließen



Hinweis

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



Achtung

Die Verwendung eines falschen Netzgerätes kann zum Defekt Ihres Geräts führen! Verwenden Sie ausschließlich das mitgelieferte Netzgerät! Falls Sie ausländische Adapter/Netzteile benötigen, wenden Sie sich bitte an unseren bintec elmeg Service.

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



Hinweis

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

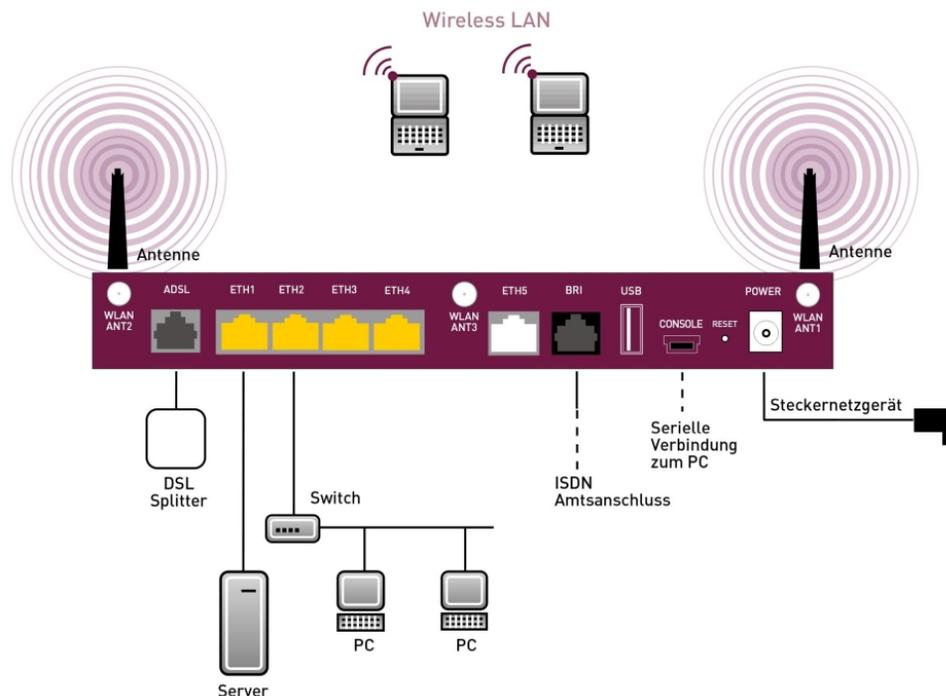


Abb. 12: Anschlussmöglichkeiten am Beispiel **bintec RS232jw**

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

- (1) Antennen

Schrauben Sie die mitgelieferten externen WLAN-Antennen (**bintec RS232jw**) auf die dafür vorgesehenen RSMA-Anschlüsse. Bei **bintec RS232j-4G** schrauben Sie die zwei UMTS/LTE-Antennen auf die SMA-Anschlüsse.
- (2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.
- (3) LAN

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

Verbinden Sie die ADSL-Schnittstelle (**ADSL**, graue Buchse) Ihres Geräts über das mitgelieferte DSL-Kabel (graues Kabel) mit dem DSL-Ausgang des Splitters.
- (5) Netzanschluss

Schließen Sie das Gerät mit das mitgelieferten Netzgerät an eine Steckdose an.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- ISDN

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

- DMZ

Verbinden Sie die WAN-Schnittstelle (**ETH**, weiße Buchse) Ihres Geräts über ein weiteres Ethernet-Kabel mit dem Ethernet-Anschluss Ihrer DMZ.

- Weitere LANs/WANs

Schließen Sie beliebige weitere Endgeräte in Ihrem Netzwerk an den verbleibenden Switch-Ports (**2, 3** oder **4**) Ihres Geräts mittels weiterer Ethernet-Kabeln an.

- Serielle Verbindung

Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs mit der seriellen Schnittstelle des Geräts (**Console**). Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen. Ein passendes Kabel ist als Zubehör erhältlich.

Das Gerät ist nun für die Konfiguration mit dem **GUI** vorbereitet. Im Kapitel [Grundkonfiguration](#) auf Seite 41 finden Sie ausführliche Schritt-für-Schritt-Anleitungen zu den grundlegenden Funktionen Ihres Geräts.

Montage

Die Geräte sind wahlweise durch Laschen im Gehäuse an die Wand, oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

Befestigen Sie die selbstklebenden Gummifüßchen an der Unterseite des Geräts. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wandmontage

Um die Geräte der **bintec RS232x**-Serie an der Wand zu montieren, benutzen Sie die Laschen an der Gehäuserückseite.



Warnung

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

Kensington Lock

Die Geräte bieten die Möglichkeit, ein Kensington Lock zu befestigen. Die dazu notwendige Aussparung finden Sie an der rechten Gehäuseseite.

3.3.2 Anschlüsse

bintec RS232j, **bintec RS232jw** und **bintec RS232j-4G** verfügen über einen 4-Port Gigabit Switch, über einen Gigabit LAN/WAN-Anschluss, eine ADSL-Schnittstelle (Annex B / J), eine BRI(S0)-Schnittstelle sowie über eine serielle Schnittstelle und einen USB-Anschluss. **bintec RS232jw** verfügt über Anschlüsse für 3 externe WLAN Antennen. **bintec RS232j-4G** verfügt über Anschlüsse für 2 externe UMTS/LTE Antennen.

Die Anschlüsse sind folgendermaßen angeordnet:

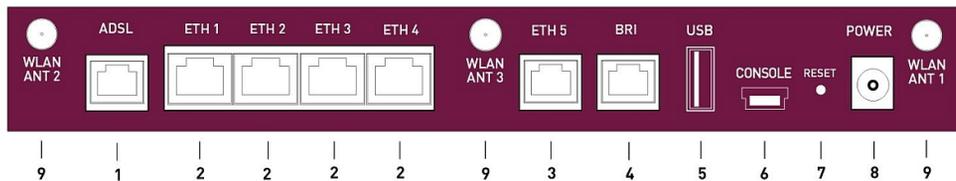


Abb. 13: **bintec RS232jw** Rückseite

Anschlüsse Rückseite

1	ADSL (grau)	ADSL2+-Schnittstelle
2	ETH1 / ETH2 / ETH3 / ETH4 (gelb)	10/100/1000 Base-T Ethernet-Schnittstelle
3	ETH5 (weiß)	10/100/1000 Base-T Ethernet-Schnittstelle
4	BRI (schwarz)	BRI-Schnittstelle
5	USB	USB-Anschluss
6	CONSOLE	Serielle Schnittstelle
7	RESET	Reset-Taste
8	POWER	Buchse für Steckernetzteil
9	WLAN ANT1 / ANT2 / ANT3	RSMA-Anschluss (nur bintec RS232jw)
ohne Abb.	UMTS MAIN/AUX	Anschlüsse für UMTS/LTE Antennen (nur bintec RS232j-4G)

3.3.3 Antennenanschlüsse

Die Geräte **bintec RS232jw** haben drei Anschlüsse für die externen WLAN-Antennen. Die Geräte **bintec RS232j-4G** haben zwei Anschlüsse für die externe UMTS/LTE-Antennen (SMA-Buchsen). Die Belegung der zwei Antennenanschlüsse können Sie den folgenden Grafiken entnehmen:



Abb. 14: Antennenbelegung der **bintec RS232j-4G**



Abb. 15: Antennenbelegung der **bintec RS232j-4G**

3.3.4 LEDs

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

Die LEDs sind folgendermaßen angeordnet:

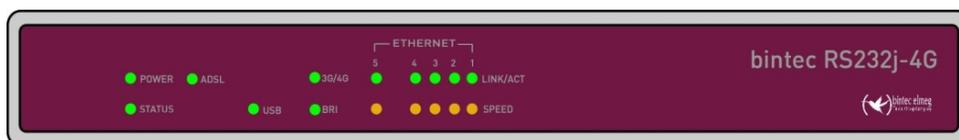


Abb. 16: Anordnung der LEDs

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	Startvorgang

LED	Farbe	Status	Information
	grün	blinkend	Normaler Betrieb
	grün	aus	Fehler
Ethernet 1 bis 4: LINK/ACT	grün	an	Die Verbindung zum LAN ist hergestellt.
	grün	blinkend	Datenverkehr über die LAN-Schnittstelle.
		aus	Kein Anschluss.
Ethernet 1 bis 4: SPEED	grün	an	Das Gerät ist an das LAN angeschlossen mit 1000 Mbit/s.
	orange	an	Das Gerät ist an das LAN angeschlossen mit 100 Mbit/s.
		aus	Das Gerät ist an das LAN angeschlossen mit 10 Mbit/s oder kein Datenverkehr.
Ethernet 5: LINK/ACT	grün	an	Die Verbindung zum WAN ist hergestellt.
	grün	blinkend	Datenverkehr über die WAN-Schnittstelle
		aus	Kein Anschluss.
Ethernet 5: SPEED	grün	an	Das Gerät ist an das WAN angeschlossen mit 1000 Mbit/s.
	orange	an	Das Gerät ist an das WAN angeschlossen mit 100 Mbit/s.
		aus	Das Gerät ist an das LAN angeschlossen mit 10 Mbit/s oder kein Datenverkehr.
ADSL	grün	an	DSL-Verbindung ist aktiv.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über die DSL-Schnittstelle.
WLAN	grün	an	Das Funkmodul ist aktiv.
		aus	Kein Anschluss zum Funkmodul.
		blinkend	Datenverkehr über die WLAN-Schnittstelle.
USB	grün	an	USB-Gerät ist verbunden.
		aus	Kein Anschluss.
		blinkend	Datenverkehr über USB-Schnittstelle.
3G/4G	grün	an	UMTS/LTE-Verbindung zum Netzwerk über das interne Modem nach erfolgreicher Einwahl.
		aus	Kein Anschluss.

LED	Farbe	Status	Information
		blinkend	Datenverkehr über das interne UMTS/LTE-Modem.
BRI	grün	an	D-Kanal ist aktiv.
		aus	Kein Anschluss.
		blinkend	Mindestens ein B-Kanal ist aktiv.

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

LED BRRP-Anzeige

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.

3.3.5 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Lieferumfang	bintec RS232j	bintec RS232jw	bintec RS232j-4G
Kabelsätze/Netzteil/Sonstiges	Ethernet-Kabel (gelb) ADSL-Kabel für Annex B / J (grau) ISDN-Kabel (schwarz) Steckernetzteil	Ethernet-Kabel (gelb) ADSL-Kabel für Annex B / J (grau) ISDN-Kabel (schwarz) Steckernetzteil 3 externe WLAN Antennen	Ethernet-Kabel (gelb) ADSL-Kabel für Annex B / J (grau) ISDN-Kabel (schwarz) Steckernetzteil 2 externe UMTS/LTE Antennen
Software	Companion DVD, Dime Manager (auf DVD)	Companion DVD, Dime Manager (auf DVD)	Companion DVD, Dime Manager (auf DVD)
Dokumentation	Kurzanleitung und Sicherheitshinweise (gedruckt) Release Notes, falls erforderlich	Kurzanleitung und Sicherheitshinweise (gedruckt) Release Notes, falls erforderlich	Kurzanleitung und Sicherheitshinweise (gedruckt) Release Notes, falls erforderlich
Online-Dokumentation	Benutzerhandbuch	Benutzerhandbuch	Benutzerhandbuch

Lieferumfang	bintec RS232j	bintec RS232jw	bintec RS232j-4G
	Workshops	Workshops	Workshops
	MIB-Referenz	MIB-Referenz	MIB-Referenz

3.3.6 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	bintec RS232j , bintec RS232jw und bintec RS232j-4G
Speicher	64 MB RAM, 16 MB Flash-ROM
Leistungsaufnahme Gerät	4,7 Watt
Spannungsversorgung	12 V DC 800 mA EU PSU
Umweltanforderungen:	
Lagertemperatur	-25 °C bis +70 °C
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET TM Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec

Weitere Produktmerkmale

Eigenschaft	bintec RS232j	bintec RS232jw	bintec RS232j-4G
Maße und Gewicht:			
Gerätemaße ohne Kabel (B x H x T)	235 mm x 32,6 mm x 147,6 mm	235 mm x 32,6 mm x 147,6 mm	235 mm x 32,6 mm x 147,6 mm
Gewicht	ca. 1000 g	ca. 1100 g	ca. 1100 g

Eigenschaft	bintec RS232j	bintec RS232jw	bintec RS232j-4G
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1500 g	ca. 1600 g	ca. 1600 g
LEDs	15 (1x Power, 1x Status, 5x2 Ethernet, 3x Funktion)	16 (1x Power, 1x Status, 5x2 Ethernet, 4x Funktion)	16 (1x Power, 1x Status, 5x2 Ethernet, 4x Funktion)
Verfügbare Schnittstellen:			
ADSL-Schnittstelle	Internes ADSL2+-Modem für Annex B / J	Internes ADSL2+-Modem für Annex B / J	Internes ADSL2+-Modem für Annex B / J
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
Ethernet	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
ISDN BRI (S0)	Fest eingebaut, nur TE-Modus	Fest eingebaut, nur TE-Modus	Fest eingebaut, nur TE-Modus
WLAN-Schnittstelle (Antennen)	-	802.11a/b/g/h mit Antenna Diversity; Datenraten von 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 MBit/s 802.11n; Datenrate bis 300 Mbit/s	-
UMTS/GPRS/LTE	-	-	Unterstützung von UMTS, HSPA+ (mit bis zu 21,1 Mbit/s downstream und bis zu 5,76 Mbit/s upstream), HSDPA, HSUPA, GPRS-, Edge- und GSM; UMTS/WCDMS Bänder 850/900/1900/2100 MHz, GSM/GPRS/EDGE Bänder

Eigenschaft	bintec RS232j	bintec RS232jw	bintec RS232j-4G
			der 850/900/1800/1900 MHz LTE Bänder 800/900/1800/2100/2600 MHz
Vorhandene Buchsen:			
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse	5-polige Mini-USB-Buchse	5-polige Mini-USB-Buchse
Ethernet-Schnittstelle (gelb)	RJ45-Buchse	RJ45-Buchse	RJ45-Buchse
ISDN BRI-Schnittstelle (schwarz)	RJ45-Buchse	RJ45-Buchse	RJ45-Buchse
ADSL-Schnittstelle (grau)	RJ11-Buchse	RJ11-Buchse	RJ11-Buchse
USB	USB-Anschluss Typ A	USB-Anschluss Typ A	USB-Anschluss Typ A
WLAN	-	RSMA-Anschluss	-
UMTS	-	-	SMA-Buchse

3.3.7 Reset

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

Gehen Sie folgendermaßen vor:

- (1) Trennen Sie Ihr Gerät vom Strom.
- (2) Drücken Sie die **Reset**-Taste Ihres Geräts.
- (3) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.
- (4) Lassen Sie nach fünfmaligem Blinken der *Status*-LED die **Reset**-Taste los.



Hinweis

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

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 41 beschrieben.

3.4 Reinigen

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

3.5 Pin-Belegungen

3.5.1 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. 17: 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

3.5.2 Ethernet-Schnittstelle

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

Der Anschluss erfolgt über eine RJ45-Buchse (gelb). Die Geräte verfügen weiterhin über eine fünfte Ethernet-Schnittstelle (weiß).

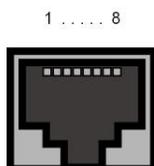


Abb. 18: 10/100/1000 Base-T Ethernet-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für LAN-Anschluss

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

3.5.3 ADSL-Schnittstelle

bintec RS230a und **bintec RS230aw**, **bintec RS230au+** sowie **bintec RS232j**, **bintec RS232jw** und **bintec RS232j-4G** verfügen über eine ADSL-Schnittstelle (grau).

Die ADSL-Schnittstelle wird mittels eines RJ11-Steckers angebunden.

Für Annex A (**bintec RS230a**, **bintec RS230aw** und **bintec RS230au+** wird zum Anschluss ein Kabel mit RJ11-Stecker für den Geräteanschluss und RJ11-Stecker für den Anschluss an den ADSL-Splitter benötigt. (Kabel im Lieferumfang enthalten.)

Für Annex B / J (**bintec RS232j** , **bintec RS232jw** und **bintec RS232j-4G**) wird zum Anschluss ein Kabel mit RJ11-Stecker für den Geräteanschluss und RJ45-Stecker für den Anschluss an den ADSL-Splitter benötigt. (Kabel im Lieferumfang enthalten.)

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

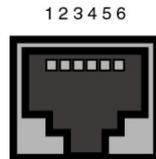


Abb. 19: ADSL-Schnittstelle (RJ11)

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

RJ11-Buchse für ADSL-Anschluss

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

3.5.4 ISDN-S0-Schnittstelle

bintec RS232j , **bintec RS232jw** und **bintec RS232j-4G** verfügen über eine zusätzliche ISDN-BRI(S0)-Schnittstelle, die z. B. für Backup-Funktionen genutzt werden kann.

Der Anschluss erfolgt über eine RJ45-Buchse (schwarz).

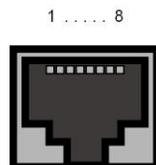


Abb. 20: ISDN-S0 -BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.5.5 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. 21: 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

3.6 SIM-Karte einsetzen

Das Gerät **bintec RS120wu** ist mit einem Kartenschacht für eine SIM-Karte ausgerüstet.

Gehen Sie für das Einsetzen der SIM-Karte wie folgt vor:

- Schrauben Sie auf der Rückseite des Geräts die mittlere Schraube ab und nehmen Sie den Gehäusedeckel nach oben ab.
- Öffnen Sie den Kartenschacht. Schieben Sie dazu den Kartenverschluss in Pfeilrichtung

↓ und heben Sie den Kartenschacht leicht an.

- Stellen Sie sicher, dass die Kontakte der SIM-Karte nach unten zeigen.
- Schieben Sie die SIM-Karte in den Kartenschacht, so dass sich die abgeschrägte Ecke der Karte oben links befindet.
- Schließen Sie den Kartenschacht. Drücken Sie dazu den Kartenschacht wieder nach unten.
- Schieben Sie den Kartenverschluss in Pfeilrichtung ↑. Sie hören ein Klickgeräusch, wenn die Karte einrastet.

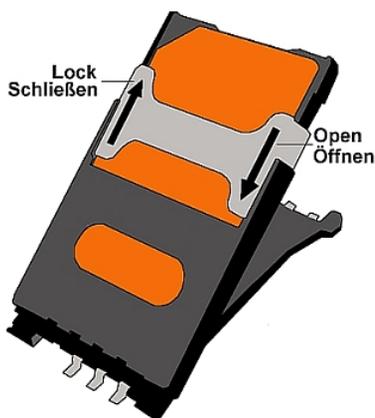


Abb. 22: SIM-Karte

3.7 Support Information

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

Internationale Supportkoordinati- Telefon: +49 911 9673 0
on

Fax: +49 911 688 0725

Endkunden-Hotline

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

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

3.8 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 4 Grundkonfiguration

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

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

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

4.1 Voreinstellungen

4.1.1 IP-Konfiguration

Ihr Gerät wird mit einer vordefinierten IP-Konfiguration ausgeliefert:

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

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

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



Hinweis

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

Die Vorgehensweise bei der Änderung von Passwörtern finden Sie unter [Systempasswort ändern](#) auf Seite 47.

Darüber hinaus ist das Gerät werksseitig als DHCP-Server eingerichtet, es übermittelt also

PCs in Ihrem LAN, die über keine IP-Konfiguration verfügen, alle für eine Verbindung notwendigen Einstellungen. Wie Sie Ihren PC für den automatischen Bezug einer IP-Konfiguration einrichten, ist in [PC einrichten](#) auf Seite 46 beschrieben.



Hinweis

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

Folgende Einstellungen werden an einen unkonfigurierten PC übertragen:

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

4.1.2 Software-Update

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

Eine Beschreibung des Update-Vorgangs finden Sie in [Softwareaktualisierung](#) auf Seite 50.

4.2 System-Voraussetzungen

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

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

4.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

- die benötigten Daten für die Grundkonfiguration und den Internet-Anschluss bereitlegen sowie ggf. die nötigen Daten für die Anbindung der gewünschten WLAN-Clients sammeln.
- überprüfen, ob der PC, von dem aus Sie die Konfiguration vornehmen wollen, die notwendigen Voraussetzungen erfüllt.

Darüber hinaus können Sie ...

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

4.3.1 Daten sammeln

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

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

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

- Grundkonfiguration (obligatorisch sofern sich Ihr Gerät im Auslieferungszustand befindet)
- Internetzugang (optional)
- Wireless LAN (optional, nur für **bintec RS120wu** , **bintec RS230aw** und **bintec RS232jw**).

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

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

Grundkonfiguration

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

Basisinformationen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	<i>192.168.0.254</i>	
Netzmaske Ihres Gateways	<i>255.255.255.0</i>	

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	<i>GoInternet</i>	
Protokoll	<i>PPP over Ethernet (PPPoE)</i>	
Enkapsulierung	<i>bridged-no-fcs</i>	
VPI (Virtual Path Identifier)	<i>1</i>	
VCI (Virtual Circuit Identifier)	<i>32</i>	
Ihr Benutzername	<i>MyName</i>	
Passwort	<i>TopSecret</i>	

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

Zusätzliche Informationen für T-Online

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



Hinweis

Geben Sie bei der Konfiguration eines T-Online-Internetzugangs in das Feld **Benutzername** nacheinander und ohne Leerzeichen folgende Nummern ein: Anschlusskennung (12-stellig) + T-Online Nummer (meist 12-stellig) + Mitbenutzernummer (für den Hauptnutzer immer 0001). Sollte Ihre T-Online Nummer weniger als 12 Stellen enthalten, muss zwischen der T-Online Nummer und der Mitbenutzernummer das Zeichen "#" stehen. Wenn Sie T-DSL nutzen, müssen Sie dieser Zahlenfolge noch die Endung "@t-online.de" hinzufügen. Ihr Benutzername könnte dann so aussehen:
00012345678906112345678#0001@t-online.de

Internetzugang über UMTS/LTE

In der nachfolgenden Tabelle sind die Zugangsdaten zusammengestellt, die Sie für eine Internet-Verbindung über UMTS/LTE benötigen:

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>	

Wireless LAN (nur bintec RS120wu , bintec RS230aw und bintec RS232jw)

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

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

Beachten Sie dazu Folgendes:

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

Daten für die Wireless LAN Konfiguration

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

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

- (1) Klicken Sie im Startmenü auf **Einstellungen -> Systemsteuerung -> Netzwerkverbindungen** (Windows XP) bzw. **Systemsteuerung -> Netzwerk- und Freigabecenter -> Adaptereinstellungen ändern** (Windows 7).
- (2) Klicken Sie auf **LAN-Verbindung**.
- (3) Klicken Sie im Statusfenster auf **Eigenschaften**.
- (4) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
- (5) Wählen Sie **IP-Adresse automatisch beziehen**.
- (6) Wählen Sie ebenfalls **DNS-Serveradresse automatisch beziehen**.

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



Hinweis

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

4.3.3 Systempasswort ändern

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

Gehen Sie dazu vor wie folgt:

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

Beachten Sie folgende Regeln zum Passwortgebrauch:

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

4.4 Internetverbindung einrichten

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

4.4.1 Internetverbindung über das interne ADSL-Modem

Bis auf **bintec RS120wu** und **bintec RS120** verfügen alle Geräte der **RS-Serie** über ein integriertes ADSL2+-Modem zum Aufbau einer schnellen Internetverbindung. Zur einfachen Konfiguration eines ADSL-Internetzugangs verfügt das **GUI** über einen Assistenten, mit dem Sie die Verbindung unkompliziert und schnell einrichten können. Eine Auswahl an vor-konfigurierten Zugängen der wichtigsten Anbieter (T-Home, Arcor) vereinfacht die Konfiguration noch einmal.

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

4.4.2 Internetverbindung über UMTS/LTE

Der Aufbau einer Internetverbindung (nur für **bintec RS120wu**, **bintec RS230au+** und **bintec RS232j-4G**) über UMTS/LTE erfordert eine aktivierte SIM-Karte Ihres UMTS/LTE-Anbieters. Setzen Sie die Karte wie in [SIM-Karte einsetzen](#) auf Seite 38 beschrieben ein.

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

4.4.3 Andere Internetverbindungen

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

4.4.4 Konfiguration prüfen

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

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

- (1) Testen Sie die Verbindung von einem beliebigen Gerät im lokalen Netzwerk zum Gerät. Klicken Sie im Windows-Startmenü auf **Ausführen** und geben Sie `ping` gefolgt

von einem Leerzeichen und der IP-Adresse Ihres Geräts ein (z. B. *192.168.0.254*). Es erscheint ein Fenster mit dem Hinweis "Antwort von...".

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



Hinweis

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

4.5 Wireless LAN einrichten

Gehen Sie folgendermaßen vor, um ihr Gerät (nur **bintec RS120wu** , **bintec RS230aw** und **bintec RS232jw**) als Access Point zu nutzen:

- (1) Gehen Sie im **GUI** in das Menü **Assistenten->Wireless LAN**.
- (2) Folgen Sie den Schritten, die der Assistent vorgibt. Der Assistent verfügt über eine eigene Online-Hilfe, die Ihnen ggf. notwendige Informationen vermittelt.
- (3) Speichern Sie die Konfiguration mit dem Button **Konfiguration speichern** oberhalb der Menünavigation.

WLAN-Adapter unter Windows XP konfigurieren

Windows XP hat nach der Installation der Treiber für Ihre WLAN-Karte eine neue Verbindung in der Netzwerkumgebung eingerichtet. Um diese Wireless-LAN-Verbindung zu konfigurieren, gehen Sie bitte folgendermaßen vor:

- (1) Klicken Sie auf **Start-> Systemsteuerung**. Dort doppelklicken Sie auf **Netzwerkverbindungen -> Drahtlose Netzwerkverbindung**.
- (2) Wählen Sie anschließend auf der linken Seite **Erweiterte Einstellungen ändern** aus.
- (3) Gehen Sie auf die Registerkarte **Drahtlosnetzwerke**.
- (4) Klicken Sie auf **Hinzufügen**.

Fahren Sie folgendermaßen fort:

- (1) Bei **Netzwerkname** geben Sie z. B. *Client-1* ein.
- (2) Unter **Netzwerkauthentifizierung** wählen Sie *WPA2-PSK*.
- (3) Bei **Datenverschlüsselung** konfigurieren Sie *AES*.

- (4) Unter **Netzwerkschlüssel** und **Netzwerkschlüssel bestätigen** geben Sie den zuvor konfigurierten Preshared Key an.
- (5) Verlassen Sie die Menüs jeweils mit **OK**.



Hinweis

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

4.6 Softwareaktualisierung

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

Gehen Sie folgendermaßen vor:

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

Optionen

Aktuell Installierte Software	
BOSS	V.9.1 Rev. 7 IPSec from 2013/08/01 00:00:00
Systemlogik	0.0
Optionen zu Software und Konfiguration	
Aktion	Systemsoftware aktualisieren ▾
Quelle	Aktuelle Software vom Update-Server ▾

Los

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

**Achtung**

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

Kapitel 5 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

5.1 Zugangsmöglichkeiten

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

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

- Über Ihr LAN
- Über die serielle Schnittstelle
- Über eine ISDN-Verbindung (nur **bintec RS232j** , **bintec RS232jw** und **bintec RS232j-4G**)

5.1.1 Zugang über LAN

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



Achtung

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

5.1.1.1 HTTP/HTTPS

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

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

5.1.1.2 Telnet

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

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

Gehen Sie folgendermaßen vor:

Windows

- (1) Klicken Sie im Windows-Startmenü auf **Ausführen...**
- (2) Geben Sie `telnet <IP-Adresse Ihres Geräts>` ein.
- (3) Klicken Sie auf **OK**.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (4) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 59.

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 59.

5.1.1.3 SSH

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

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

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

Schlüssel zur Verschlüsselung

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

- (1) Loggen Sie sich auf eine der bereits verfügbaren Arten auf Ihrem Gerät ein (z. B. über Telnet - zum Login siehe [Anmelden](#) auf Seite 58).
- (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 62).
- (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 58 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 58 fort.



Hinweis

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

5.1.2 Zugang über die serielle Schnittstelle

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

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

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

Windows

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

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

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

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

Überprüfen

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

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

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

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

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

Unix

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

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

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

5.1.3 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 59.

5.2 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.

5.2.1 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 im Setup Tool nicht im Klartext, sondern nur als Sternchen am Bildschirm sichtbar. Die Benutzernamen erscheinen hingegen im Klartext.

Ein Sicherheitskonzept Ihres Geräts besteht darin, dass Sie mit dem Benutzernamen `read`

alle anderen Konfigurationseinstellungen lesen können, nicht aber die Zugangsdaten. Es ist also nicht möglich, sich mit `read` einzuloggen, das Passwort des Benutzers `admin` auszulesen und sich dann anschließend mit `admin` einzuloggen, um Konfigurationsänderungen vorzunehmen.



Achtung

Alle bintec elmeg-Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Sie sind daher nicht gegen einen unautorisierten Zugriff geschützt, solange die Passwörter nicht geändert werden. Die Vorgehensweise bei der Änderung von Passwörtern ist unter *Passwörter* auf Seite 80 beschrieben.

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

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

5.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in *Zugangsmöglichkeiten* auf Seite 52 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. `rs232jw:>`. Das Einloggen war erfolgreich. Sie befinden sich auf der SNMP-Shell.

Um die SNMP-Shell nach Beenden der Konfiguration zu verlassen, geben Sie `exit` ein

und bestätigen mit der **Eingabetaste**.

5.3 Konfigurationsmöglichkeiten

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

Sie haben folgende Möglichkeiten, Ihr Gerät zu konfigurieren:

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



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.

5.3.1 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 auf www.bintec-elmeg.com heruntergeladen und auf dem Gerät installiert werden. Gehen Sie hierzu vor wie in *Optionen* auf Seite 494 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	300	Sekunden	Übernehmen
! Warnung: Systempasswort nicht geändert!			
Systeminformationen			
Uptime	10 Tag(e) 22 Stunde(n) 42 Minute(n)		
Systemdatum	Donnerstag, 13 Apr 2000, 05:21:41		
Seriennummer	SR6AAA009400008		
BOSS-Version	V.9.1 Rev. 7 IPSec from 2013/08/01 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: **GUI** Startseite

5.3.1.1 Das GUI aufrufen

- (1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind (siehe auf Seite).
- (2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe *PC einrichten* auf Seite 46).
- (3) Öffnen Sie einen Webbrowser.
- (4) Geben Sie `http://192.168.0.254` in das Adressfeld des Webbrowsers ein.
- (5) Geben Sie in das Feld **User** `admin` und in das Feld **Password** `admin` ein und klicken Sie auf **LOGIN**.

Sie befinden sich nun im Statusmenü des **GUI** Ihres Geräts (siehe *Status* auf Seite 74).

5.3.1.2 Bedienelemente

GUI Fenster

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

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

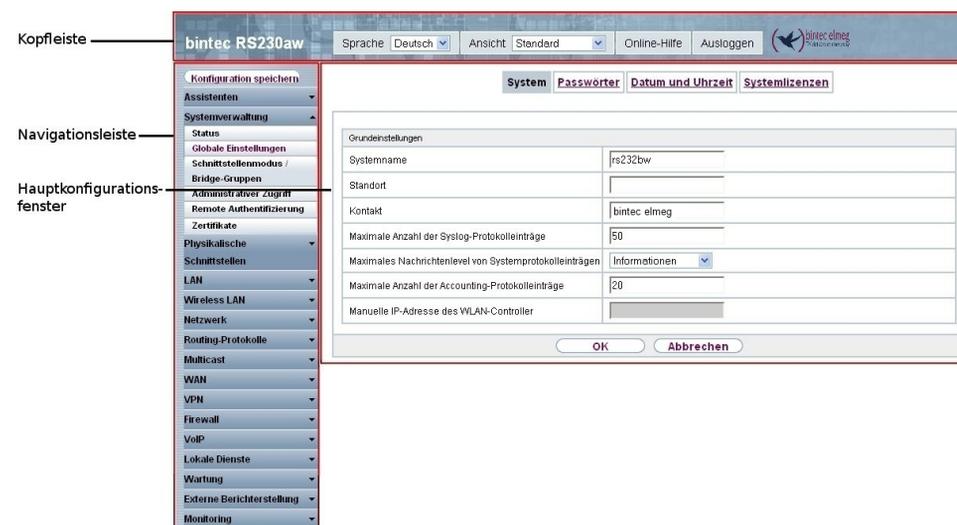


Abb. 25: Bereiche des **GUI**

Kopfleiste



Abb. 26: GUI Kopfleiste

GUI Kopfleiste

Menü	Funktion
Sprache <input type="text" value="Deutsch"/>	Sprache: Wählen Sie in dem Dropdown-Menü die gewünschte Sprache aus, in der das GUI angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen Deutsch und Englisch.
Ansicht <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. 27: Konfiguration speichern Schaltfläche



Abb. 28: Menüs

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

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

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

Sie haben folgende zwei Wahlmöglichkeiten:

- *Konfiguration speichern*, d.h. aktuelle Konfiguration als Boot-Konfiguration speichern
- *Konfiguration speichern und vorhergehende Boot-Konfiguration sichern.*, d.h. aktuelle Konfiguration als Boot-Konfiguration speichern und zusätzlich 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**, wählen Sie **Aktion = Konfiguration importieren** und klicken Sie auf **Los**. Das archivierte Backup wird als aktuelle Boot-Konfiguration verwendet.

Die Navigationsleiste enthält weiterhin die Hauptkonfigurationsmenüs und deren Untermenüs.

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

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

Statusseite

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

Hauptkonfigurationsfenster

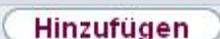
Die Untermenüs enthalten im Allgemeinen mehrere Seiten. Diese werden über die im Hauptfenster oben stehenden Schalter aufgerufen. Durch Klicken auf einen Schalter öffnet sich das Fenster mit den Basis-Parametern, welches durch Klicken auf den Reiter **Erweiterte Einstellungen** erweiterbar ist und dann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

Konfigurationselemente

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

GUI Schaltflächen

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

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

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 ei-

Symbol	Funktion
	ner Verbindung.
	Kennzeichnet den Status "Aktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Inaktiv" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Blockiert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet den Status "Wird aktiviert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet, dass der Datenverkehr verschlüsselt wird.
	Löst einen WLAN-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.

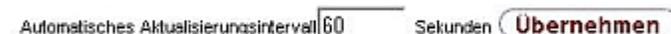


Abb. 29: Konfiguration des Aktualisierungsintervalls



Abb. 30: 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
	 Textfeld mit verdeckter Eingabe  Geben Sie entsprechende Daten ein.
Radiobuttons	z. B.  Wählen Sie die entsprechende Option aus.
Checkboxes	z. B. Aktivieren durch Auswahl der Checkbox  Auswahl verschiedener möglicher Optionen 
Dropdown-Menüs	z. B.  Klicken Sie auf den Pfeil, um die Liste zu öffnen. Wählen Sie die gewünschte Option mit der Maus.
Interne Listen	z. B.  Klicken Sie auf die Schaltfläche Hinzufügen . Ein neuer Listeneintrag wird angelegt. Geben Sie die entsprechenden Daten ein. Bleiben die Felder des Listeneintrags leer, wird dieser bei Bestätigen mit OK nicht gespeichert. Löschen Sie Einträge, indem Sie auf das  -Symbol klicken.

Darstellung von Optionen, die nicht zur Verfügung stehen

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



Wichtig

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

Warnsymbole

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

Achten Sie besonders auf folgenden Hinweis:

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

5.3.1.3 GUI Menüs

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



Hinweis

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

SNMP-Browser

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

SNMP (Simple Network Management Protocol) ist ein Protokoll, das den Zugriff für die Konfiguration Ihres Geräts ermöglicht. Alle Konfigurationsparameter werden in der sog. MIB (Management Information Base) in Form von MIB-Tabellen und MIB-Variablen gespei-

chert. Diese können Sie über den SNMP-Browser direkt lesen und verändern.



Achtung

Diese Konfigurationsmethode setzt vertiefte Systemkenntnisse über bintec-Geräte voraus!

5.3.2 SNMP Shell

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

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

5.4 BOOTmonitor

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

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

- (1) Boot System (Neustart des Systems):
Das Gerät lädt die komprimierte Boot-Datei vom Flash-Speicher in den Arbeitsspeicher. Dies wird beim Hochfahren automatisch ausgeführt.
- (2) Software Update via TFTP (Softwareaktualisierung über TFTP):
Das Gerät führt ein Software-Update über einen TFTP-Server aus.
- (3) Software Update via XMODEM (Softwareaktualisierung über XMODEM):
Das Gerät führt ein Software-Update über eine serielle Schnittstelle mit XMODEM aus.
- (4) Delete configuration (Konfiguration löschen):
Das Gerät wird in den Auslieferungszustand zurückversetzt. Alle Konfigurationsdateien werden gelöscht, die BOOTmonitor-Einstellungen werden auf die Standardwerte gesetzt.
- (5) Default BOOTmonitor Parameters (Standardeinstellungen des BOOTmonitors):
Sie können die Standard-Einstellungen des BOOTmonitors des Geräts verändern, z. B. die Baudrate für serielle Verbindungen.
- (6) Show System Information (Systeminformationen anzeigen):

Zeigt nützliche Informationen des Geräts, wie z. B. 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
```

```
RS232bw Bootmonitor V.7.9 Rev.1 from 2009/10/19 00:00:00  
Copyright (c) 1996-2005 by bintec elmeg 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 6 Assistenten

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

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

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

Kapitel 7 Systemverwaltung

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

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

7.1 Status

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

Sie erhalten einen Überblick über folgende Daten:

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

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



Achtung

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

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. 7 IPSec from 2013/08/01 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. 32: 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 Systemssoftware an.
Letzte gespeicherte Konfiguration	Zeigt Tag, Datum und Uhrzeit der letzten Konfigurationsspeicherung (Boot-Konfiguration im Flash) an.

Felder im Menü Ressourceninformationen

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

Felder im Menü Physikalische Schnittstellen

Feld	Wert
Schnittstelle - Verbindungsinformation - Link	<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>Verbindungsinformation für Ethernet-Schnittstellen:</p> <ul style="list-style-type: none"> • IP-Adresse • Netzmaske <p>Verbindungsinformation für ISDN-Schnittstellen:</p> <ul style="list-style-type: none"> • Konfiguriert • Nicht konfiguriert <p>Verbindungsinformation für xDSL-Schnittstellen:</p> <ul style="list-style-type: none"> • Leitungsgeschwindigkeit Downstream/Upstream <p>Verbindungsinformation für WLAN-Schnittstellen:</p> <p>Access-Point-Modus:</p> <ul style="list-style-type: none"> • Betriebsmodus: Access Point oder Aus

Feld	Wert
	<ul style="list-style-type: none"> • Der auf diesem Funkmodul verwendete Kanal • Anzahl der verbundenen Clients • Anzahl der WDS-Links • Softwareversion der Funkkarte <p>Verbindungsinformation für UMTS/LTE-Schnittstellen:</p> <ul style="list-style-type: none"> • <i>SIM einlegen erforderlich</i> wird angezeigt, wenn keine SIM-Karte gesteckt ist. • <i>PIN Eingabe erforderlich</i> wird angezeigt, wenn die SIM-Karte gesteckt, aber die PIN noch nicht eingegeben ist. • <i>Init</i> wird angezeigt, wenn die SIM-Karte initialisiert wird. • Wenn die SIM-Karte in Betrieb ist, wird die Netzwerkqualität angezeigt.

Felder im Menü WAN-Schnittstellen

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

7.2 Globale Einstellungen

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

7.2.1 System

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

System		Passwörter	Datum und Uhrzeit	Systemlizenzen
Grundeinstellungen				
Systemname	<input type="text" value="Produktname"/>			
Standort	<input type="text"/>			
Kontakt	<input type="text" value="bintec elmeg"/>			
Maximale Anzahl der Syslog-Protokolleinträge	<input type="text" value="50"/>			
Maximales Nachrichtenlevel von Systemprotokolleinträgen	Informationen ▾			
Maximale Anzahl der Accounting-Protokolleinträge	<input type="text" value="20"/>			
Manuelle IP-Adresse des WLAN-Controller	<input type="text"/>			
LED-Modus	Status ▾			
Energieeinstellungen				
Zeit bis zum Abschalten	<input type="text" value="900"/>	Sekunden		
<input type="button" value="OK"/>		<input type="button" value="Abbrechen"/>		

Abb. 33: Systemverwaltung ->Globale Einstellungen->System

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

Felder im Menü Grundeinstellungen

Feld	Wert
Systemname	Geben Sie den Systemnamen Ihres Geräts ein. Dieser wird auch als PPP-Host-Name benutzt. Möglich ist eine Zeichenkette mit maximal 255 Zeichen. Als Standardwert ist der Gerätetyp voreingestellt.
Standort	Geben Sie an, wo sich Ihr Gerät befindet.
Kontakt	Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden. Möglich ist eine Zeichenkette mit maximal 255 Zeichen. Standardwert ist <i>bintec elmeg</i> .
Maximale Anzahl der Syslog-Protokolleinträge	Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen. Mögliche Werte sind 0 bis 1000.

Feld	Wert
	<p>Standardwert ist <i>50</i>.</p> <p>Sie können die gespeicherten Meldungen in Monitoring->Internes Protokoll anzeigen lassen.</p>
<p>Maximales Nachrichtenlevel von Systemprotokolleinträgen</p>	<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. • <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.
<p>Maximale Anzahl der Accounting-Protokolleinträge</p>	<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 <i>0</i> bis <i>1000</i>.</p> <p>Standardwert ist <i>20</i>.</p>
<p>Manuelle IP-Adresse des WLAN-Controller</p>	<p>Diese Funktion ist nur bei Geräten mit Wireless LAN Controller</p>

Feld	Wert
	<p>verfügbar.</p> <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>
LED-Modus	<p>Diese Funktion ist nur für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n verfügbar.</p> <p>Wählen Sie das Leuchtverhalten der 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.

Felder im Menü Energieeinstellungen (nur für Geräte mit GPS)

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

7.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

[System](#) | [Passwörter](#) | [Datum und Uhrzeit](#) | [Systemlizenzen](#)

Systempasswort	
Systemadministrator-Passwort	••••••
Systemadministrator-Passwort bestätigen	••••••
SNMP-Communities	
SNMP Read Community	••••••
SNMP Write Community	••••••
Globale Passwortoptionen	
Passwörter und Schlüssel als Klartext anzeigen	Anzeigen

|

Abb. 34: Systemverwaltung ->Globale Einstellungen->Passwörter



Hinweis

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

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

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

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

Felder im Menü Systempasswort

Feld	Wert
Systemadministrator-Passwort	Geben Sie das Passwort für den Benutzernamen <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.

Feld	Wert
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	<p>Wählen Sie aus, ob die Passwörter im Klartext angezeigt werden sollen.</p> <p>Mit <i>Anzeigen</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn Sie die Funktion aktivieren, werden alle Passwörter und Schlüssel in allen Menüs als Klartext angezeigt und können in Klartext bearbeitet werden.</p> <p>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.</p>

7.2.3 Datum und Uhrzeit

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

System		Passwörter		Datum und Uhrzeit		Systemlizenzen	
Grundeinstellungen							
Zeitzone	Europe/Berlin						
Aktuelle Ortszeit	Dienstag, 22 Okt 2013, 13:29:50						
Manuelle Zeiteinstellung							
Datum einstellen	Tag	Monat	Jahr				
Zeit einstellen	Stunde	Minute					
Automatische Zeiteinstellung (Zeitprotokoll)							
Erster Zeitserver		SNTP					
Zweiter Zeitserver		SNTP					
Dritter Zeitserver		SNTP					
Zeitaktualisierungsintervall	1440	Minute(n)					
Zeitaktualisierungsrichtlinie	Normal						
System als Zeitserver	<input type="checkbox"/> Aktiviert						
Zeiteinstellungen (GPS)							
Zeitaktualisierungsintervall	<input type="checkbox"/> Aktiviert						
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

Abb. 35: Systemverwaltung ->Globale Einstellungen->Datum und Uhrzeit

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

ISDN/Manuell

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

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

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

Zeitserver

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



Hinweis

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Zeitzone	Wählen Sie die Zeitzone aus, in der Ihr Gerät installiert ist. Möglich ist die Auswahl der Universal Time Coordinated (UTC) plus oder minus der Abweichung davon in Stunden oder ein vordefinierter Ort, z. B. <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	Geben Sie ein neues Datum ein. Format: <ul style="list-style-type: none"> • Tag: dd • Monat: mm • Jahr: yyyy
Zeit einstellen	Geben Sie eine neue Uhrzeit ein.

Feld	Beschreibung
	Format: <ul style="list-style-type: none"> • Stunde: hh • Minute: mm

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	<p>Nur für Geräte mit ISDN-Schnittstelle.</p> <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 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.
Zweiter Zeitserver	<p>Geben Sie den zweiten Zeitserver an, entweder mit Domännennamen oder IP-Adresse.</p>

Feld	Beschreibung
	<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 Domännennamen oder 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.
Zeitaktualisierungsintervall	<p>Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird.</p> <p>Der Standardwert ist <i>1440</i>.</p>
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 Minu-

Feld	Beschreibung
	<p>ten versucht, den Zeitserver zu erreichen.</p> <ul style="list-style-type: none"> • <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>

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

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

7.2.4 Systemlizenzen

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

Es sind generell folgende Lizenztypen zu unterscheiden:

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

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

Lizenzdaten eintragen

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

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

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

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

Mögliche Werte für Status

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

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



Hinweis

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

7.2.4.1 Bearbeiten oder Neu

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

Abb. 36: **Systemverwaltung -> Globale Einstellungen -> Systemlizenzen -> Neu**

Freischalten von Zusatzlizenzen

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

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

Felder im Menü Grundeinstellungen

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



Hinweis

Wenn als Status *Nicht OK* angezeigt wird:

- Geben Sie die Lizenzdaten erneut ein.

- Überprüfen Sie gegebenenfalls Ihre Hardware-Seriennummer.

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

Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

- (1) Gehen Sie zu **Systemverwaltung->Globale Einstellungen->Systemlizenzen->Neu**.
- (2) Betätigen Sie das -Symbol in der Zeile, in der die zu löschende Lizenz steht.
- (3) Bestätigen Sie mit **OK**.

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

7.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

Mit Bridging werden gleichartige Netze verbunden. Im Gegensatz zum Routern arbeiten Bridges auf Schicht 2 (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 Schicht 3 (Netzwerkschicht) des OSI-Modells verbunden und Informationen von einem Netz in das andere weitergeleitet (routen).

Konventionen für die Port-/Schnittstellennamen

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

- (a) WLAN
- (b) Nummer des physischen Ports (1 oder 2)

Beispiel: *WLAN1*

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

- (a) ETH
- (b) Nummer des Ports

Beispiel: *ETH1*

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

- (a) Abkürzung für den Schnittstellentyp, dabei steht *en* für Ethernet
- (b) Nummer des Ethernet-Ports
- (c) Nummer der Schnittstelle

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

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

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

Beispiel: *br0* (erste Bridge-Gruppe)

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

- (a) Abkürzung für den Schnittstellentyp, dabei steht *vss* für Drahtlosnetzwerk
- (b) Nummer des Funkmoduls
- (c) Nummer der Schnittstelle

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

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

- (a) Abkürzung für den Schnittstellentyp
- (b) Nummer des Funkmoduls, auf dem der WDS-Link bzw. Bridge-Link konfiguriert ist
- (c) Nummer des WDS-Links bzw. Bridge-Link

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

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

- (a) Abkürzung für den Schnittstellentyp
- (b) Nummer des Funkmoduls, auf dem der Client-Link konfiguriert ist
- (c) Nummer des Client-Links

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

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

- (a) Abkürzung für den Schnittstellentyp
- (b) Nummer des Ethernet-Ports
- (c) Nummer der Schnittstelle, die an den Ethernet-Port gebunden ist
- (d) Nummer der virtuellen Schnittstelle

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

7.3.1 Schnittstellen

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

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

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

Schnittstellen

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

Konfigurationsschnittstelle

Abb. 37: Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen

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

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschrei-	Zeigt den Namen der Schnittstelle an.

Feld	Beschreibung
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</i> , <i>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	Wählen Sie aus, über welche Schnittstelle die Konfiguration durchgeführt wird. Mögliche Werte: <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.

7.3.1.1 Hinzufügen

Hinzufügen

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

Schnittstellen

Schnittstelle
Eine auswählen ▾

OK
Abbrechen

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

Das Menü **Systemverwaltung ->Schnittstellenmodus /**

->**Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

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

Bearbeiten für Geräte der Wlxxxxn und RS-Serie

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

Schnittstellen

Layer 2.5-Optionen	
Schnittstelle	sta1-0
Wildcard-Modus	letzte <input type="button" value="v"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

- (1) Wählen Sie das **GUI Menü Wireless LAN->WLAN->Einstellungen Funkmodul** und klicken Sie auf das Symbol zur Änderung eines Eintrags.
- (2) Wählen Sie **Betriebsmodus = Access Client** und speichern Sie die Einstellungen mit **OK**.
- (3) Wählen Sie das Menü **Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen**. Die zusätzliche Schnittstelle **sta1-0** wird angezeigt.
- (4) Wählen Sie für die Schnittstelle **sta1-0** Modus / Bridge-Gruppe = *br0* (*<IPAdresse>*) sowie **Konfigurationsschnittstelle = en1-0** und speichern Sie die Einstellungen mit **OK**.
- (5) Klicken Sie auf die Schaltfläche **Konfiguration speichern**, um alle Konfigurationseinstellungen zu speichern. Sie können die MAC-Bridge verwenden.

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

Felder im Menü Layer 2.5-Optionen

Feld	Wert
Schnittstelle	Zeigt die Schnittstelle an, die gerade bearbeitet wird.
Wildcard-Modus	<p>Wählen Sie aus, welchen Wildcard-Modus Sie auf der Schnittstelle nutzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird kein Wildcard-Modus verwendet. • <i>statisch</i>: Mit dieser Einstellung müssen Sie bei Wildcard-MAC-Adresse die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist. Jedes Paket ohne IP und ohne ARP wird an dieses Gerät weitergereicht. Dieses Vorgehen wird auch dann beibehalten, wenn das entsprechende Gerät nicht mehr angeschlossen ist. • <i>zuerst</i>: Mit dieser Einstellung wird die MAC-Adresse des ersten Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame, der an irgendeiner der Ethernet-Schnittstellen ankommt, als Wildcard-MAC-Adresse benutzt. Diese Wildcard-MAC-Adresse kann nur durch einen Neustart des Geräts oder die Auswahl eines anderen Wildcard-Modus zurückgesetzt werden. • <i>letzte</i>: Mit dieser Einstellung wird die eigene WLAN-MAC-Adresse benutzt, um die Verbindung zum Access Point herzustellen. Sobald ein Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame auftaucht, wird er an diejenige MAC-Adresse weitergeleitet, von welcher der letzte Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame bei einer Ethernet-Schnittstelle des Geräts eingetroffen ist. Diese Wildcard-MAC-Adresse wird mit jedem Nicht-IP-Unicast-Frame bzw Nicht-ARP-Unicast-Frame erneuert.
Wildcard-MAC-Adresse	<p>Nur für Wildcard-Modus = <i>statisch</i></p> <p>Geben Sie die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist.</p>
Transparente MAC-Adresse	<p>Nur für Wildcard-Modus = <i>statisch, zuerst</i></p> <p>Wählen Sie aus, ob die Wildcard-MAC-Adresse zusätzlich als WLAN-MAC-Adresse benutzt werden, um damit die Verbindung</p>

Feld	Wert
	zum Access Point herzustellen.
	Mit <i>Aktiviert</i> wird die Funktion aktiv.
	Standardmäßig ist die Funktion nicht aktiv.

7.4 Administrativer Zugriff

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

7.4.1 Zugriff

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

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"/>					
bri-0	<input type="checkbox"/>	<input checked="" type="checkbox"/>					

Erweiterte Einstellungen

Standardeinstellungen wiederherstellen

Hinzufügen OK Abbrechen

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

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

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

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

Felder im Menü **Erweiterte Einstellungen**

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

7.4.1.1 Hinzufügen

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



Abb. 41: **Systemverwaltung ->Administrativer Zugriff ->Zugriff ->Hinzufügen**

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

Felder im Menü Zugriff

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

7.4.2 SSH

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

Zugriff SSH SNMP

SSH-Parameter (Secure Shell)	
SSH-Dienst aktiv	<input checked="" type="checkbox"/> Aktiviert
SSH-Port	<input type="text" value="22"/>
Maximale Anzahl gleichzeitiger Verbindungen	<input type="text" value="1"/>
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	Nicht generiert [Generieren]
Erweiterte Einstellungen	
Toleranzzeit beim Login	<input type="text" value="600"/> Sekunden
Komprimierung	<input type="checkbox"/> Aktiviert
TCP-Keepalives	<input checked="" type="checkbox"/> Aktiviert
Protokollierungslevel	<input type="text" value="Informationen"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

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

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



Hinweis

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

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

Felder im Menü SSH-Parameter (Secure Shell)

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

Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

Feld	Wert
Verschlüsselungsalgorithmen	Wählen Sie die Algorithmen, die für die Verschlüsselung der SSH-Verbindung verwendet werden sollen. Mögliche Optionen: <ul style="list-style-type: none"> • <i>3DES</i> • <i>Blowfish</i> • <i>AES-128</i> • <i>AES-256</i> Standardmäßig sind <i>3DES</i> , <i>Blowfish</i> und <i>AES-128</i> aktiv.
Hashing-Algorithmen	Wählen Sie die Algorithmen, die zur Message-Authentisierung der SSH-Verbindung verwendet werden sollen. Mögliche Optionen: <ul style="list-style-type: none"> • <i>MD5</i> • <i>SHA-1</i> • <i>RipeMD 160</i> Standardmäßig sind <i>MD5</i> , <i>SHA-1</i> und <i>RipeMD 160</i> aktiv.

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 Speicherplatz im FlashROM.</p>

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

Felder im Menü Erweiterte Einstellungen

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

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

7.4.3 SNMP

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

Die Datenobjekte, die per SNMP abgefragt werden können, sind in Tabellen und Variablen strukturiert und in der sogenannten MIB (Management Information Base) definiert. Sie 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. 43: Systemverwaltung ->Administrativer Zugriff->SNMP

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

Felder im Menü Grundeinstellungen

Feld	Wert
SNMP-Version	<p>Wählen Sie aus, welche SNMP-Version Ihr Gerät für externe SNMP-Zugriffe verwenden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • v1: SNMP-Version 1 • v2c: Community-Based SNMP-Version 2 • v3: SNMP-Version 3 <p>Standardmäßig sind v1, v2c und v3 aktiv.</p> <p>Ist keine Option ausgewählt, ist die Funktion nicht aktiv.</p>
SNMP-Listen-UDP-Port	<p>Zeigt den UDP-Port (161) 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.

7.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

7.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete

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

Pakettypen

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

Feld	Wert
ACCESS_ACCEPT	Server -> Client Wenn der RADIUS-Server die im ACCESS_REQUEST enthaltenen Informationen authentifiziert hat, sendet er ein ACCESS_ACCEPT zu Ihrem Gerät mit den für den Verbindungsaufbau zu verwendenden Parametern.
ACCESS_REJECT	Server -> Client Wenn die im ACCESS_REQUEST enthaltenen Informationen nicht den Informationen in der Benutzerdatenbank des RADIUS-Servers entsprechen, sendet er ein ACCESS_REJECT zur 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.

7.5.1.1 Bearbeiten oder Neu

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

RADIUS TACACS+ Optionen

Basisparameter	
Authentifizierungstyp	PPP-Authentifizierung ▾
Server-IP-Adresse	<input type="text"/>
RADIUS-Passwort	••••••••
Standard-Benutzerpasswort	••••••••
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. 44: Systemverwaltung ->Remote Authentifizierung ->RADIUS->Neu

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

Felder im Menü Basisparameter

Feld	Wert
Authentifizierungstyp	Wählen Sie aus, wofür der RADIUS-Server verwendet werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>PPP-Authentifizierung</i> (Standardwert, nur für PPP-Verbindungen): Der RADIUS-Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln. • <i>Accounting</i> (nur für PPP-Verbindungen): 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 kon-

Feld	Wert
	<p>trollieren.</p> <ul style="list-style-type: none"> • <i>IPSec-Authentifizierung</i>: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln. • <i>WLAN (802.1x)</i>: Der RADIUS-Server wird verwendet, um den Zugang zu einem Drahtlosnetzwerk zu regeln. • <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 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	<p>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.</p> <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>

Feld	Wert
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>Standardgruppe 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.
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 Gebührenerfas-</p>

Feld	Wert
	<p>sung (1646 in ältere 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 der 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> <p>Mögliche Werte sind ganze Zahlen zwischen <i>0</i> und <i>10</i>.</p> <p>Standardwert ist <i>1</i>. Um zu verhindern, dass Status auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf <i>0</i>.</p>

Feld	Wert
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 Optionen 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 <i>0</i> eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>

7.5.2 TACACS+

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

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

Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:

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

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

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

7.5.2.1 Bearbeiten oder Neu

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

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Authentifizierungstyp	<p>Zeigt an, welche TACACS+-Funktion genutzt werden soll. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <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.

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Richtlinie	Wählen Sie die Interpretation der TACACS+-Antwort aus. Mögliche Werte: <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. Die Geräte-interne Benutzerverwaltung wird durch TACACS+ nicht ausgeschaltet. Sie wird geprüft, nachdem alle TACACS+-Server abgefragt wurden.
TCP-Port	Zeigt den für das TACACS+-Protokoll verwendeten Standard-

Feld	Beschreibung
	TCP-Port (49) an. Der Wert kann nicht verändert werden.
Timeout	<p>Geben Sie die Zeit in Sekunden ein, die der NAS auf eine Antwort von TACACS+ warten soll.</p> <p>Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster 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>

7.5.3 Optionen

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

Abb. 46: Systemverwaltung ->Remote Authentifizierung ->Optionen

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

Felder im Menü Globale RADIUS-Optionen

Feld	Beschreibung
Authentifizierung für PPP-Einwahl	<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>

7.6 Konfigurationszugriff

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

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

7.6.1 Zugriffsprofile

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

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



Abb. 47: Systemverwaltung -> Konfigurationszugriff -> Zugriffsprofile

7.6.1.1 Bearbeiten oder Neu

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

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

Zugriffsprofile Benutzer

Grundeinstellungen	
Beschreibung	<input style="width: 100%;" type="text"/>
Level Nr.	7
Schaltflächen	
Konfiguration speichern	<input type="checkbox"/> Aktiviert
Zum SNMP Browser wechseln	<input type="checkbox"/> Aktiviert
Navigationseinträge	
Assistenten ▲ ✖	
Erste Schritte ▼ ✖	
PBX ▼ ✖	
Systemverwaltung ▼ ✖	
Physikalische Schnittstellen ▼ ✖	
VoIP ▼ ✖	
Nummerierung ▼ ✖	
Endgeräte ▼ ✖	
Anrufkontrolle ▼ ✖	
Anwendungen ▼ ✖	
LAN ▼ ✖	
Netzwerk ▼ ✖	
Firewall ▼ ✖	
VoIP ▼ ✖	
Lokale Dienste ▼ ✖	
Wartung ▼ ✖	
Externe Berichterstellung ▼ ✖	
Monitoring ▼ ✖	
Benutzerzugang ▼ ✖	

OK Abbrechen

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

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

Felder im Menü Grundeinstellungen

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

Feld	Beschreibung
	Zugriffsprofil. Diese kann nicht editiert werden.

Felder im Menü Schaltflächen

Feld	Beschreibung
Konfiguration speichern	<p>Wenn Sie die Schaltfläche Konfiguration speichern aktivieren, darf der Benutzer Konfigurationen speichern.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> Hinweis</p> <p>Beachten Sie, dass die Passwörter in der gespeicherten Datei im Klartext eingesehen werden können.</p> </div> <p>Aktivieren oder deaktivieren Sie Konfiguration speichern.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zum SNMP Browser wechseln	<p>Wenn Sie die Schaltfläche Zum SNMP Browser wechseln aktivieren, kann der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und alle dort angezeigten Einstellungen ändern.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> Achtung</p> <p>Beachten Sie, dass die Berechtigung für Zum SNMP Browser wechseln bedeutet, dass der Benutzer auf die gesamte MIB zugreifen kann, da in dieser Ansicht kein individuelles Zugangsprofil angelegt werden kann. Mit der Berechtigung für Konfiguration speichern kann er die geänderte MIB speichern.</p> <p>Mit der Berechtigung für Zum SNMP Browser wechseln heben Sie die konfigurierten GUI- Einschränkungen auf der MIB-Ebene wieder auf.</p> </div> <p>Aktivieren oder deaktivieren Sie Zum SNMP Browser wechseln.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü Navigationseinträge

Feld	Beschreibung
Menüs	<p>Sie sehen alle Menüs aus der Navigationsleiste des GUI. Menüs, die mindestens ein Untermenü enthalten, sind mit  bzw.  gekennzeichnet. Das Symbol  kennzeichnet Seiten.</p> <p>Wenn Sie ein neues Zugriffsprofil anlegen, sind noch keine Elemente zugewiesen, d.h. alle verfügbaren Menüs, Untermenüs und Seiten sind mit dem Symbol  gekennzeichnet.</p> <p>Jedes Element in der Navigationsleiste kann drei Werte annehmen. Klicken Sie in der gewünschten Zeile auf das Symbol , um diese drei Werte anzeigen zu lassen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Verweigern</i>: Das Menü und alle untergeordneten Menüs sind gesperrt. • <i>Zulassen</i>: Das Menü ist freigegeben. Untergeordnete Menüs müssen gegebenenfalls gesondert freigegeben werden. • <i>Alle zulassen</i>: Das Menü und alle untergeordneten Menüs sind freigegeben. <p>Sie können in der entsprechenden Zeile <i>Zulassen</i> bzw. <i>Alle zulassen</i> wählen, um dem aktuellen Zugriffsprofil Elemente zuzuweisen.</p> <p>Elemente, die dem aktuellen Zugriffsprofil zugewiesen sind, sind mit dem Symbol  gekennzeichnet.</p> <p> kennzeichnet ein Menü, das gesperrt ist, das aber mindestens über ein freigegebenes Untermenü verfügt.</p>

7.6.2 Benutzer

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

 löschen.



Abb. 49: Systemverwaltung -> Konfigurationszugriff -> Benutzer

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

Zugriffsprofile Benutzer

Grundeinstellungen	
Benutzer	user 1
Benutzer muss das Passwort ändern	Deaktiviert
Schaltflächen	
Konfiguration speichern	Deaktiviert
Zum SNMP Browser wechseln	Deaktiviert
Navigationseinträge	
Assistenten	▲ 🔒 🔒
Erste Schritte	▼ 🔒 🔒
PBX	▼ 🔒 🔒
Systemverwaltung	▼ 🔒 🔒
Physikalische Schnittstellen	▼ 🔒 🔒
VoIP	▼ 🔒 🔒
Nummerierung	▼ 🔒 🔒
Endgeräte	▼ 🔒 🔒
Anrufkontrolle	▼ 🔒 🔒
Anwendungen	▼ 🔒 🔒
LAN	▼ 🔒 🔒
Netzwerk	▼ 🔒 🔒
Firewall	▼ 🔒 🔒
VoIP	▼ 🔒 🔒
Lokale Dienste	▼ 🔒 🔒
Wartung	▼ 🔒 🔒
Externe Berichterstellung	▼ 🔒 🔒
Monitoring	▼ 🔒 🔒
Benutzerzugang	▼ 📄 📄

Abbrechen

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

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

7.6.2.1 Bearbeiten oder Neu

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

Zugriffsprofile
Benutzer

Grundeinstellungen	
Benutzer	<input type="text"/>
Passwort	<input type="password" value="....."/>
Benutzer muss das Passwort ändern	<input type="checkbox"/> Aktiviert
Zugangs-Level	<div style="border: 1px solid gray; padding: 2px; display: inline-block;"> Zugangs-Level Nur lesen </div> <div style="margin-top: 5px; text-align: center;"> Hinzufügen </div>

OK
Abbrechen

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

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

Felder im Menü Grundeinstellungen

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

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

7.7 Zertifikate

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

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

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

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

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

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

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

bindungen über Voice over IP ausgestattet.

7.7.1 Zertifikatsliste

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

7.7.1.1 Bearbeiten

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

Zertifikatsliste CRLs Zertifikatsserver

Parameter bearbeiten	
Beschreibung	xp.ptx
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. 52: **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsliste** -> 

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

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

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

Felder im Menü Parameter bearbeiten

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.
Zertifikat ist ein CA-Zertifikat	<p>Markieren Sie das Zertifikat als Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA).</p> <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>
Überprüfung anhand einer Zertifikatsperrliste (CRL)	<p>Nur für Zertifikat ist ein CA-Zertifikat = <i>Wahr</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 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</i> (Standardwert): Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden. • <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.
Vertrauenswürdigkeit des Zertifikats erzwingen	Legen Sie fest, dass dieses Zertifikat ohne weitere Überprüfung bei der Authentifizierung als Benutzerzertifikat akzeptiert werden soll.

Feld	Beschreibung
	<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.

7.7.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

[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. 53: Systemverwaltung ->Zertifikate->Zertifikatsliste->Zertifikatsanforderung

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

Felder im Menü Zertifikatsanforderung

Feld	Beschreibung
Zertifikatsanforderungsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Modus	<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.beispiel.com: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 Subjekname

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.

7.7.1.3 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. 54: Systemverwaltung ->Zertifikate->Zertifikatsliste->Importieren

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

Felder im Menü Importieren

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen des Zertifikats ein, welches importiert werden soll oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät das Zertifikat dekodieren kann. Mögliche Werte: <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.

7.7.2 CRLs

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

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

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

7.7.2.1 Importieren

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

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

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

Felder im Menü CRL-Import

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

Feld	Beschreibung
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für die CRL ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät die CRL decodieren kann. Mögliche Werte: <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.

7.7.3 Zertifikatsserver

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

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

7.7.3.1 Neu

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

Zertifikatsserver	
Basisparameter	
Beschreibung	<input type="text"/>
LDAP-URL-Pfad	<input type="text" value="ldap://"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

Felder im Menü Basisparameter

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

Kapitel 8 Physikalische Schnittstellen

8.1 Ethernet-Ports

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

Die Ethernet-Ports **ETH1** bis **ETH4** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle *en1-0* ist zugewiesen und mit **IP-Adresse** *192.168.0.254* und **Netzmaske** *255.255.255.0* vorkonfiguriert.

Der Port **ETH5** (mit Anschlussmöglichkeit eines SFP-Moduls nur für **bintec RS120 / bintec RS120wu** verfügbar) ist 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 - ETH4

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

ETH5 (mit Anschlussmöglichkeit eines SFP-Moduls nur für bintec RS120 / bintec RS120wu verfügbar)

Standardmäßig ist dem Port **ETH5** die logische Ethernet-Schnittstelle *en1-4* zugewiesen. Die Konfigurationsoptionen sind identisch mit denen der Ports **ETH1 - ETH4**.



Hinweis

Wenn Sie den Port **ETH5** 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 **ETH5**-Port ohne SFP-Modul möglich. Soll der **ETH5**-Port nach Einsatz eines SFP-Moduls verwendet werden, muss das Gerät neu gestartet werden.

Die wechselnde Nutzung des **ETH5**-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, 40km

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.

8.1.1 Portkonfiguration

Portseparation

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

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

Portkonfiguration

Automatisches Aktualisierungsintervall Sekunden

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

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

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

Felder im Menü Switch-Konfiguration

Feld	Beschreibung
Switch-Port	<p>Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.</p> <p>Switch-Port 5: Hier wird Port ETH5 konfiguriert (Anschlussmöglichkeit eines SFP-Moduls nur für bintec RS120 / bintec RS120wu verfügbar).</p>
Ethernet-Schnittstellenauswahl	<p>Ordnen Sie dem jeweiligen Switch-Port eine logische Ethernet-Schnittstelle zu.</p> <p>Zur Auswahl stehen fünf Schnittstellen, <i>en1-0</i> bis <i>en1-4</i>. In der Grundeinstellung ist Switch Port 1-4 die Schnittstelle <i>en1-0</i>, Switch Port 5 die Schnittstelle <i>en1-4</i> zugeordnet.</p>
Konfigurierte Geschwindigkeit/konfigurierter Modus	<p>Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Vollständige automatische Aushandlung</i> (Standardwert) <i>Auto 1000 Mbit/s only</i> <i>Auto 100 Mbit/s only</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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.

Für die Nutzung des Ports **ETH5** mit SFP-Modul, können für den Eintrag **Switch-Port 5** in diesem Menü folgende Einstellungen getätigt werden:

Felder im Menü **Switch-Konfiguration für Switch Port 5 im SFP Modus**

Feld	Beschreibung
Ethernet-Schnittstellenauswahl	<p>Ordnen Sie dem Switch-Port die gewünschte logische Ethernet-Schnittstelle zu.</p> <p>Zur Auswahl stehen fünf Schnittstellen, <i>en1-0</i> bis <i>en1-4</i>. Switch Port 5 ist im Auslieferungszustand die Schnittstelle <i>en1-4</i> zugeordnet.</p>
Konfigurierte Geschwindigkeit/konfigurierter Modus	<p>Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Fest 1000 Mbit/s / Full Duplex</i> (Standardwert) • <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>Inaktiv</i>

8.2 ISDN-Ports

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

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

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

8.2.1 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.

8.2.1.1 Bearbeiten

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

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	<input type="text" value="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
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 58: **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.

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

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>

8.2.2 MSN-Konfiguration

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

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

Das Gerät unterstützt die Dienste:

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

8.2.2.1 Neu

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

Abb. 59: **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)</i>, <i>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)

8.3 DSL-Modem

8.3.1 DSL-Konfiguration

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

DSL-Konfiguration

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen	
DSL-Portstatus	
DSL-Chipsatz	Lantiq VRX288
Physikalische Verbindung	Unbekannt
Aktuelle Leitungsgeschwindigkeit	
Downstream	0Bit/s
Upstream	0Bit/s
DSL Parameter	
DSL-Modus	VDSL/ADSL Multimodus ▾
Transmit Shaping	Standard (Leitungsgeschwindigkeit) ▾
Erweiterte Einstellungen	
ADSL-Leitungsprofil	Deutsche Telekom ▾
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 60: Physikalische Schnittstellen->DSL-Modem->DSL-Konfiguration

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

Felder im Menü DSL-Portstatus

Feld	Beschreibung
DSL-Chipsatz	Zeigt die Kennung des eingebauten Chipsatzes an.
Physikalische Verbindung	<p>Zeigt den aktuellen ADSL-Betriebsmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Unbekannt</i>: Der ADSL-Link ist nicht aktiv. • <i>ANSI T1.413</i>: ANSI T1.413 • <i>ADSL1</i>: ADSL classic, G.DMT, ITU G.992.1 • <i>G.lite G992.2</i>: Splitterless ADSL, ITU G.992.2

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>ADSL2</i>: G.DMT.Bis, ITU G.992.3 • <i>ADSL2 DELT</i>: ADSL2 Double Ended Line Test • <i>ADSL2 Plus</i>: ADSL2 Plus, ITU G.992.5 • <i>ADSL2 Plus DELT</i>: ADSL2 Plus Double Ended Line Test • <i>READSL2</i>: Reach Extended ADSL2 • <i>READSL2 DELT</i>: Reach Extended ADSL2 Double Ended Line Test. • <i>ADSL2 ITU-T G.992.3 Annex M</i> • <i>ADSL2+ ITU-T G.992.5 Annex M</i> • <i>ADSL2 Annex J</i> • <i>ADSL2+ Annex J</i>

Felder im Menü Aktuelle Leitungsgeschwindigkeit

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

Felder im Menü DSL Parameter

Feld	Beschreibung
DSL-Modus	<p>Wählen Sie den ADSL-Synchronisierungstyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Modus (ADSL)</i> (Standardwert): Der ADSL-Modus wird dem der Gegenstelle automatisch angepasst. • <i>ADSL1</i>: ADSL1 / G.DMT wird angewendet. • <i>ADSL2</i>: ADSL2 / G.992.3 wird angewendet. • <i>ADSL2 Plus</i>: ADSL2 Plus / G.992.5 wird angewendet. • <i>Automatischer Modus (Annex-M)</i>: Nur für Annex-A-Geräte. Der ADSL-Modus wird dem der Gegenstelle auto-

Feld	Beschreibung
	<p>matisch angepasst unter Einbeziehung von G.992.3 Annex-M.</p> <ul style="list-style-type: none"> • <i>ADSL2 Plus (Annex-M)</i>: Nur für Annex-A-Geräte. ADSL2 Plus / G.992.3 Annex-M wird angewendet. • <i>ADSL2 Annex J</i>: Nur für Annex-J-Geräte. ADSL2 Plus / G.992.3 Annex-J wird angewendet. • <i>ADSL2+ Annex J</i>: Nur für Annex-J-Geräte. ADSL2 Plus / G.992.5 Annex-J wird angewendet. • <i>Inaktiv</i>: Die ADSL-Schnittstelle ist nicht aktiv.
Transmit Shaping	<p>Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DSLAMs notwendig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard (Leitungsgeschwindigkeit)</i>: Die Datenrate in Senderichtung wird nicht reduziert. • <i>128.000 Bit/s, 192.000 Bit/s, 256.000 Bit/s, 512.000 Bit/s, 768.000 Bit/s, 1.024.000 Bit/s, 1.536.000 Bit/s und 2.048.000 Bit/s</i>: Die Datenrate in Senderichtung wird reduziert auf maximal 128.000 Bit/s bis 2.048.000 Bit/s in festgesetzten Schritten. • <i>Benutzerdefiniert</i>: Die Datenrate wird reduziert auf den in Maximale Upstream-Bandbreite eingegebenen Wert. <p>Standardwert ist <i>Standard (Leitungsgeschwindigkeit)</i>.</p>
Maximale Upstream-Bandbreite	<p>Nur für Transmit Shaping = <i>Benutzerdefiniert</i></p> <p>Geben Sie die maximale Datenrate in Senderichtung in Bits pro Sekunde ein.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
ADSL-Leitungsprofil	<p>Wählen Sie den gewünschten Internet-Service-Provider und damit implizit den von diesem Provider verwendeten Modem-Parametersatz aus.</p> <p><i>Deutsche Telekom</i> ist als Standardwert voreingestellt.</p>

Feld	Beschreibung
	Wenn Sie Ihren Provider in der Liste nicht finden, verwenden Sie die Einstellung <i>Standard</i> .

8.4 UMTS/LTE

8.4.1 UMTS/LTE

Im Menü **UMTS/LTE** konfigurieren Sie die Anbindung des integrierten UMTS/HSD-PA/LTE-Modems (für **bintec RS232j-4G**), UMTS/HSDPA-Modems (für **bintec RS120wu** und **bintec RS230au+**) oder eines optional steckbaren UMTS/LTE-USB-Sticks (für **bintec RS120wu**, **bintec RS230au+** und **bintec RS232j-4G**).

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



Hinweis

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



Hinweis

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

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

8.4.1.1 Bearbeiten

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

Wählen Sie folgenden Eintrag für das entsprechende UMTS/LTE-Modem:

- *Slot6 Unit 0*: Das integrierte Modem soll konfiguriert werden.
- *Slot6 Unit 1*: Der gesteckte UMTS/LTE-USB-Stick soll konfiguriert werden.



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

Erweiterte Einstellungen	
Roaming/PLNM-Auswahl	
Roaming-Modus	Deaktiviert
Geschlossene Benutzergruppe	
Authentifizierungsmethode	pap-chap
Benutzername	
Passwort	
Feste IP-Adresse	

Abb. 61: 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	Wählen Sie aus, ob das gewählte UMTS/LTE-Modem aktiviert werden soll oder nicht.

Feld	Beschreibung
	<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> • <i>SIM Einlegen erforderlich</i> • <i>PIN Eingabe erforderlich</i> • <i>Fehler</i> • <i>Nicht verbunden</i>
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>
Aktuelles Netzwerk	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Zeigt das aktuelle Netzwerk an, z. B. GSM oder UMTS.</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>

Feld	Beschreibung
	<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 bevorzugt LTE verwendet, sollte LTE nicht verfügbar sein, wird UMTS verwendet, sollte UMTS nicht verfügbar sein, wird GPRS verwendet • <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 ausreichenden

Feld	Beschreibung
	<p>der Signalstärke und Signalqualität von LTE wird GPRS verwendet..</p> <ul style="list-style-type: none"> • <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. <div data-bbox="539 713 1320 1202" style="border: 1px solid gray; padding: 10px; margin-top: 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 Diensttyp	<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 zugewie-

Feld	Beschreibung
	<p>sen.</p> <ul style="list-style-type: none"> • <i>IPSec</i>: Der Ruf erfolgt über IPSec. <p>Beachten Sie für die Einstellung Eingehender Diensttyp <i>IPSec</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> <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>
	<div data-bbox="539 1374 621 1426" style="float: left; margin-right: 10px;"></div> <p>Hinweis</p> <p>Die Eingabe einer falschen PIN unterbindet die Kommunikation bis der Eintrag korrigiert wird.</p>

Feld	Beschreibung
	<div data-bbox="539 211 1319 433" style="border: 1px solid gray; padding: 5px;">  <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> </div>
<p>Fallback-Nummer</p>	<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-Modus aktiviert (Option Immer aktiv aktiviert in WAN->Internet + Einwählen->UMTS/LTE->), führt dies zu sofortigem Verbindungswiederaufbau.</p> <div data-bbox="539 924 1319 1111" 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 = <i>Aktiviert</i></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>

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

Felder im Menü Roaming/PLMN-Auswahl

Feld	Beschreibung
Roaming-Modus	<p>Wählen Sie aus, ob Sie Roaming verwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i>: Roaming ist ausgeschaltet. Das Home PLMN (Public Land Mobile Network) wird verwendet, d.h. der Anbieter, bei dem die SIM-Karte registriert ist. • <i>Automatische Auswahl</i> (Standardeinstellung): Verwenden Sie diesen Modus, wenn weder Roaming-Modus = Deaktiviert noch Roaming-Modus = Fest eingestellt Ihren Anforderungen entspricht. Beachten Sie, dass bei diesem Modus zuerst ein Scan über alle APNs durchgeführt wird. Das System versucht eine kostenoptimierte Weiterleitung zu nutzen um Roaming-Gebühren zu sparen. • <i>Uneingeschränkt</i>: Dieser Modus ist für spezielle Anforderungen vorgesehen. Beachten Sie, dass bei diesem Modus zuerst ein Scan über alle APNs durchgeführt wird. • <i>Fester Netzbetreiber</i>: Bei Roaming-Modus = Fest eingestellt wird kein Scan durchgeführt, nur der manuell ausgewählter Mobilnetzbetreiber wird verwendet. Wenn der ausgewählte Mobilnetzbetreiber nicht zur Verfügung steht, ist keine Verbindung möglich. • <i>Vollständig automatische Auswahl</i>: Bei dieser Auswahl wird kein Scan durchgeführt. Das Modem wählt automatisch den stärksten verfügbaren Mobilnetzbetreiber aus. Das kann in Grenznähe auch das Netz eines ausländischen Roamingpartners sein.
Mobilnetzbetreiber	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i><Anbieter></i>: Wählen Sie einen Mobilnetzbetreiber aus der Liste aus. • <i>Manuelle Eingabe</i>: Damit kann manuell eine Provider ID (PLMN) eingegeben werden.
Mobilnetzbetreiber	<p>Hier können Sie einen PLMN (Public Land Mobile Network) eintragen.</p> <p>Jedes Mobilfunknetz wird durch eine weltweit eindeutige Kennung identifiziert, die sich aus der MCC (Mobile Country Code) und der MNC (Mobile Network Code) zusammensetzt, z.B. die MCC für Deutschland ist 262, und die MNC für T-Mobile in</p>

Feld	Beschreibung
	Deutschland ist 01. Dadurch ergibt sich das PLMN <i>26201</i> .

Felder im Menü Geschlossene Benutzergruppe

Feld	Beschreibung
Authentifizierungsmethode	<p>Wählen Sie das Authentifizierungsprotokoll für die Geschlossene Benutzergruppe aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option. • <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> (Standardwert): Vorrangig CHAP, sonst PAP ausführen.
Benutzername	Geben Sie den Benutzernamen ein, den Sie von Ihrem Provider erhalten haben.
Passwort	Geben Sie das Passwort ein, das Sie von Ihrem Provider erhalten haben.
Feste IP-Adresse	Geben Sie die IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.

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

UMTS/LTE

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden		Übernehmen	
Status des Mobilgerätes			
Gerät	/dev/usbTTY0		
Modemmodell	MC7710		
IMEI	355060020096827		
Oper Status	Verbinden		
ICC ID	89490200000756575697		
Rufnummer			
Adresse des Service-Centers	+491710760000		
Home PLMN	26201 Telekom.de		
Ausgewähltes PLMN	26201		
Aktuelles Netzwerk	GSM		
Netzwerkqualität	-		
Funkzellen Code	4427		
Cell ID	00001EA7		
Letzter Befehl	AT+C SQ		
Letzte Antwort	22,99		
Netzbetreiber			
PLMN	Name	Zugangstyp	Status
26201	Telekom.de	GSM	Aktuell

Abb. 62: Physikalische Schnittstellen ->UMTS/LTE-> 

Werte in der Liste Status des Mobilgerätes

Feld	Beschreibung
Gerät	Zeigt die Bezeichnung des internen Modemanschlusses an.
Modemmodell	Zeigt die Bezeichnung des Modems an.
IMEI	Die IMEI (International Mobile Station Equipment Identity) zeigt die 15-stellige Seriennummer des Modems an.
Oper Status	Zeigt den Betriebszustand des Modems an.
ICC ID	Zeigt die Karten-ID an, die auf der SIM-Karte hinterlegt ist.
Rufnummer	Zeigt die Rufnummer an, die auf der SIM-Karte hinterlegt ist.
Adresse des Service-Centers	Zeigt die Adresse des Provider Service-Centers an, die auf der SIM-Karte hinterlegt ist.
Home PLMN	Zeigt das Home PLMN (Public Land Mobile Network) an, d.h. den Anbieter, bei dem die SIM-Karte registriert ist.
Ausgewähltes PLMN	Zeigt ein eventuell ausgewähltes PLMN an. Falls kein PLMN ausgewählt wurde, wird das Home PLMN angezeigt.
Aktuelles Netzwerk	Zeigt an, welches Netz aktuell verwendet wird (z. B. UMTS oder GSM).

Feld	Beschreibung
Netzwerkqualität	Zeigt die aktuelle Qualität der Verbindung an.
Funkzellen Code	Zeigt den Funkzellen Code der Funkzelle an, in der das Modem aktuell registriert ist.
Cell ID	Zeigt die Cell ID der Funkzelle an, in der das Modem aktuell registriert ist.
Letzer Befehl	Zeigt den letzten Befehl an, der vom System an das Modem geschickt wurde.
Letzte Antwort	Zeigt die letzte Antwort an, die vom Modem gegeben wurde.

Werte in der Liste Netzbetreiber

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

Kapitel 9 LAN

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

9.1 IP-Konfiguration

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

9.1.1 Schnittstellen

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

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

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

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



Hinweis

Beachten Sie bitte:

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

Sollten sie dagegen bei der Erstkonfiguration eine Verbindung zum Gerät über die Standard-IP-Adresse aufgebaut oder eine IP-Adresse mit dem **Dime Manager** vergeben haben, ist es nur noch über diese IP-Adresse erreichbar. Es kann nicht mehr dynamisch über DHCP eine IP-Konfiguration erhalten.

Beispiel Teilnetze

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

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

9.1.1.1 Bearbeiten oder Neu

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

Schnittstellen

Basisparameter					
Basierend auf Ethernet-Schnittstelle	<input type="text" value="Eine auswählen"/>				
Adressmodus	<input checked="" type="radio"/> Statisch <input 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><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"/>					
Schnittstellenmodus	<input type="radio"/> Untagged <input checked="" type="radio"/> Tagged (VLAN)				
MAC-Adresse	<input type="text" value="00:a0:f9"/> <input checked="" type="checkbox"/> Voreingestellte verwenden				
VLAN-ID	<input type="text" value="1"/>				
Erweiterte Einstellungen					
Proxy ARP	<input type="checkbox"/> Aktiviert				
TCP-MSS-Clamping	<input type="checkbox"/> Aktiviert				
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 63: LAN->IP-Konfiguration->Schnittstellen-> /Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird.

Feld	Beschreibung
	Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.
Adressmodus	<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 virtuellen Schnittstelle ein.</p>
Schnittstellenmodus	<p>Nur bei physikalischen Schnittstellen im Routing-Modus und bei virtuelle Schnittstellen.</p> <p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Untagged</i> (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet. • <i>Tagged (VLAN)</i>: 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>
MAC-Adresse	Geben Sie die mit der Schnittstelle verbundene MAC-Adresse ein. Sie können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde, wenn Sie Voreingestellte verwenden aktivieren. Die VLAN IDs müssen sich jedoch unterscheiden. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt (sie können jedoch geändert werden).

Feld	Beschreibung
	<p>Wenn Voreingestellte verwenden aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet.</p> <p>Standardmäßig ist Voreingestellte verwenden aktiv.</p>
VLAN-ID	<p>Nur für Schnittstellenmodus = <i>Tagged</i> (VLAN)</p> <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 1 (Standardwert) bis 4094.</p>

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

Felder im Menü **Erweiterte 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> <p>Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-</p>

Feld	Beschreibung
	<p>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>

9.2 VLAN

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

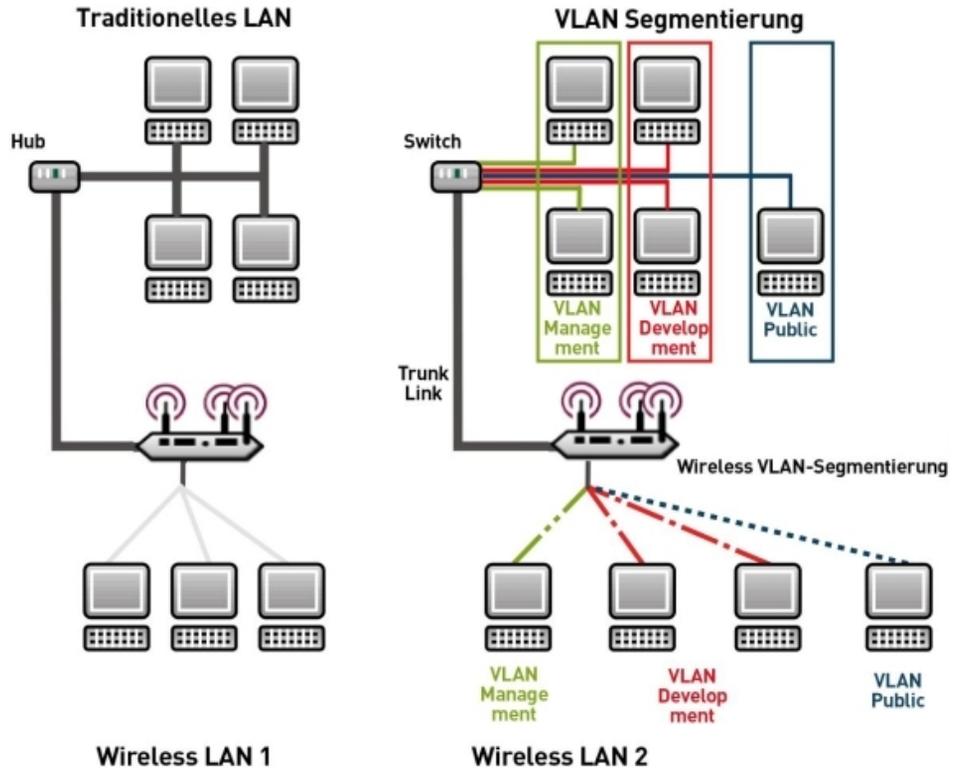


Abb. 64: VLAN-Segmentierung

VLAN für Bridging und VLAN für Routing

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



Achtung

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

9.2.1 VLANs

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

9.2.1.1 Bearbeiten oder Neu

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



Abb. 65: LAN->VLAN->VLANs->Neu

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

Felder im Menü VLAN konfigurieren

Feld	Beschreibung
VLAN Identifier	Geben Sie die Ziffer ein, die das VLAN identifiziert. Im  -Menü kann dieser Wert nicht mehr verändert werden. Mögliche Werte sind 1 bis 4094
VLAN-Name	Geben Sie einen eindeutigen Namen für das VLAN ein. Möglich ist eine Zeichenkette mit bis zu 32 Zeichen.
VLAN-Mitglieder	Wählen Sie die Ports aus, die zu diesem VLAN gehören sollen. Über die Schaltfläche Hinzufügen können Sie weitere Mitglieder hinzufügen. Wählen Sie weiterhin zu jedem Eintrag aus, ob die Frames, die von diesem Port übertragen werden, <i>Tagged</i> (also mit VLAN-Information) oder <i>Untagged</i> (also ohne VLAN-Information)

Feld	Beschreibung
	übertragen werden sollen.

9.2.2 Portkonfiguration

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

Abb. 66: LAN->VLANs->Portkonfiguration

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

Felder im Menü Portkonfiguration

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

9.2.3 Verwaltung

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

The screenshot shows a configuration window with the following elements:

- Navigation tabs: VLANs, Portkonfiguration, **Verwaltung** (selected)
- Title bar: Bridge-Gruppe br0 VLAN-Optionen
- Field 1: VLAN aktivieren, Aktiviert
- Field 2: Verwaltungs-VID, 1 - Management (dropdown)
- Buttons: OK, Abbrechen

Abb. 67: 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	<p>Aktivieren oder deaktivieren Sie die spezifizierte Bridge-Gruppe für VLAN.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>
Verwaltungs-VID	<p>Wählen Sie die VLAN-ID des VLANs aus, in dem Ihr Gerät arbeiten soll.</p>

Kapitel 10 Wireless LAN

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

Netzwerkfunktionen

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

Derzeit gültiger Standard: IEEE 802.11

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

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

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

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

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

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

10.1 WLAN

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

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

10.1.1 Einstellungen Funkmodul

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

Einstellungen Funkmodul

Einstellungen Funkmodul							
MAC-Adresse	Betriebsmodus	Frequenzband	Verwendeter Kanal	Maximale Bitrate	Sendeleistung	Status	
00:0d:f0:00:8b:17	Aus	2,4 GHz	-	Auto	Max.		

Abb. 68: **Wireless LAN->WLAN->Einstellungen Funkmodul**

10.1.1.1 Einstellungen Funkmodul->

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie das Symbol  um die Konfiguration zu bearbeiten.

Einstellungen Funkmodul

WLAN-Einstellungen	
Betriebsmodus	Access-Point / Bridge Link Master ▾
Frequenzband	2,4 GHz In/Outdoor ▾
Kanal	Auto ▾
Ausgewählter Kanal	0
Sendeleistung	Max. ▾
Performance-Einstellungen	
Drahtloser Modus	802.11g ▾
Airtime Fairness	<input type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Kanalplan	Alle ▾
RTS Threshold	Immer inaktiv ▾
Short Guard Interval	<input checked="" type="checkbox"/> Aktiviert
Fragmentation Threshold	2346 Bytes
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 69: **Wireless LAN->WLAN->Einstellungen Funkmodul->**  **für Betriebsmodus** *Access-Point*

Einstellungen Funkmodul

WLAN-Einstellungen	
Betriebsmodus	Access Client
Client-Modus	<input checked="" type="radio"/> Infrastruktur <input type="radio"/> Ad-Hoc
Frequenzband	2,4 GHz
IEEE 802.11d-Konformität	Flexibel
Kanal	0
Ausgewählter Kanal	0
Zweiter Verwendeter Kanal	0
Bandbreite	40 MHz
Anzahl der Spatial Streams	2
Sendeleistung	Max.
Performance-Einstellungen	
Drahtloser Modus	802.11b/g/n
Max. Übertragungsrate	Auto
Burst-Mode	<input checked="" type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 70: Wireless LAN WLAN Einstellungen Funkmodul  für Betriebsmodus *Access Client*

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

Felder im Menü WLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	<p>Legen Sie fest, in welchem Modus das Funkmodul Ihres Geräts betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Das Funkmodul ist nicht aktiv. • <i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk. • <i>Access Client</i>: Ihr Gerät dient als Access Client in Ihrem Netzwerk.
Client-Modus	<p>Nur für Betriebsmodus = <i>Access Client</i></p> <p>Wählen Sie den Modus der Verbindung des Clients zum Access Point aus.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Infrastruktur</i> (Standardwert): In einem Netz im Infrastruktur Modus kommunizieren alle Clients ausschließlich über Access Points miteinander. Es läuft keine Kommunikation zwischen den einzelnen Clients direkt ab. • <i>Ad-Hoc</i>: Ein Access Client kann im Ad-Hoc-Modus als zentrale Schnittstelle zwischen mehreren Endgeräten verwendet werden. Auf diese Weise können Geräte wie Computer und Drucker kabellos miteinander verbunden werden. <p>Wählen Sie den Kanal aus, der verwendet werden soll.</p>
Frequenzband	<p>Wählen Sie das Frequenzband und ggf. den Einsatzbereich des Funkmoduls aus.</p> <p>Für Betriebsmodus = <i>Access-Point</i> oder Betriebsmodus = <i>Access Client</i> und Client-Modus = <i>Ad-Hoc</i></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 und Mode 802.11g) innerhalb oder außerhalb von Gebäuden betrieben. • <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb von Gebäuden betrieben. • <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) außerhalb von Gebäuden betrieben. • <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb oder außerhalb von Gebäuden betrieben. <p>Für Betriebsmodus = <i>Access Client</i> und Client-Modus = <i>Infrastruktur</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2,4 und 5 GHz</i>: Ihr Gerät wird mit 2,4 (Mode 802.11b und Mode 802.11g) oder 5 GHz (Mode 802.11a/h) betrieben. • <i>5 GHz</i> (Standardwert): Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) betrieben. • <i>2,4 GHz</i>: Ihr Gerät wird mit 2.4 GHz (Mode 802.11b und Mode 802.11g) betrieben.

Feld	Beschreibung
Nutzungsbereich	<p>Nur für Betriebsmodus = <i>Access Client</i>, Client-Modus = <i>Infrastruktur</i> und Frequenzband = 2,4 und 5 GHz oder 5 GHz</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Indoor-Outdoor</i> (Standardwert) • <i>Indoor</i> • <i>Outdoor</i>
IEEE 802.11d-Konformität	<p>Nur für Betriebsmodus = <i>Access Client</i></p> <p>Wählen Sie aus, wie die Länderinformation ermittelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Flexibel</i> (Standardwert): Es wird versucht, die Länderinformation des Access Points zu ermitteln, ansonsten wird die eigene Länderinformation verwendet. • <i>Keine</i>: Die eigene Länderinformation wird verwendet. • <i>Strikt</i>: Die Länderinformation des Access Points wird verwendet.
Kanal	<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 4 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 Clients diese Kanäle auch unterstützen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</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> und <i>5,8 GHz Outdoor</i> <p>Hier ist nur die Option <i>Auto</i> möglich.</p> <p>Access Client Modus:</p> <p>Im Access Client Modus können Sie nur im Client-Modus = <i>Ad-Hoc</i> den erforderlichen Kanal auswählen.</p> <p>Mögliche Werte:</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> und <i>5,8 GHz Outdoor</i> <p>Hier ist nur die Option <i>Auto</i> möglich.</p>
Ausgewählter Kanal	Zeigt den verwendeten Kanal an.
Zweiter Verwendeter Kanal	<p>Nicht für Betriebsmodus = <i>Access-Point</i> und Frequenzband = <i>2,4 GHz In/Outdoor</i></p> <p>Zeigt den zweiten verwendeten Kanal an.</p>
Bandbreite	<p>Nur für Drahtloser Modus = <i>802.11b/g/n, 802.11g/n, 802.11n, 802.11a/n</i></p> <p>Wählen Sie aus, wie viele Kanäle verwendet werden sollen.</p>

Feld	Beschreibung
	<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 Kontroll-Kanal und der andere als Erweiterungs-Kanal.
<p>Anzahl der Spatial Streams</p>	<p>Nur für Drahtloser Modus = <i>802.11b/g/n, 802.11g/n, 802.11n, 802.11a/n</i></p> <p>Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>3</i>: Drei Datenströme werden verwendet. • <i>2</i>: Zwei Datenströme werden verwendet. • <i>1</i>: Ein Datenstrom wird verwendet.
<p>Sendeleistung</p>	<p>Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die tatsächlich abgestrahlte Antennenleistung kann abhängig von der übertragenen Datenrate auch niedriger liegen als der eingestellte Maximalwert. Der Maximalwert der verfügbaren Sendeleistung ist länderspezifisch.</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>

Felder im Menü Performance-Einstellungen

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

Feld	Beschreibung
	<p>Nur 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>Im Betriebsmodus <i>Access Client</i> mit Client-Modus <i>Ad-Hoc</i> stehen zusätzliche Optionen für Frequenzband = 5 GHz <i>Indoor</i>, 5 GHz <i>Outdoor</i>, 5 GHz <i>In/Outdoor</i>, 5,8 GHz <i>Outdoor</i> zur Verfügung</p> <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. • <i>802.11a/b/g/n</i> (nur Anzeige): Nur im Betriebsmodus <i>Access Client</i> mit Client-Modus <i>Infrastruktur</i>.

Feld	Beschreibung
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 aktiviert.</p> <p>Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion deaktiviert werden.</p>
Airtime Fairness	<p>Diese Funktion ist nicht für alle Geräte verfügbar.</p> <p>Mit der Airtime Fairness -Funktion wird gewährleistet, dass Senderressourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.</p>

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

Felder im Menü Erweiterte Einstellungen für Betriebsmodus = Access-Point

Feld	Beschreibung
Kanalplan	Nur für Betriebsmodus = <i>Access-Point</i> und Kanal = <i>Auto</i>

Feld	Beschreibung
	<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> <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>: Wählen Sie die gewünschten Kanäle selbst aus.
Ausgewählte Kanäle	<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>Nur für Betriebsmodus = <i>Access-Point</i> oder <i>Access Client</i> mit Client-Modus <i>Ad-Hoc</i>.</p> <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>Der Standardwert ist 100 ms.</p>
DTIM Period	<p>Nur für Betriebsmodus = <i>Access-Point</i> oder <i>Access Client</i> mit Client-Modus <i>Ad-Hoc</i>.</p>

Feld	Beschreibung
	<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>Hier wählen Sie aus, wie der RTS/CTS-Mechanismus ein- bzw. ausgeschaltet werden soll.</p> <p>Wählen Sie <i>Benutzerdefiniert</i> aus, können Sie in das Eingabefeld den Schwellwert in Bytes (1 - 2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch unabhängig von der Datenpaketlänge ein- bzw. ausgeschaltet werden, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.</p>
Short Guard Interval	<p>Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.</p>
Short Retry Limit	<p>Geben Sie die maximale Anzahl an Sendeversuchen für ein Frames ein. Dieser Wert muss kürzer oder gleich dem in RTS Threshold definierten Wert sein. Nach dieser Anzahl an Fehlversuchen wird das 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 an Sendeversuchen eines Datenpakets ein. Dieser Wert muss länger sein, als der in RTS Threshold definierte Wert. Nach dieser Anzahl an Fehlversuchen wird das Paket verworfen.</p>

Feld	Beschreibung
	Mögliche Werte sind 1 bis 255. Der Standardwert ist 4.
Fragmentation Thresh- hold	Geben Sie die maximale Größe an, ab der Datenpakete fragmentiert (d. h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert. Möglich Werte sind 256 bis 2346. Der Standardwert ist 2346 Bytes.

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

Erweiterte Einstellungen	
Kanäle scannen	Alle
Roaming-Profil	Normales Roaming
Scan-Schwelle	-70 dBm
Scan-Intervall	5000 ms
Channel Sweep	2
Min. Zeitraum aktiver Scan	10 ms
Max. Zeitraum aktiver Scan	40 ms
Min. Zeitraum passiver Scan	20 ms
Max. Zeitraum passiver Scan	120 ms
RTS Threshold	Immer inaktiv
Short Guard Interval	<input checked="" type="checkbox"/> Aktiviert
Short Retry Limit	7
Long Retry Limit	4
Fragmentation Threshold	2346 Bytes

Abb. 71: Wireless LAN->WLAN->Einstellungen Funkmodul->Erweiterte Einstellungen für Betriebsmodus *Access Client*

Felder im Menü Erweiterte Einstellungen für Access Client Modus

Feld	Beschreibung
Kanäle scannen	Wählen Sie aus, auf welchen Kanälen der WLAN-Client automatisch nach verfügbaren Drahtlosnetzwerken scannen soll.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Damit wird auf allen Kanälen gescannt. • <i>Auto</i>: Der Kanal wird automatisch ausgewählt. • <i>Benutzerdefiniert</i>: Damit können die gewünschten Kanäle manuell festgelegt werden.
Benutzerdefinierter Kanalplan	<p>Nur für Kanäle scannen = <i>Benutzerdefiniert</i></p> <p>Legen Sie fest, auf welchen Kanälen der WLAN-Client nach verfügbaren Drahtlosnetzwerken scannen soll.</p>
Roaming-Profil	<p>Wählen Sie das Roaming-Profil aus. Die zur Verfügung stehende Optionen fassen typische Roaming-Funktionen zusammen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnelles Roaming</i>: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, sobald das Funksignal der bestehenden Funkverbindung für höhere Datenraten ungeeignet ist. • <i>Normales Roaming</i> (Standardwert): Standard-Roaming. • <i>Langsames Roaming</i>: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, sobald das Funksignal der bestehenden Funkverbindung schwächer wird. • <i>Kein Roaming</i>: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, wenn er nicht mit einem Drahtlosnetzwerk verbunden ist. • <i>Benutzerdefiniertes Roaming</i>: Legen Sie individuelle Roaming-Parameter fest.
Scan-Schwelle	<p>Zeigt an, ab welchem Wert in dBm im Hintergrund nach verfügbaren Drahtlosnetzwerken gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>-70 dBm</i>.</p>
Scan-Intervall	<p>Zeigt an, in welchen Abständen in Millisekunden nach verfügbaren Drahtlosnetzwerken gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>5000</i></p>

Feld	Beschreibung
	<i>ms.</i>
Channel Sweep	<p>Zeigt an, wie viele Frequenzen im Hintergrund gescannt werden sollen.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefinier-tes Roaming</i> verändert werden. Der Standardwert ist 2. Der Wert 0 deaktiviert den Scan im Hintergrund. Der Wert -1 aktiviert den Scan aller verfügbarer Frequenzen.</p>
Min. Zeitraum aktiver Scan	<p>Zeigt die minimale, aktive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefinier-tes Roaming</i> verändert werden. Der Standardwert ist 10 <i>ms.</i></p>
Max. Zeitraum aktiver Scan	<p>Zeigt die maximale, aktive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefinier-tes Roaming</i> verändert werden. Der Standardwert ist 40 <i>ms.</i></p>
Min. Zeitraum passiver Scan	<p>Zeigt die minimale, passive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefinier-tes Roaming</i> verändert werden. Der Standardwert ist 20 <i>ms.</i></p>
Max. Zeitraum passiver Scan	<p>Zeigt die maximale, passive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefinier-tes Roaming</i> verändert werden. Der Standardwert ist 120 <i>ms.</i></p>
RTS Threshold	<p>Wählen Sie aus, wie der RTS/CTS-Mechanismus ein- bzw. ausgeschaltet werden soll.</p> <p>Wählen Sie <i>Benutzerdefiniert</i> aus, können Sie in dem Eingabefeld den Schwellwert in Bytes (1 - 2346) angegeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch unabhängig von der Datenpaketlänge ein- bzw. ausgeschaltet wer-</p>

Feld	Beschreibung
	den, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.
Short Guard Interval	Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
Short Retry Limit	<p>Geben Sie die maximale Anzahl an Sendeversuchen für einen Frame ein. Dieser Wert muss kleiner oder gleich dem in RTS Threshold definierten Wert sein. Nach dieser Anzahl an Fehlversuchen wird das 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 an Sendeversuchen für ein Datenpaket ein. Dieser Wert muss größer als der in RTS Threshold definierte Wert sein. Nach dieser Anzahl an Fehlversuchen wird das Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 4.</p>
Fragmentation Threshold	<p>Geben Sie maximale Größe 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 Bytes.</p>

10.1.2 Drahtlosnetzwerke (VSS)

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



Hinweis

Das voreingestellte Drahtlosnetzwerk default verfügt im Auslieferungszustand über folgende Sicherheitseinstellungen:

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

Einstellen von Netzwerknamen

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

Absicherung von Funknetzwerken

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

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

WEP

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

IEEE 802.11i

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

WPA

WPA (Wi-Fi Protected Access) bietet zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern PSK (Pre-Shared-Keys) oder Extensible Authentication Protocol (EAP) über 802.1x (z. B. RADIUS) an.

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

WPA 2

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

Zugangskontrolle

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

reless LAN haben dürfen. Alle anderen Clients haben keinen Zugriff.

Sicherheitsmaßnahmen

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

- Ändern Sie die Zugangspasswörter Ihres Geräts.
- Ändern Sie die Standard-SSID, **Netzwerkname (SSID)** = *default*, Ihres Access Points. Setzen Sie **Sichtbar** = *Aktiviert*. Damit werden alle WLAN-Clients ausgeschlossen, die mit dem allgemeinen Wert für **Netzwerkname (SSID)** *Beliebig* einen Verbindungsaufbau versuchen und welche die eingestellten SSIDs nicht kennen.
- Nutzen Sie die zur Verfügung stehenden Verschlüsselungsmethoden. Wählen Sie dazu **Sicherheitsmodus** = *WEP 40*, *WEP 104*, *WPA-PSK* oder *WPA-Enterprise* und tragen Sie den entsprechenden Schlüssel im Access Point unter **WEP-Schlüssel 1 - 4** bzw. **Preshared Key** sowie in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmäßig geändert werden. Wechseln Sie dazu den **Übertragungsschlüssel**. Wählen Sie den längeren 104-Bit-WEP-Schlüssel.
- Für die Übertragung von extrem sicherheitsrelevanten Informationen sollte der **Sicherheitsmodus** = *WPA-Enterprise* mit **WPA-Modus** = *WPA 2* konfiguriert werden. Diese Methode beinhaltet eine hardwarebasierte Verschlüsselung und RADIUS-Authentifizierung des Clients. In Sonderfällen ist auch eine Kombination mit IPSec möglich.
- Beschränken Sie den Zugriff im WLAN auf zugelassene Clients. Tragen Sie die MAC-Adressen der Funknetzwerkkarten dieser Clients in die **Erlaubte Adressen**-Liste im Menü **MAC-Filter** ein (siehe *Felder im Menü MAC-Filter* auf Seite 191).

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

10.1.2.1 Bearbeiten oder Neu

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

Einstellungen Funkmodul
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	<div style="border: 1px solid #ccc; padding: 2px;"> <input type="text" value="MAC-Adresse"/> </div> <input type="button" value="Hinzufügen"/>

Abb. 72: Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)->->Neu

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

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	<p>Geben Sie den Namen des Wireless Netzwerks (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>
ARP Processing	<p>Wählen Sie aus, ob die Funktion ARP Processing aktiv sein</p>

Feld	Beschreibung
	<p>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 in Zusammenhang 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 verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p> <p>Mögliche Werte sind ganze Zahlen von 1 bis 254.</p> <p>Der Standardwert ist 32.</p>

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	<p>Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <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>: 802.11i/TKIP
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel <1 - 4> 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>wep1</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 WPA 2 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 und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): AES wird angewendet. • <i>AES und TKIP</i>: AES oder TKIP werden angewendet.
<p>WPA2 Cipher</p>	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA 2</i> und <i>WPA und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA 2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): AES wird angewendet. • <i>AES und TKIP</i>: AES oder TKIP werden angewendet.
<p>Preshared Key</p>	<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> <div data-bbox="539 935 1315 1123" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Hinweis</p> <p>Ändern Sie unbedingt den Standard Preshared Key! Solange der Schlüssel nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p> </div>
<p>EAP-Vorabauthentifizierung</p>	<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
Zugriffskontrolle	<p>Wählen Sie aus, ob für dieses Wireless Netzwerk 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>

10.1.3 WDS-Links

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



Wichtig

Der WDS Link ist nur im 2.4 GHz und im 5 GHz Band Indoor konfigurierbar wenn der Kanal NICHT *Auto* ist.

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

WDS Links (WDS = Wireless Distribution System) sind statische Links zwischen Access Points (AP), welche im allgemeinen dazu genutzt werden, Clients mit Netzen zu verbinden, die für diese nicht direkt erreichbar sind, z. B. wegen zu großer Entfernung. Der Access Point sendet dabei Daten des einen Client zu einem weiteren Access Point, der dann die Daten an den anderen Client weiterleitet.



Wichtig

Beachten Sie, dass die Daten zwischen den Access Points in der Standardkonfiguration über den WDS-Link unverschlüsselt übertragen werden. Daher wird dringend empfohlen, eine der zur Verfügung stehenden Sicherheitsmethoden (**WEP 40** bzw. **WEP 104**) anzuwenden, um die Daten auf WDS-Links abzusichern.

WDS Links werden als Interfaces mit dem Präfix *WDS* konfiguriert. Sie verhalten sich wie VSS-Schnittstellen und unterscheiden sich von diesen nur durch vordefiniertes Routing. Ein WDS Link wird als Transfernetzwerk definiert: es handelt sich um eine Punkt-zu-Punkt-Verbindung oder eine Punkt-zu-Mehrpunkt-Verbindung zwischen zwei Access Points, die in verschiedene Netzwerke eingebunden sind.

10.1.3.1 Bearbeiten oder Neu

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



Abb. 73: **Wireless LAN->WLAN->WDS-Links->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
WDS-Beschreibung	Geben Sie einen Namen für den WDS-Link ein. Ist die Option <i>Benutze Standard</i> aktiviert, wird der automatisch generierte Name der Schnittstelle übernommen. Ist die Option nicht aktiviert, können Sie einen geeigneten Namen in das Eingabefeld eintragen. Standardmäßig ist die Option <i>Benutze Standard</i> aktiviert.

Felder im Menü WDS-Sicherheitseinstellungen

Feld	Beschreibung
Schutz	Wählen Sie aus, ob und wenn ja welche Verschlüsselungsmethode auf diesem WDS Link angewendet werden soll.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Der Datenverkehr auf diesem WDS Link wird nicht verschlüsselt. • <i>WEP 40</i>: Der Datenverkehr auf diesem WDS Link wird mit WEP 40 verschlüsselt. Geben Sie in WEP-Schlüssel 1 bis WEP-Schlüssel 4 die Schlüssel für diesen WDS-Link ein und wählen Sie in Übertragungsschlüssel den Standard-Schlüssel aus. • <i>WEP 104</i>: Der Datenverkehr auf diesem WDS Link wird mit WEP104 verschlüsselt. Geben Sie in WEP-Schlüssel 1 bis WEP-Schlüssel 4 die Schlüssel für diesen WDS-Link ein und wählen Sie in Übertragungsschlüssel den Standard-Schlüssel aus. • <i>WPA</i>: Der Datenverkehr auf diesem WDS Link wird mit WPA verschlüsselt. Geben Sie in Preshared Key den Schlüssel für diesen WDS-Link ein. • <i>WPA 2</i>: Der Datenverkehr auf diesem WDS Link wird mit WPA verschlüsselt. Geben Sie in Preshared Key den Schlüssel für diesen WDS-Link ein.
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel 1 bis WEP-Schlüssel 4 konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Standardwert ist <i>Schlüssel 1</i>.</p>
WEP-Schlüssel 1 bis WEP-Schlüssel 4	<p>Nur für Schutz = <i>WEP 40</i>, <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein. Es gibt zwei Möglichkeiten, einen WEP-Schlüssel einzugeben:</p> <ul style="list-style-type: none"> • Direkte Eingabe in hexadezimaler Form <p>Beginnt die Eingabe mit <i>0x</i>, wird der Generator deaktiviert. Geben Sie eine hexadezimale Zeichenfolge mit exakt der für den gewählten WEP-Modus passenden Zeichenanzahl ein. 10 Zeichen für <i>WEP 40</i> oder 26 Zeichen für <i>WEP 104</i> z. B.</p> <p><i>WEP 40: 0xA0B23574C5, WEP 104: 0x81DC9BDB52D04DC20036DBD831</i></p> <ul style="list-style-type: none"> • Direkte Eingabe von ASCII Zeichen

Feld	Beschreibung
	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>wep1</i> für <i>WEP 104</i> .
Preshared Key	Nur für Schutz = <i>WPA</i> , <i>WPA 2</i> Geben Sie das WPA-Passwort ein. Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.

Felder im Menü Entfernter Partner

Feld	Beschreibung
Entfernte MAC-Adresse	Geben Sie die MAC-Adresse des WDS-Partners ein.

10.1.4 Client Link

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

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

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

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

10.1.4.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Einstellungen Funkmodul
Client Link

Basisparameter	
Netzwerkname (SSID)	<input type="text"/>
Sicherheitseinstellungen	
Sicherheitsmodus	<input type="text" value="Inaktiv"/> ▼
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 74: Wireless LAN->WLAN->Client Link->

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

Felder im Menü Basisparameter

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

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: <ul style="list-style-type: none"> <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung <i>WEP 40</i>: WEP 40 Bit <i>WEP 104</i>: WEP 104 Bit <i>WPA None</i>: Nur für Client-Modus = Ad-Hoc. WPA None <i>WPA-PSK</i>: Nur für Client-Modus = Infrastruktur. WPA Preshared Keys
Übertragungsschlüssel	Nur für Sicherheitsmodus = WEP 104 Wählen Sie einen der in WEP-Schlüssel <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus. Standardwert ist <i>Schlüssel 1</i> .
WEP-Schlüssel 1 - 4	Nur für Sicherheitsmodus = WEP 40, WEP 104

Feld	Beschreibung
	<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>wep1</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Wählen Sie aus, ob Sie WPA oder WPA 2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> (Standardwert): Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 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>
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA</i></p> <p>Wählen Sie aus welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): Temporal Key Integrity Protocol • <i>AES</i>: Advanced Encryption Standard. <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.</p>
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA 2</i></p> <p>Wählen Sie aus, welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): Advanced Encryption Standard. • <i>TKIP</i>: Temporal Key Integrity Protocol

Feld	Beschreibung
	Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.

10.1.4.2 Client Link Scan

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

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

Einstellungen Funkmodul Client Link

Scan						
Beschreibung des Client Links		sta1-0				
Aktion		[Scan]				
AP-MAC-Adresse	Netzwerkname (SSID)	Kanal	Modus	Signal	Verbunden	Aktion
02:6f:83:3a:c5:b8	bla1	13	Access-Point, WPA and WPA 2 PSK	-86 dBm		[Auswählen]
02:6f:83:3a:ab:50	bla2	2	Access-Point, WPA and WPA 2 PSK	-92 dBm		[Auswählen]

Zurück

Abb. 75: **Wireless LAN->WLAN->Client Link->Scan**

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

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

Felder im Menü Scan

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des von Ihnen konfigurierten Client-Links an.
Aktion	Lösen Sie den Scan durch Klicken von Scan aus. Bei sachgerechter Installation der Antennen auf beiden Seiten und freier LOS wird der Client verfügbare Clients finden und in der folgenden Liste anzeigen.

Feld	Beschreibung
	Sollte die Partner-Client nicht gefunden werden, überprüfen Sie die Line-of-Sight und die Antenneninstallation. Führen Sie dann erneut Scan aus. Der Partner sollte daraufhin gefunden werden.
AP-MAC-Adresse	Zeigt die MAC-Adresse der entfernten Clients an.
Netzwerkname (SSID)	Zeigt den Namen der entfernten Clients an.
Kanal	Zeigt den Kanal an, der verwendet worden ist.
Modus	Zeigt den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes an.
Signal	Zeigt die Signalstärke des erkannten Client-Links in dBm an.
Verbunden	Zeigt den Status des Links auf Ihrem Client an.
Aktion	Sie können den Status der Client-Links verändern. In diesem Feld werden die zur Verfügung stehenden Aktionen angezeigt.

10.2 Verwaltung

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

10.2.1 Grundeinstellungen

The screenshot shows a dialog box titled "Grundeinstellungen". Inside the dialog, there is a section labeled "WLAN Administration" which contains a "Region" dropdown menu currently set to "Germany". Below the main content area, there are two buttons: "OK" and "Abbrechen".

Abb. 76: **Wireless LAN->Verwaltung->Grundeinstellungen**

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

Felder im Menü WLAN Administration

Feld	Beschreibung
Region	Wählen Sie das Land, in welchem der Access Point betrieben werden soll.

Feld	Beschreibung
	<p>Mögliche Werte sind alle auf dem Wireless-Modul des Geräts vorkonfigurierten Länder.</p> <p>Der Bereich der auswählbaren Kanäle (Kanal im Menü Wireless LAN->WLAN->Einstellungen Funkmodul) variiert je nach Ländereinstellung.</p> <p>Standardwert ist <i>Germany</i>.</p>

Kapitel 11 Netzwerk

11.1 Routen

Standard-Route (Default Route)

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

11.1.1 Konfiguration von IPv4-Routen

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

11.1.1.1 Bearbeiten oder Neu

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

Konfiguration von IPv4-Routen		IPv4-Routing-Tabelle	Optionen
Basisparameter			
Routentyp	Netzwerkroute via Schnittstelle		
Schnittstelle	Keine		
Routenklasse	<input checked="" type="radio"/> Standard <input type="radio"/> Erweitert		
Routenparameter			
Ziel-IP-Adresse/Netzmaske	/		
Lokale IP-Adresse	0.0.0.0		
Metrik	1		
OK		Abbrechen	

Abb. 77: Netzwerk->Routen->Konfiguration von IPv4-Routen ->Neu mit Erweiterte Route = Standard.

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

Konfiguration von IPv4-Routen		IPv4-Routing-Tabelle	Optionen
Basisparameter			
Routentyp	Netzwerkroute via Schnittstelle		
Schnittstelle	Keine		
Routenklasse	<input type="radio"/> Standard <input checked="" type="radio"/> Erweitert		
Routenparameter			
Ziel-IP-Adresse/Netzmaske	/		
Lokale IP-Adresse	0.0.0.0		
Metrik	1		
Erweiterte Routenparameter			
Beschreibung			
Quellschnittstelle	Beliebig		
Quell-IP-Adresse/Netzmaske	0.0.0.0 / 0.0.0.0		
Layer 4-Protokoll	Beliebig		
Quell-Port	Beliebig Port bis Port		
Zielport	Beliebig Port bis Port		
DSCP-/TOS-Wert	Nicht beachten		
Modus	Wählen und warten		
OK		Abbrechen	

Abb. 78: Netzwerk->Routen->Konfiguration von IPv4-Routen ->Neu mit Erweitert = Aktiviert

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

Feld im Menü Basisparameter

Feld	Beschreibung
Routentyp	<p>Wählen Sie die Art der Route aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standardroute über Schnittstelle</i>: Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist. • <i>Standardroute über Gateway</i>: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist. • <i>Host-Route über Schnittstelle</i>: Route zu einem einzelnen Host über eine spezifische Schnittstelle. • <i>Host-Route via Gateway</i>: Route zu einem einzelnen Host über ein spezifisches Gateway. • <i>Netzwerkroute via Schnittstelle</i> (Standardwert): Route zu einem Netzwerk über eine spezifische Schnittstelle. • <i>Netzwerkroute via Gateway</i>: Route zu einem Netzwerk über ein spezifisches Gateway. <p>Nur für Schnittstellen, die im DHCP-Client-Modus betrieben werden:</p> <p>Auch wenn eine Schnittstelle für den DHCP-Client-Betrieb konfiguriert ist, ist es möglich, Routen für den Datenverkehr über diese Schnittstelle zu konfigurieren. Die vom DHCP-Server erhaltenen Einstellungen werden dann mit den hier konfigurierten gemeinsam in die aktive Routing-Tabelle übernommen. Dadurch ist es z. B. möglich, bei dynamisch wechselnden Gateway-Adressen bestimmte Routen aufrecht zu erhalten oder Routen mit unterschiedlicher Metrik (d. h. unterschiedlicher Priorität) festzulegen. Wenn der DHCP-Server allerdings statische Routen (sog. Classless Static Routes) übermittelt, werden die hier konfigurierten Einstellungen nicht ins Routing übernommen.</p> <ul style="list-style-type: none"> • <i>Vorlage für Standardroute per DHCP</i>: Die Routing-Informationen werden vollständig vom DHCP-Server übernommen. Lediglich erweiterte Parameter können zusätzlich konfiguriert werden. Diese Route bleibt von weiteren für diese

Feld	Beschreibung
	<p>Schnittstelle angelegten Routen unverändert und wird parallel mit diesen in die Routing-Tabelle übernommen.</p> <ul style="list-style-type: none"> • <i>Vorlage für Host-Route per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Host ergänzt. • <i>Vorlage für Netzwerkroute per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Netzwerk ergänzt.
	<p> Hinweis</p> <p>Durch dem Ablauf des DHCP Leases oder durch einen Neustart des Geräts werden die Routen, die aus der Kombination von DHCP- und hier vorgenommenen Einstellungen entstehen, zunächst wieder aus dem aktiven Routing gelöscht. Mit einer erneuten DHCP-Konfiguration werden sie dann neu generiert und wieder aktiviert.</p>
Schnittstelle	Wählen Sie die Schnittstelle aus, welche für diese Route verwendet werden soll.
Routenklasse	<p>Wählen Sie die Art der Routenklasse aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i>: Definiert eine Route mit den Standardparametern. • <i>Erweitert</i>: Wählen Sie aus, ob die Route mit erweiterten Parametern definiert werden soll. Ist die Funktion aktiv, wird eine Route mit erweiterten Routing-Parametern wie Quell-Schnittstelle und Quell-IP-Adresse sowie Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und der Status der Geräte-Schnittstelle angelegt.

Felder im Menü Routenparameter

Feld	Beschreibung
Lokale IP-Adresse	Nur für Routentyp = <i>Standardroute über Schnittstelle, Host-Route über Schnittstelle oder Netzwerkroute via Schnittstelle</i>

Feld	Beschreibung
	Geben Sie die IP-Adresse des Hosts ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Ziel-IP-Adresse/Netzmaske	Nur für Routentyp <i>Host-Route über Schnittstelle</i> oder <i>Netzwerkroute via Schnittstelle</i> Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein. Bei Routentyp = <i>Netzwerkroute via Schnittstelle</i> Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.
Gateway-IP-Adresse	Nur für Routentyp = <i>Standardroute über Gateway, Host-Route via Gateway</i> oder <i>Netzwerkroute via Gateway</i> Geben Sie die IP-Adresse des Gateways ein, an den Ihr Gerät die IP-Pakete weitergeben soll.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von 0 bis 15. Standardwert ist 1.

Felder im Menü Erweiterte Routenparameter

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

Feld	Beschreibung
	Standardwert ist <i>Beliebig</i> .
Quell-Port	<p>Nur für Layer 4-Protokoll = <i>TCP</i> oder <i>UDP</i></p> <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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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>
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>

Feld	Beschreibung
Modus	<p>Wählen Sie aus, wann die in Routenparameter->Schnittstelle definierte Schnittstelle benutzt werden soll.</p> <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", dann wählen und warten, 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", dann wählen und solange die Alternative Route benutzen (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 wählen und warten, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

11.1.2 IPv4-Routing-Tabelle

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

[Konfiguration von IPv4-Routen](#)
[IPv4-Routing-Tabelle](#)
[Optionen](#)

Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp	Erweiterte Route	Protokoll	
0.0.0.0	0.0.0.0	10.0.0.232	BRIDGE_BR0	1	Standardroute über Gateway	<input type="checkbox"/>	Lokal	
10.0.0.0	255.255.255.0	10.0.0.1	BRIDGE_BR0	0	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	Lokal	

Seite: 1, Objekte: 1 - 2

Abb. 79: **Netzwerk**->**Routen**->**IPv4-Routing-Tabelle**

Felder im Menü IPv4-Routing-Tabelle

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

11.1.3 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.

Konfiguration von IPv4-Routen
IPv4-Routing-Tabelle
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	br0	<input type="checkbox"/> Aktiviert

Seite: 1, Objekte: 1 - 1

OK
Abbrechen

Abb. 80: 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>

Feld	Beschreibung
	<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>

11.2 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in *NAT-Konfiguration* auf Seite 211).

11.2.1 NAT-Schnittstellen

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



Abb. 81: **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	<p>Wählen Sie aus, ob NAT für die Schnittstelle aktiviert werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Loopback aktiv	<p>Mithilfe der NAT-Loopback-Funktion ist Network Address Translation auch bei Anschlüssen möglich, auf denen NAT nicht aktiv ist. Dies wird verwendet, um Anfragen aus dem LAN so zu interpretieren, als ob sie aus dem WAN kämen. Sie können damit Server Services testen.</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 gleichzeitiger 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>

11.2.2 NAT-Konfiguration

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

11.2.2.1 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. 82: 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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>exklusiv (ohne NAT)</i>: Der Datenverkehr, der von NAT ausgenommen ist.
NAT-Methode	<p>Nur für Art des Datenverkehrs = <i>ausgehend (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 (Quell-NAT)</i> und NAT-Methode = <i>full-cone, restricted-cone</i> oder <i>port-restricted-cone</i>.</p> <p>Wählen Sie einen der vorkonfigurierten Dienste aus.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Benutzerdefiniert</i> (Standardwert) • <i><Dienstname></i>
Aktion	<p>Nur für Art des Datenverkehrs = <i>exklusiv (ohne NAT)</i></p> <p>Wählen Sie, welche Datenpakete von NAT ausgenommen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ausschließen</i> (Standardwert): Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) übereinstimmen, werden von NAT ausgenommen. • <i>Nicht ausschließen</i>: Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) nicht übereinstimmen, werden von NAT ausgenommen.
Protokoll	<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</i> oder <i>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>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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> • <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 ur-</p>

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

Feld	Beschreibung
	sprünglichen Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> bedeutet, dass der Port nicht näher spezifiziert ist.

Im Menü **NAT-Konfiguration** ->**Substitutionswerte** können Sie, abhängig davon, ob es sich um eingehenden oder ausgehenden Datenverkehr handelt, neue Adressen und Ports definieren, auf welche bestimmte Adressen und Ports aus dem Menü **NAT-Konfiguration** ->**Ursprünglichen Datenverkehr angeben** umgesetzt werden.

Felder im Menü Substitutionswerte

Feld	Beschreibung
Neue Ziel-IP-Adresse/Netzmaske	Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i> Geben Sie diejenige Ziel-IP-Adresse und die zugehörige Netzmaske ein, auf welche die ursprüngliche Ziel-IP-Adresse umgesetzt werden soll.
Neuer Ziel-Port	Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i> , Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i> Belassen Sie den Ziel-Port oder geben Sie denjenigen Ziel-Port ein, auf den der ursprüngliche Ziel-Port umgesetzt werden soll. 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. Standardmäßig ist <i>Original</i> aktiv.
Neue Quell-IP-Adresse/Netzmaske	Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i> und NAT-Methode = <i>symmetrisch</i> Geben Sie diejenige Quell-IP-Adresse ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.
Neuer Quell-Port	Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i> , NAT-Methode = <i>symmetrisch</i> , Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i> Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-Port ein, auf den der ursprüngliche Quell-Port umgesetzt werden soll.

Feld	Beschreibung
	<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> <p>Haben Sie für Original Quell-Port/Bereich <i>Portbereich angeben</i> gewählt, stehen folgende Auswahlmöglichkeiten zur Verfügung:</p> <ul style="list-style-type: none"> • <i>Original Quell-Port/Bereich verwenden</i>: Der in Original Quell-Port/Bereich angegebene Bereich wird nicht verändert, die Portnummern bleiben erhalten. • <i>Verwende Port/Bereich beginnend bei</i>: Es erscheint ein Eingabefeld, in das Sie die Portnummer eingeben können, bei der der Portbereich beginnen soll, durch den der ursprüngliche Portbereich ersetzt wird. Die Anzahl der Ports bleibt dabei gleich.

11.3 Lastverteilung

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

11.3.1 Lastverteilungsgruppen

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

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

Im Menü **Netzwerk->Lastverteilung->Lastverteilungsgruppen** wird eine Liste aller konfigurierten Lastverteilungsgruppen angezeigt. Mit einem Klick auf das -Symbol neben einem Listeneintrag gelangen Sie zu einer Übersicht diese Gruppe betreffende Grundpara-

meter.



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.

11.3.1.1 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
Hinzufügen			
OK Abbrechen			

Abb. 83: **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 zugewiesen. Die Anzahl der Sessions ist maßgeblich.

Feld	Beschreibung
	<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 **Schnittstelle** fügen Sie Schnittstellen hinzu, die dem aktuellen Gruppenkontext entsprechen und konfigurieren diese. Sie können auch Schnittstellen löschen.

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

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

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

Abb. 84: 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>

11.3.2 Special Session Handling

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

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

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

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

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

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

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

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

11.3.2.1 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 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. 85: 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>

11.4 QoS

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

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen
- Daten klassifizieren
- Daten priorisieren

11.4.1 QoS-Filter

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

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

11.4.1.1 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 ▾

OK
Abbrechen

Abb. 86: **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>

Feld	Beschreibung
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <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 Zielport-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</p>

Feld	Beschreibung
	<p>Quell-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.
<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. Wertebereich 0 bis 7.</p> <p>Der Standardwert ist <i>Nicht beachten</i>.</p>

11.4.2 QoS-Klassifizierung

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

11.4.2.1 Neu

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

The screenshot shows the 'QoS-Klassifizierung' configuration window with the 'Neu' tab selected. The window has three tabs: 'QoS-Filter', 'QoS-Klassifizierung', and 'QoS-Schnittstellen/Richtlinien'. The 'Basisparameter' section contains the following fields:

- Klassenplan:** A dropdown menu with 'Neu' selected.
- Beschreibung:** An empty text input field.
- Filter:** A dropdown menu with 'Eine auswählen' selected.
- Richtung:** A dropdown menu with 'Ausgehend' selected.
- High-Priority-Klasse:** An unchecked checkbox.
- Klassen-ID:** A dropdown menu with '1' selected.
- Setze DSCP/TOS Wert (Layer 3):** A dropdown menu with 'Erhalten' selected.
- Setze CoS Wert (802.1p/Layer 2):** A dropdown menu with 'Erhalten' selected.
- Schnittstellen:** A section with a 'Schnittstelle' label and a 'Hinzufügen' button.

At the bottom of the window are 'OK' and 'Abbrechen' buttons.

Abb. 87: **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="539 269 1320 457" style="border: 1px solid gray; padding: 5px;">  <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>

11.4.3 QoS-Schnittstellen/Richtlinien

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



Hinweis

Daten können nur ausgehend priorisiert werden.

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

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

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

11.4.3.1 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; margin-bottom: 5px;"> <thead> <tr> <th style="font-size: small;">Beschreibung</th> <th style="font-size: small;">Typ</th> <th style="font-size: small;">Klassen-ID</th> <th style="font-size: small;">Priorität</th> <th style="font-size: small;">Bandbreite für Traffic Shaping</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <p style="text-align: center; margin: 0;">Hinzufügen</p>	Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping					
Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping							

OK
Abbrechen

Abb. 88: 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>Nur für Traffic Shaping = aktiviert.</p> <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. <p>Mögliche Werte sind <i>0</i> bis <i>100</i>.</p> <ul style="list-style-type: none"> • <i>Undefiniert</i> (<i>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>

Feld	Beschreibung
Verschlüsselungsmethode	<p>Nur wenn als Schnittstelle ein IPSec Peer gewählt ist, Traffic 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

Feld	Beschreibung
	<p>erkannt wurde.</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • <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

Feld	Beschreibung
	<p>Daten.</p> <ul style="list-style-type: none"> • <i>Standard</i>: Queue für Daten, die nicht klassifiziert wurden 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>

Feld	Beschreibung
Traffic Shaping	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung.</p> <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 den unteren Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 0.</p>
Max. Queue-Größe	<p>Geben Sie den oberen Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 16384.</p>

11.5 Zugriffsregeln

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

Sie definieren Filter für IP-Pakete, um den Zugang von bzw. zu den verschiedenen Hosts in angeschlossenen Netzwerken zu erlauben oder zu sperren. So können Sie verhindern, dass über das Gateway unzulässige Verbindungen aufgebaut werden. Access-Listen definieren die Art des IP-Traffics, den das Gateway annehmen oder ablehnen soll. Die 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 elmeg-Gateway miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access-Listen ein effektives Mittel.

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

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

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

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

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

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

oder

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

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

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

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

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.



Achtung

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

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

11.5.1 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.

Zugriffsfiler Regelketten Schnittstellenzuweisung

Ansicht	20	pro Seite	<<	>>	Filtern in	Keiner	▼	gleich	▼	Los
Index	Beschreibung	Quelle	Ziel	TOS-Dezimalwert						
Seite: 1										
<input type="button" value="Neu"/>										

Abb. 89: **Netzwerk->Zugriffsregeln->Zugriffsfiler**

11.5.1.1 Bearbeiten oder Neu

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

Zugriffsfiler 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. 90: Netzwerk->Zugriffsregeln->Zugriffsfiler->Neu

Das Menü **Netzwerk->Zugriffsregeln->Zugriffsfiler->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>

11.5.2 Regelketten

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

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



Abb. 91: **Netzwerk->Zugriffsregeln->Regelketten**

11.5.2.1 Bearbeiten oder Neu

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

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

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

Abb. 92: 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 zutrifft</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 *über* eine andere Regel dieser Regelkette verschoben wird.

11.5.3 Schnittstellenzuweisung

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

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



Abb. 93: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung**

11.5.3.1 Bearbeiten oder Neu

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

Zugriffsfiler
Regelketten
Schnittstellenzuweisung

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

OK
Abbrechen

Abb. 94: **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	<p>Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll.</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert) : Der Absender wird nicht informiert. • <i>Deaktiviert</i>: Der Absender erhält eine ICMP-Nachricht.
Berichtsmethode	<p>Legen Sie fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll.</p> <p>Mögliche Werte:</p> <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 Pakets wird generiert.

11.6 Drop-In

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

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

11.6.1 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.

11.6.1.1 Neu

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

Drop-In-Gruppen

Basisparameter	
Gruppenbeschreibung	<input type="text"/>
Modus	Transparent ▾
Vom NAT ausnehmen (DMZ)	<input type="checkbox"/> Aktiviert
Netzwerkconfiguration	Statisch ▾
Netzwerkadresse	<input type="text"/>
Netzmaske	<input type="text"/>
Lokale IP-Adresse	<input type="text"/>
ARP Lifetime	3600 Sekunden
DNS-Zuweisung über DHCP	Unverändert ▾
Schnittstellenauswahl	<div style="border: 1px solid gray; padding: 2px;"> Schnittstelle <input type="button" value="Hinzufügen"/> </div>

Abb. 95: **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	<p>Wählen Sie, welcher Modus für die Übermittlung der MAC-Adressen von Netzwerkkomponenten verwendet werden soll.</p> <p>Mögliche Werte:</p> <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.
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>
Netzwerkkonfiguration	<p>Wählen Sie aus, auf welche Weise dem Drop-In-Netzwerk eine IP-Adresse/Netzmaske zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert) • <i>DHCP</i>
Netzwerkadresse	<p>Nur für Netzwerkkonfiguration = <i>Statisch</i></p> <p>Geben Sie die Netzwerkadresse des Drop-In-Netzwerks ein.</p>
Netzmaske	<p>Nur für Netzwerkkonfiguration = <i>Statisch</i></p> <p>Geben Sie die zugehörige Netzmaske ein.</p>
Lokale IP-Adresse	<p>Nur für Netzwerkkonfiguration = <i>Statisch</i></p> <p>Geben Sie die lokale IP-Adresse ein. Diese IP-Adresse muss</p>

Feld	Beschreibung
	für alle Ethernet-Ports eines Netzwerks identisch sein.
DHCP Client an Schnittstelle	<p>Nur für Netzwerkconfiguration = <i>DHCP</i></p> <p>Hier können Sie eine Ethernet-Schnittstelle Ihres Routers wählen, die als DHCP-Client agieren soll.</p> <p>Diese Einstellung benötigen Sie zum Beispiel, wenn der Router 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>
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 12 Routing-Protokolle

12.1 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.

12.1.1 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. 96: **Routing-Protokolle -> RIP -> RIP-Schnittstellen**

12.1.1.1 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. 97: 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.

12.1.2 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. 98: **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.

12.1.2.1 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. 99: 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 .

12.1.3 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. 100: 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).

Kapitel 13 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.

13.1 Allgemein

13.1.1 Allgemein

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

Abb. 101: **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.

13.2 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.

13.2.1 IGMP

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

13.2.1.1 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. 102: 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.

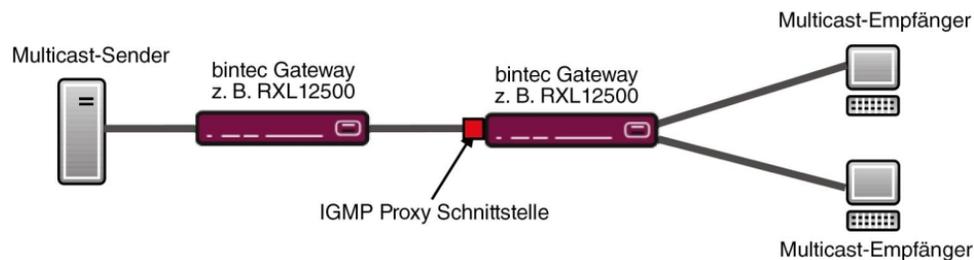


Abb. 103: IGMP Proxy

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>

13.2.2 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. 104: 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 = <i>Aktiv</i> 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>

13.3 Weiterleiten

13.3.1 Weiterleiten

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

13.3.1.1 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. 105: 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	<p>Wählen Sie die Schnittstelle Ihres Geräts aus, an dem die gewünschte Multicast-Gruppe eingeht.</p>
Zielschnittstelle	<p>Wählen Sie die Schnittstelle Ihres Geräts aus, zu der die gewünschte Multicast-Gruppe weitergeleitet werden soll.</p>

Kapitel 14 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.

14.1 Internet + Einwählen

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

Um mit Ihrem Gerät Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner auf Ihrem Gerät einrichten. Dies gilt sowohl für ausgehende Verbindungen (z. B. Ihr Gerät wählt sich bei einem entfernten Partner ein), als auch für eingehende Verbindungen (z. B. ein entfernter Partner wählt sich bei Ihrem Gerät ein).

Wenn Sie einen Internetzugang herstellen wollen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider (ISP) einrichten. Für Breitband-Internetzugänge stellt Ihr Gerät die Protokolle PPP-over-Ethernet (PPPoE), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung. Ein Internetzugang mittels ISDN ist ebenfalls konfigurierbar.



Hinweis

Beachten Sie die Vorgaben Ihres Providers!

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

Alle eingetragenen Verbindungen werden in der entsprechenden Liste angezeigt, welche die **Beschreibung**, den **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
	nicht verbunden (z. B. ist aufgrund eines Fehlers beim Aufbau einer ausgehenden Verbindung ein erneuter Versuch erst nach

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

Authentifizierung

Wenn ein Ruf eingeht, wird über den ISDN-D-Kanal die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann Ihr Gerät den Anrufer identifizieren (CLID), wenn dieser auf Ihrem Gerät eingetragen ist. Nach der Identifizierung mit CLID kann Ihr Gerät zusätzlich eine PPP-Authentisierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird. Dazu benötigt Ihr Gerät Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll, anschließend tragen Sie ein gemeinsames Passwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf Ihrem Gerät eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Default Route

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

NAT aktivieren

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

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

Callback

Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann für jede Verbindung der Callback-Mechanismus verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf zustande, nachdem der Anrufende 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.

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 Gebühren ggf. zu sparen.

Blockieren nach Verbindungsfehler

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

Kanalbündelung

Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. 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.

Statisch

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

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

14.1.1 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.

14.1.1.1 Neu

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

PPPoE
PPTP
PPPoA
ISDN
AUX
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	<input type="password" value="••••••"/>
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	<input type="text" value="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	<input type="text" value="60"/> Sekunden
Maximale Anzahl der erneuten Einwählversuche	<input type="text" value="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
MTU	<input checked="" type="checkbox"/> Automatisch
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 106: **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	<p>Wählen Sie aus, ob Sie eine Standard-Internetverbindung über 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 WAN->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-</p>

Feld	Beschreibung
	Schaltfläche, um weitere Einträge anzulegen.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
VLAN	Einige Internet Service Provider erfordern eine VLAN-ID. Aktivieren Sie diese Funktion, um unter VLAN-ID einen Wert eingeben zu können.
VLAN-ID	Nur wenn VLAN aktiviert ist. Geben Sie die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	Nur wenn Immer aktiv deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold. Standardwert ist 300. Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.

Feld	Beschreibung
	<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	<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.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Standardwert ist <i>60</i> .
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind <i>0</i> bis <i>100</i> . Der Standardwert ist <i>5</i> .
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: <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	Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

Feld	Beschreibung
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 auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
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>

14.1.2 PPTP

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

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

14.1.2.1 Neu

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

Basisparameter	
Beschreibung	<input type="text"/>
PPTP-Ethernet-Schnittstelle	Eine auswählen ▼
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
PPTP-Adressmodus	Statisch
Lokale PPTP-IP-Adresse	10.0.0.140
Entfernte PPTP-IP-Adresse	10.0.0.138
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 107: WAN->Internet + Einwählen->PPTP->Neu

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

Felder im Menü **Basisparameter**

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

Feld	Beschreibung
	<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 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 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>

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 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 Primärer DNS-Server und Sekundärer DNS-Server 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>

14.1.3 PPPoA

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

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

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

werden.

14.1.3.1 Neu

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

Basisparameter	
Beschreibung	<input type="text"/>
ATM PVC	Eine auswählen ▾
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. 108: WAN->Internet + Einwählen->PPPoA->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
ATM PVC	Wählen Sie ein im Menü ATM->Profile angelegtes ATM-Profil, dargestellt durch die vom Provider vorgegebenen globalen ID

Feld	Beschreibung
	VPI und VCI.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort für die PPPoA-Verbindung ein.
Immer aktiv	<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 den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen soll.</p> <p>Mögliche Werte sind 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold.</p> <p>Der Standardwert ist 300.</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihr Gerät eine statische IP-Adresse hat oder diese dynamisch erhält.</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	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.

Feld	Beschreibung
	<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>Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.</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. 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 sind 0 bis 100.</p>

Feld	Beschreibung
	Standardwert ist 5.
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 Primärer DNS-Server und Sekundärer DNS-Server 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-	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch

Feld	Beschreibung
Erreichbarkeitsprüfung	<p>Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Diese 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>

14.1.4 ISDN

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

In diesem Menü konfigurieren Sie folgende ISDN-Verbindungen:

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

14.1.4.1 Neu

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

<input type="button" value="PPPoE"/> <input type="button" value="PPTP"/> <input type="button" value="PPPoA"/> <input checked="" type="button" value="ISDN"/> <input type="button" value="AUX"/> <input type="button" value="IP Pools"/>							
Basisparameter							
Beschreibung	<input type="text"/>						
Verbindungstyp	ISDN 64 kbit/s <input type="button" value="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"> <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 <input type="button" value="v"/></td> </tr> </tbody> </table> <input type="button" value="Hinzufügen"/>	Entfernte IP-Adresse	Netzmaske	Metrik	<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>
Entfernte IP-Adresse	Netzmaske	Metrik					
<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>					
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 <input type="button" value="v"/>						
Callback-Modus	<input checked="" type="radio"/> Keiner <input type="radio"/> Aktiv <input type="radio"/> Passiv						
Optionen für Bandbreite auf Anforderung							
Kanalbündelung	Keine <input type="button" value="v"/>						
Wahlnummern							
Einträge	<table border="1"> <thead> <tr> <th>Modus</th> <th>Rufnummer</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table> <input type="button" value="Hinzufügen"/>	Modus	Rufnummer	<input type="text"/>	<input type="text"/>		
Modus	Rufnummer						
<input type="text"/>	<input type="text"/>						
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. 109: 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	Geben Sie die Kennung Ihres Geräts (lokaler PPP-Benutzername) ein.
Entfernter Benutzer (nur Einwahl)	Geben Sie die Kennung der Gegenstelle (entfernter PPP-Benutzername) ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<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 Nutzdatenpakets und Abbau der Verbindung vergehen sollen.</p>

Feld	Beschreibung
	<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>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Weisen Sie der ISDN-Schnittstelle die IP-Adresse aus Ihrem</p>

Feld	Beschreibung
	LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</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). Der Standardwert ist 1.
IP-Zuordnungspool	<p>Nur bei IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>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>.</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>
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 0 bis 100.</p> <p>Der Standardwert ist 5.</p>
Nutzungsart	<p>Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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. MS-STAC für die Verbindung aktiv ist. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p>

Feld	Beschreibung
	<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 Sekunden zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert worden ist. Nur sinnvoll bei CLID. • <i>Windows-Servermodus, Rückruf optional</i>: Wie

Feld	Beschreibung
	<p><i>Windows-Servermodus</i> mit Abbruchoption. Diese Einstellung ist aus Sicherheitsgründen zu vermeiden. Der Microsoft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu Ihrem Gerät ohne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer für den Verbindungspartner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit Abbrechen geschlossen wird.</p>

Felder im Menü Optionen für Bandbreite auf Anforderung

Feld	Beschreibung
<p>Kanalbündelung</p>	<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
<p>Einträge</p>	<p>Fügen Sie weitere Einträge mit Hinzufügen hinzu.</p>

Felder im Menü Konfiguration der Wahlnummern (erscheint nur für Einträge = Hinzufügen)

Feld	Beschreibung
Modus	<p>Nur wenn Einträge = <i>Hinzufügen</i></p> <p>Die Calling Party Number des Rufes wird mit der unter Rufnummer eingetragenen Nummer verglichen. Wählen Sie aus, ob Rufnummer für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte:</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 Nummer des Anrufers eines eingehenden Rufs (Calling Party Number) 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

Feld	Beschreibung
	<p>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.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server und WINS-Server Primär und Sekundär vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

14.1.5 UMTS/LTE



Hinweis

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

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

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

14.1.5.1 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. 110: **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 RS120wu ist das integrierte Modem mit Slot 6 Einheit 0 UMTS vorausgewählt, für Geräte mit optional gestecktem UMTS/LTE-Stick der

Feld	Beschreibung
	USB-Port des Geräts.
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>

Feld	Beschreibung
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.

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 Ih-</p>

Feld	Beschreibung
	<p>rem Provider spezifiziert ist.</p> <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.
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 auf eine Backup-Verbindung umzuschalten.</p>

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

14.1.6 IP Pools

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

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

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adress-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft Ihr Gerät zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann Ihr Gerät eine IP-Adresse aus einem Adress-Pool zuweisen (falls verfügbar). Bei Adress-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher Verbindungspartner welche Adresse bekommt. Die Adressen werden zunächst einfach der Reihe nach vergeben. Bei einer erneuten Einwahl innerhalb eines Intervalls von einer Stunde wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

14.1.6.1 Bearbeiten oder Neu

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

PPPoE PPTP PPPoA ISDN **IP Pools**

Basisparameter	
IP-Poolname	<input type="text"/>
IP-Adressbereich	<input type="text"/> - <input type="text"/>
DNS-Server	Primär <input type="text"/>
	Sekundär <input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 111: WAN->Internet + Einwählen->IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

14.2 ATM

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

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

In einem ATM-Netz können unterschiedliche Anwendungen wie z. B. Sprache, Video und Daten nebeneinander im asynchronen Zeitmultiplexverfahren übertragen werden. Jedem Sender werden dabei Zeitabschnitte zum Übertragen seiner Daten zur Verfügung gestellt. Beim asynchronen Verfahren werden ungenutzte Zeitabschnitte eines Senders von einem anderen Sender verwendet.

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

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

Über ATM werden verschiedene Arten von Datenströmen transportiert. Um den unterschiedlichen Ansprüchen dieser Datenströme an das Netz, z. B. bezüglich Zellverlust und Verzögerungszeit, gerecht zu werden, können mit Hilfe der Dienstkategorien dafür geeig-

nete Werte festgelegt werden. Für unkomprimierte Videodaten werden z. B. andere Parameter benötigt als für zeitunkritische Daten.

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

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

14.2.1 Profile

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

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

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



Hinweis

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

14.2.1.1 Neu

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

Profile Dienstkategorien OAM-Regelung

ATM-Profilparameter							
Provider	-- Benutzerdefiniert --						
Beschreibung	<input type="text"/>						
Typ	Ethernet über ATM						
Virtual Path Identifier (VPI)	8						
Virtual Channel Identifier (VCI)	32						
Encapsulierung	LLC Bridged no FCS						
Einstellungen für Ethernet über ATM							
Standard-Ethernet für PPPoE-Schnittstellen	<input type="checkbox"/> Aktiviert						
Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> DHCP						
IP-Adresse/Netzmaske	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%;">IP-Adresse</td> <td style="width: 50%;">Netzmaske</td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></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"/>	<input type="button" value="Hinzufügen"/>	
IP-Adresse	Netzmaske						
<input type="text"/>	<input type="text"/>						
<input type="button" value="Hinzufügen"/>							
MAC-Adresse	<input type="text"/> <input checked="" type="checkbox"/> Voreingestellte verwenden						
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

Abb. 112: WAN->ATM->Profile->Neu

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

Felder im Menü ATM-Profilparameter

Feld	Beschreibung
Provider	Wählen Sie eines der vorkonfigurierten ATM-Profile für Ihren Provider aus der Liste aus oder definieren Sie mit -- <i>Benutzerdefiniert</i> -- ein Profil.
Beschreibung	Nur für Provider = -- <i>Benutzerdefiniert</i> -- Geben Sie eine beliebige Beschreibung für die Verbindung ein.
ATM-Schnittstelle	Nur, wenn mehrere ATM-Schnittstellen verfügbar sind, z. B. wenn bei Geräten mit SHDSL mehrere Schnittstellen separat konfiguriert sind. Wählen Sie die ATM-Schnittstelle, die Sie für die Verbindung verwenden wollen.
Typ	Nur für Provider = -- <i>Benutzerdefiniert</i> -- Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte:

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Ethernet über ATM</i> (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet. • <i>Geroutete Protokolle über ATM</i>: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) werden geroutete Protokolle über ATM (RPoA) verwendet. • <i>PPP über ATM</i>: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.
Virtual Path Identifier (VPI)	<p>Nur für Provider = -- <i>Benutzerdefiniert</i> --</p> <p>Geben Sie den VPI-Wert der ATM-Verbindung ein. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades. Verwenden Sie die Vorgaben Ihres Providers.</p> <p>Mögliche Werte sind 0 bis 255.</p> <p>Der Standardwert ist 8.</p>
Virtual Channel Identifier (VCI)	<p>Nur für Provider = -- <i>Benutzerdefiniert</i> --</p> <p>Geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten. Verwenden Sie die Vorgaben Ihres Providers.</p> <p>Mögliche Werte sind 32 bis 65535.</p> <p>Der Standardwert ist 32.</p>
Enkapsulierung	<p>Nur für Provider = -- <i>Benutzerdefiniert</i> --</p> <p>Wählen Sie die zu verwendende Enkapsulierung aus. Verwenden Sie die Vorgaben Ihres Providers.</p> <p>Mögliche Werte (nach RFC 2684):</p> <ul style="list-style-type: none"> • <i>LLC Bridged no FCS</i> (Standardwert für Ethernet über ATM): Wird nur für Typ = <i>Ethernet über ATM</i> angezeigt. <p>Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> • <i>LLC Bridged FCS</i>: Wird nur für Typ = <i>Ethernet über</i>

Feld	Beschreibung
	<p><i>ATM</i> angezeigt.</p> <p>Bridged Ethernet mit LLC/SNAP-Encapsulierung mit Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> • <i>Nicht ISO</i> (Standardwert für Geroutete Protokolle über ATM): Wird nur für Typ = <i>Geroutete Protokolle über ATM</i> angezeigt. <p>Encapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing.</p> <ul style="list-style-type: none"> • <i>LLC</i>: Wird nur für Typ = <i>PPP über ATM</i> angezeigt. <p>Encapsulierung mit LLC-Header.</p> <ul style="list-style-type: none"> • <i>VC-Multiplexing</i> (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Encapsulierung (Null Encapsulierung) mit Frame Check Sequence (Prüfsummen).

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

Feld	Beschreibung
Standard-Ethernet für PPPoE-Schnittstellen	<p>Nur für Typ = <i>Ethernet über ATM</i></p> <p>Wählen Sie aus, ob diese Ethernet-over-ATM-Schnittstelle für alle PPPoE-Verbindungen verwendet werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Adressmodus	<p>Nur für Typ = <i>Ethernet über ATM</i></p> <p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen werden soll.</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>

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

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

Feld	Beschreibung
IP-Adresse/Netzmaske	Geben Sie die IP-Adressen (IP-Adresse) und die entsprechenden Netzmasken (Netzmaske) der ATM-Schnittstelle ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

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

Feld	Beschreibung
Client-Typ	<p>Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auf Anforderung</i> (Standardwert): Die PPPoA wird nur bei Bedarf aufgebaut, z. B. für den Internetzugang. <p>Zusätzliche Informationen zu PPP über ATM finden Sie unter PPPoA auf Seite 285.</p>

14.2.2 Dienstkategorien

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

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



Achtung

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

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

14.2.2.1 Neu

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

Profile
Dienstkategorien
OAM-Regelung

Basisparameter	
Virtual Channel Connection (VCC)	VPI8, VCI32 ▾
ATM-Dienstkategorie	Eine auswählen ▾
Peak Cell Rate (PCR)	0 Bit/s
Sustained Cell Rate (SCR)	0 Bit/s
Maximale Burst-Größe (MBS)	0 Bit/s

OK
Abbrechen

Abb. 113: WAN->ATM->Dienstkategorien->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Virtual Channel Connection (VCC)	Wählen Sie die bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus, für welche die Dienstkategorie festgelegt werden soll.
ATM-Dienstkategorie	<p>Wählen Sie aus, auf welche Art der Datenverkehr der ATM-Verbindung geregelt werden soll.</p> <p>Durch die Auswahl der ATM-Dienstkategorie wird implizit eine Priorität zugeordnet: von CBR (höchste Priorität) über VBR.1 / VBR.3 bis VBR (niedrigste Priorität).</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Unspecified Bit Rate (UBR)</i> (Standardwert): Der Verbindung wird keine bestimmte Datenrate garantiert. Die Peak Cell Rate (PCR) legt die Grenze fest, bei deren Überschreiten Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen. • <i>Constant Bit Rate (CBR)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen, die von der Peak Cell Rate (PCR) bestimmt wird. Diese Kategorie eignet sich für kritische Anwendungen (Real-Time), die eine garantierte Datenrate voraussetzen. • <i>Variable Bit Rate V.1 (VBR.1)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen - Sustained Cell Rate (SCR). Diese darf insgesamt um das in Maximale Burst-Größe (MBS) konfigurierte Volumen überschritten werden.

Feld	Beschreibung
	<p>Jeglicher weiterer ATM-Traffic wird verworfen. Die Peak Cell Rate (PCR) bildet dabei die maximal mögliche Datenrate. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen.</p> <ul style="list-style-type: none"> • <i>Variable Bit Rate V.3 (VBR.3)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen - Sustained Cell Rate (SCR). Diese darf insgesamt um das in Maximale Burst-Größe (MBS) konfigurierte Volumen überschritten werden. Weiterer ATM-Traffic wird markiert und je nach Auslastung des Zielnetzes mit niedriger Priorität behandelt, d. h. wird bei Bedarf verworfen. Die Peak Cell Rate (PCR) bildet dabei die maximal mögliche Datenrate. Diese Kategorie eignet sich für kritische Anwendungen mit stoßweisem Datenaufkommen.
Peak Cell Rate (PCR)	<p>Geben Sie einen Wert für die maximale Datenrate in Bits pro Sekunde ein.</p> <p>Mögliche Werte: 0 bis 10000000.</p> <p>Der Standardwert ist 0.</p>
Sustained Cell Rate (SCR)	<p>Nur für ATM-Dienstkategorie = Variable Bit Rate V.1 (VBR.1) oder Variable Bit Rate V.3 (VBR.3)</p> <p>Geben Sie einen Wert für die mindestens zur Verfügung stehende, garantierte Datenrate in Bits pro Sekunde ein.</p> <p>Mögliche Werte: 0 bis 10000000.</p> <p>Der Standardwert ist 0.</p>
Maximale Burst-Größe (MBS)	<p>Nur für ATM-Dienstkategorie = Variable Bit Rate V.1 (VBR.1) oder Variable Bit Rate V.3 (VBR.3)</p> <p>Geben Sie hier einen Wert für die maximale Anzahl in Bits pro Sekunde ein, um welche die PCR kurzzeitig überschritten werden darf.</p> <p>Mögliche Werte: 0 bis 100000.</p> <p>Der Standardwert ist 0.</p>

14.2.3 OAM-Regelung

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



Hinweis

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

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



Achtung

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

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

14.2.3.1 Neu

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

[Profile](#) | [Dienstkategorien](#) | **OAM-Regelung**

OAM-Flusskonfiguration	
OAM-Fluss-Level	F5
Virtual Channel Connection (VCC)	VPI1, VCI32
Loopback	
Loopback Ende-zu-Ende	<input type="checkbox"/> Aktiviert
Loopback-Segment	<input type="checkbox"/> Aktiviert
CC-Aktivierung	
Continuity Check (CC) Ende-zu-Ende	Passiv Richtung: Beide
Continuity Check (CC) Segment	Passiv Richtung: Beide
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 114: WAN->ATM->OAM-Regelung->Neu

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

Felder im Menü OAM-Flusskonfiguration

Feld	Beschreibung
OAM-Fluss-Level	<p>Wählen Sie den zu überwachenden OAM-Fluss-Level.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>F5</i>: (Virtual Channel Level) Die OAM-Einstellungen werden auf den virtuellen Kanal angewendet (Standardwert). • <i>F4</i>: (Virtual Path Level) Die OAM-Einstellungen werden auf den virtuellen Pfad angewendet.
Virtual Channel Connection (VCC)	<p>Nur für OAM-Fluss-Level = <i>F5</i></p> <p>Wählen Sie die zu überwachende bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus.</p>
Virtual Path Connection (VPC)	<p>Nur für OAM-Fluss-Level = <i>F4</i></p> <p>Wählen Sie die zu überwachende bereits konfigurierte Virtual Path Connection (angezeigt durch den VPI) aus.</p>

Felder im Menü Loopback

Feld	Beschreibung
Loopback Ende-	Wählen Sie aus, ob Sie den Loopback-Test für die Verbindung

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

Feld	Beschreibung
	<p>Mögliche Werte sind 1 bis 99.</p> <p>Der Standardwert ist 5.</p>

Felder im Menü CC-Aktivierung

Feld	Beschreibung
Continuity Check (CC) Ende-zu-Ende	<p>Wählen Sie aus, ob Sie den OAM-CC-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • <i>Keine Aushandlung</i>: Je nach Einstellung im Feld Richtung werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine CC-Aushandlung statt. • <i>Passiv</i>: Die Funktion ist nicht aktiv. <p>Wählen Sie außerdem aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • <i>Senke</i>: CC-Daten werden empfangen. • <i>Quelle</i>: CC-Daten werden generiert.
Continuity Check (CC) Segment	<p>Wählen Sie aus, ob Sie den OAM-CC-Test für die Segment-Verbindung (Segment=Verbindung des lokalen Endpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • <i>Keine Aushandlung</i>: Je nach Einstellung im Feld Richtung werden OAM CC Requests entweder gesendet und/oder beantwortet, es findet keine CC-Aushandlung statt. • <i>Keiner</i>: Die Funktion ist nicht aktiv. <p>Wählen Sie weiterhin aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • <i>Senke</i>: CC-Daten werden empfangen. • <i>Quelle</i>: CC-Daten werden generiert.

14.3 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 Sprachdaten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

14.3.1 Regulierte Schnittstellen

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

14.3.1.1 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	0 kbit/s

Abb. 115: 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 Sprachdaten wird nicht durchgeführt. • <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 15 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.

15.1 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 121) integriert werden. Die IPSec-Implementierung erreicht dieses Ziel zum einen durch die Benutzung des Authentication-Header-(AH)-Protokolls und des Encapsulated-Security-Payload-(ESP)-Protokolls. Zum anderen werden kryptografische Schlüsselverwaltungsmechanismen wie das Internet-Key-Exchange-(IKE)-Protokoll verwendet.

Zusätzlicher Filter des Datenverkehrs

bintec elmeg Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der 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.

15.1.1 IPSec-Peers

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

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

zeigt.

IPSec-Peers Phase-1-Profil Phase-2-Profil XAUTH-Profil IP Pools Optionen

IKEv1 (Internet Key Exchange, Version 1)

Ansicht pro Seite << >> Filtern in Keiner gleich Los

Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion

Seite: 1

IKEv2 (Internet Key Exchange, Version 2)

Ansicht pro Seite << >> Filtern in Keiner gleich Los

Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion

Seite: 1

Neu

Abb. 116: 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 519.

15.1.1.1 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	Peer-1													
Peer-Adresse														
Peer-ID	Fully Qualified Domain Name (FQDN) Peer-1.													
IKE (Internet Key Exchange)	IKEv1													
Preshared Key														
Schnittstellenrouten														
IP-Adressenvergabe	Statisch													
Standardroute	<input type="checkbox"/> Aktiviert													
Lokale IP-Adresse														
Routeneinträge	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>1</td> </tr> </tbody> </table> <p>Hinzufügen</p>						Entfernte IP-Adresse	Netzmaske	Metrik			1		
Entfernte IP-Adresse	Netzmaske	Metrik												
		1												
Zusätzlicher Filter des Datenverkehrs														
Zusätzlicher Filter des Datenverkehrs	<table border="1"> <thead> <tr> <th>Beschreibung</th> <th>Protokoll</th> <th>Quell-IP/Maske:Port</th> <th>Ziel-IP/Maske:Port</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Hinzufügen</p>						Beschreibung	Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port				
Beschreibung	Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port											
Erweiterte Einstellungen														
Erweiterte IPSec-Optionen														
Phase-1-Profil	Keines (Standardprofil verwenden)													
Phase-2-Profil	Keines (Standardprofil verwenden)													
XAUTH-Profil	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														
Öffentliche Schnittstelle	Vom Routing ausgewählt													
Öffentlicher Schnittstellenmodus	<input checked="" type="radio"/> Erzwingen <input type="radio"/> Bevorzugt													
Öffentliche Quell-IP-Adresse	<input type="checkbox"/> Aktiviert													
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	Inaktiv													
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>														

Abb. 117: 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	<p>Wählen Sie den Zustand aus, in den Sie den Peer nach dem 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>: Beliebige Zeichenkette • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüssel-ID</i>: Beliebige Zeichenkette <p>Auf dem Peer-Gerät entspricht diese ID dem Parameter Lokaler ID-Wert.</p>
IKE (Internet Key Exchange)	<p>Für Geräte der Wlxxxxn-Serie nicht verfügbar. Diese Geräte unterstützen nur IKEv1.</p>

Feld	Beschreibung
	<p>Wählen Sie die Version des Internet-Key-Exchange-Protokolls, die verwendet werden soll.</p> <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 Zeichenkette
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 Subjektname aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektname aus Zertifikat verwenden</p>

Feld	Beschreibung
	<p>aktivieren, wird der erste im Zertifikat angegebene Subjekt-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 121), 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 <code>0x</code> 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 IKEv1 auswählbar. 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 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 oder 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 oder 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 oder 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 <i>0</i> bis <i>15</i>. Standardwert ist <i>1</i>.</p>
Routeneinträge	<p>Nur für IP-Adressenvergabe = <i>Statisch oder Client im IKE-Konfigurationsmodus</i></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 <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 elmeg Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IP-Sec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IP-Sec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des Datenverkehrs**, so wird es verworfen.

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



Hinweis

Der Parameter **Zusätzlicher Filter des Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.



Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

Fügen Sie weitere Filter mit **Hinzufügen** hinzu.

The screenshot shows the configuration page for an IPSec Peer. The 'Phase-2-Profil' tab is active. A dialog box titled 'Basisparameter' is open, allowing the user to add a new filter. The dialog contains the following fields:

- Beschreibung:** A text input field.
- Protokoll:** A dropdown menu currently set to 'Beliebig'.
- Quell-IP-Adresse/Netzmaske:** A dropdown menu set to 'Netzwerk' followed by two input fields for IP and mask.
- Ziel-IP-Adresse/Netzmaske:** A dropdown menu set to 'Netzwerk' followed by two input fields for IP and mask.

Buttons for 'Übernehmen' and 'Abbrechen' are located at the bottom of the dialog. Below the dialog, the main configuration form shows 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 a table for 'Zusätzlicher Filter des Datenverkehrs' with columns for 'Beschreibung', 'Protokoll', 'Quell-IP/Maske/Port', and 'Ziel-IP/Maske/Port'. A 'Hinzufügen' button is positioned below the table. At the bottom of the page, there are 'Erweiterte Einstellungen', 'OK', and 'Abbrechen' buttons.

Abb. 118: VPN->IPSec->IPSec-Peers->Neu->Hinzufügen

Felder im Menü Basisparameter

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

Feld	Beschreibung
Protokoll	Wählen Sie ein Protokoll aus. Die Option <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.
Quell-Port	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i> 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.
Ziel-Port	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	Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: <ul style="list-style-type: none"> • <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in VPN->IPsec->Phase-1-Profil als Standard markiert ist • <i>Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/

Feld	Beschreibung
	<p>MD5 enthält ungeachtet der Proposalauswahl im Menü VPN->IPSec->Phase-1-Profile.</p> <ul style="list-style-type: none"> • <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 Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü VPN->IPSec->Phase-2-Profile. • <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, wieviele 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. <p>Die Konfiguration des dynamischen Peers darf keine Peer ID und keine Peer-IP-Adresse enthalten. Die Clients, die sich mit dem Gateway verbinden, müssen jedoch über eine Peer</p>

Feld	Beschreibung
	<p>ID verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen.</p> <p>Der resultierende Peer auf dem Gateway würde nun auf alle eingehenden Tunnel-Requests zutreffen. Daher ist es notwendig, ihn an das Ende der IPSec-Peer-Liste zu stellen. Andernfalls wären alle in der Listen folgenden Peers inaktiv.</p>
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
Öffentliche Schnittstelle	<p>Legen Sie diejenige öffentliche (oder WAN-) Schnittstelle fest, über die dieser Peer sich mit seinem VPN-Partner verbinden soll. Wenn Sie <i>Vom Routing ausgewählt</i> auswählen, wird die Entscheidung, über welche Schnittstelle der Datenverkehr geleitet wird, gemäß der aktuellen Routingtabelle getroffen. Wenn Sie eine Schnittstelle auswählen, wird unter Beachtung der Einstellung unter Öffentlicher Schnittstellenmodus diese Schnittstelle verwendet.</p>
Öffentlicher Schnittstellenmodus	<p>Legen Sie fest, wie strikt die Einstellung unter Öffentliche Schnittstelle gehandhabt wird. Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erzwingen</i>: Unabhängig von den Prioritäten der aktuellen Routingtabelle wird nur die ausgewählte Schnittstelle verwendet. • <i>Bevorzugt</i>: In Abhängigkeit der Prioritäten der aktuellen Routingtabelle wird die ausgewählte Schnittstelle dann verwendet, wenn keine günstigere Route über eine andere Schnittstelle vorhanden ist.
Öffentliche Quell-IP-Adresse	<p>Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die Öffentliche Quell-IP-Adresse</p>

Feld	Beschreibung
	<p>aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
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>
MobiKE	<p>Nur für Peers mit IKEv2.</p> <p>MobiKE ermöglicht es, bei wechselnden öffentlichen IP-Adressen lediglich diese Adressen in den SAs zu aktualisieren, ohne die SAs selbst neu aushandeln zu müssen.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Beachten Sie, dass MobiKE einen aktuellen IPSec Client voraussetzt, z. B. den aktuellen Windows-7- oder Windows-8-Client oder die neuste Version des bintec elmeg IPSec Clients.</p>
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

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

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen bintec elmeg-Geräte den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit IPSec-Callback geschaffen: Mithilfe eines direkten ISDN-Rufs bei einem Peer kann diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf von Ihrem Gerät nicht angenommen werden muss. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muss zunächst auf der passiven Seite im Menü **Physikalische Schnittstellen->ISDN-Ports->MSN-Konfiguration->Neu** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld **Dienst** der Wert *IPSec* zur Verfügung. Dieser Eintrag sorgt dafür, dass auf dieser Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Bei aktivem Callback wird, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlasst, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer (**MSN** im Menü **Physikalische Schnittstellen->ISDN-Ports->MSN-Konfiguration->Neu** für **Dienst** *IPSec*) eingeht. Auf diese Weise wird sichergestellt, dass beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt, wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.



Hinweis

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec-Daemon zunächst die Schnittstelle aktiviert, über die der Tunnel realisiert werden soll. Sofern auf dem lokalen Gerät IPSec mit DynDNS konfiguriert ist, wird die eigene IP-Adresse propagiert und erst dann der ISDN-Ruf an das entfernte Gerät abgesetzt. Auf diese Art ist sichergestellt, dass das entfernte Gerät das lokale auch tatsächlich erreichen kann, wenn es den Tunnelaufbau initiiert.

Übermittlung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Geräts über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs. Einschränkungen, die bei der IPSec-Konfiguration mit dynamischen IP-Adressen auftreten, können so umgangen werden.



Hinweis

Um die Funktion IP-Adressübermittlung über ISDN nutzen zu können, müssen Sie eine kostenfreie Zusatzlizenz erwerben.

Die Lizenzdaten der Zusatzlizenzen erhalten Sie über die Online-Lizenzierungs-Seiten im Support-Bereich auf www.bintec-elmeg.com. Bitte folgen Sie den Anweisungen der Online-Lizenzierung.

Vor Systemsoftware Release 7.1.4 unterstützte der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Auslösers auf indirektem Wege (z. B. über DynDNS) ermittelt werden konnte. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse über ISDN umgangen. Darüber hinaus ermöglicht es diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus (Haupt Modus) für den Tunnelaufbau zu verwenden.

Funktionsweise: Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht. Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in *Felder im Menü IPSec-Callback* auf Seite 337 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der

automatischen Auswahl durch das Gerät sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.



Hinweis

Damit Ihr Gerät die Informationen des gerufenen Peers über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Geräten analog vorgenommen werden.

Folgende Rollenverteilungen sind möglich:

- Eine Seite übernimmt die aktive, die andere die passive Rolle.
- Beide Seiten können beide Rollen (Beide) übernehmen.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

- (1) Peer A (der Auslöser des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.
- (2) Ihr Gerät erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden MIB-Eintrag.
- (3) Ihr Gerät setzt den initialen ISDN-Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.
- (4) Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten Calling Party Number (der ISDN-Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.
- (5) Der IPSec-Daemon auf Ihrem Gerät von Peer B kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil des Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.
- (6) Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.



Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Die folgenden Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü IPsec-Callback

Feld	Beschreibung
Modus	<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>
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</p>

Feld	Beschreibung
	das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.
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> <p>Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen.</p>

Feld	Beschreibung
	<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.

15.1.2 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 20 pro Seite << >> Filtern in Keiner gleich Los

Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer

Seite: 1

Neues IKEv1-Profil erstellen Neu

IKEv2 (Internet Key Exchange, Version 2)

Ansicht 20 pro Seite << >> Filtern in Keiner gleich Los

Beschreibung	Proposals	Lebensdauer

Seite: 1

Neues IKEv2-Profil erstellen Neu

OK
Abbrechen

Abb. 119: VPN->IPSec->Phase-1-Profile

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

15.1.2.1 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		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			
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									
OK						Abbrechen					

Abb. 120: 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 Algorithmus mit einer effektiven Schlüssellänge von 112 Bit,

Feld	Beschreibung
	<p>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 elmeg-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>Folgende Optionen stehen für die Definition der Lebensdauer</p>

Feld	Beschreibung
	<p>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>, das bedeutet, dass die Schlüssel erneuert werden, wenn vier Stunden abgelaufen sind. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-1- Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist <i>0</i>; das bedeutet, dass die Anzahl der gesendeten kBytes keine Rolle spielt.
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 Pre Shared 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 Phase-1-Parameter (IKE)</p> <p>Nur für Authentifizierungsmethode = DSA-Signatur, RSA-Signatur oder RSA-Verschlüsselung</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. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>

Feld	Beschreibung
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 Subjektname aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektname 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 121), 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
Erreichbarkeitsprüfung	<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> <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.

Feld	Beschreibung
	<p>Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option.</p> <ul style="list-style-type: none"> • <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>
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>

Feld	Beschreibung
	<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 Phase-1-Parameter (IKE)</p> <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>

15.1.3 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-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [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. 121: VPN->IPSec->Phase-2-Profil

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

15.1.3.1 Neu

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | [XAUTH-Profil](#) | [IP Pools](#) | [Optionen](#)

Phase-2-Parameter (IPSEC)													
Beschreibung	IPSec-2												
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"/>											
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 erneut 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. 122: VPN->IPSec->Phase-2-Profil->Neu

Das Menü **VPN->IPSec->Phase-2-Profil->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 IKE 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 elmeg IPSec-Heartbeat implementiert worden. Dieser sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Automatische Erkennung, ob die Gegenstelle ein bintec elmeg-Gerät ist. Wenn ja, wird <i>Heartbeats (Senden &Erwarten)</i> (bei Gegenstelle mit bintec elmeg) oder <i>Inaktiv</i> (bei Gegenstelle ohne bintec elmeg) 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>

15.1.4 XAUTH-Profil

Im Menü **XAUTH-Profil** wird eine Liste aller XAuth-Profile angezeigt.

Extended Authentication für IPSec (XAuth) ist eine zusätzliche Authentifizierungsmethode für Benutzer eines IPSec-Tunnels.

Das Gateway kann bei Nutzung von XAuth zwei verschiedene Rollen übernehmen, es kann als Server oder als Client dienen:

- Das Gateway fordert als Server einen Berechtigungsnachweis an.
- Das Gateway weist als Client seine Berechtigung nach.

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Die Berechtigung wird entweder anhand einer Liste oder über einen RADIUS Server geprüft. Bei Verwendung eines Einmalpassworts (One Time Password, OTP) kann die Passwortüberprüfung von einem Token-Server übernommen werden (z. B. beim Produkt SecOVID von Kobil), der hinter dem RADIUS-Server installiert ist. Wenn über IPSec eine Firmenzentrale mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden. Je nach Zuordnung verschiedener Profile kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechselnd in verschiedenen Filialen arbeitet, jeder Peer eine Filiale repräsentiert und der Angestellte jeweils vor Ort Zugriff auf den Tunnel haben will.

Nachdem IPSec IKE (Phase 1) erfolgreich beendet ist und bevor IKE (Phase 2) beginnt, wird XAuth realisiert.

Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.

15.1.4.1 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
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 123: 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	<p>Wählen Sie die Rolle des Gateways bei der XAuth-Authentifizierung aus.</p> <p>Mögliche Werte:</p> <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	<p>Nur für Rolle = <i>Server</i></p> <p>Wählen Sie aus, wie die Authentifizierung durchgeführt wird.</p> <p>Mögliche Werte:</p> <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	<p>Nur für Rolle = <i>Client</i></p> <p>Geben Sie den Authentifizierungsnamen des Clients ein.</p>

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.

15.1.5 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.

15.1.5.1 Bearbeiten oder Neu

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

[IPSec-Peers](#) | [Phase-1-Profile](#) | [Phase-2-Profile](#) | [XAUTH-Profile](#) | **IP Pools** | [Optionen](#)

Basisparameter					
IP-Poolname	<input style="width: 90%;" type="text"/>				
IP-Adressbereich	<input style="width: 45%;" type="text"/> - <input style="width: 45%;" type="text"/>				
DNS-Server	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Primär</td> <td style="padding: 2px;"><input style="width: 70%;" type="text"/></td> </tr> <tr> <td style="padding: 2px;">Sekundär</td> <td style="padding: 2px;"><input style="width: 70%;" type="text"/></td> </tr> </table>	Primär	<input style="width: 70%;" type="text"/>	Sekundär	<input style="width: 70%;" type="text"/>
Primär	<input style="width: 70%;" type="text"/>				
Sekundär	<input style="width: 70%;" type="text"/>				

Abb. 124: VPN->IPSec->IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

15.1.6 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	
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 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. 125: 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</p>

Feld	Beschreibung
	<p>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 elmeg-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	<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,</p>

Feld	Beschreibung
	<p>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>
<p>Initial Contact Message senden</p>	<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>
<p>SAs mit dem Status der ISP-Schnittstelle synchronisieren</p>	<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>
<p>Zero Cookies verwenden</p>	<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>
<p>Größe der Zero Cookies</p>	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten und auf Null gesetzten SPI in Bytes ein.</p> <p>Der Standardwert ist 32.</p>
<p>Dynamische RADIUS-Authentifizierung</p>	<p>Wählen Sie aus, ob die RADIUS-Authentifizierung über IPsec aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	<p>Wählen Sie aus, ob Zertifikatanforderungen, 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 der IKE (Phase 1) Zertifikatanforderungen 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> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
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</p>

Feld	Beschreibung
	zu unterdrücken.

15.2 L2TP

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

Ihr bintec elmeg-Gerät unterstützt die folgenden zwei Modi:

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

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

15.2.1 Tunnelprofile

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

15.2.1.1 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. 126: 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 zu Entfernter 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 bis 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>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

15.2.2 Benutzer

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

15.2.2.1 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	<input type="password"/>		
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	Entfernte IP-Adresse	Netzmaske	Metrik
	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/> <input type="text"/>
Hinzufügen			
Erweiterte Einstellungen			
Blockieren nach Verbindungsfehler für	<input type="text" value="300"/>	Sekunden	
Authentifizierung	MS-CHAPv2 <input type="text"/>		
Verschlüsselung	<input type="radio"/> Keine <input checked="" type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel		
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. 127: 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. Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.</p>

Feld	Beschreibung
Verbindungstyp	<p>Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerksservers (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 Nutz-Datenpakets 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	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.

Feld	Beschreibung
	<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> <p>Geben Sie Entfernte IP-Adresse und Netzmaske des LANs des L2TP-Partners und die dazugehörige Metrik ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.</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 einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Der Standardwert ist <i>300</i>.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus.</p> <p>Mögliche Werte:</p> <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	<p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</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

Feld	Beschreibung
	<p>mit 128 Bit wird nach RFC 3078 angewendet.</p> <ul style="list-style-type: none"> • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.
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 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>

Feld	Beschreibung
	<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 Primärer DNS-Server und Sekundärer DNS-Server und WINS-Server Primär und Sekundär vom L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

15.2.3 Optionen

Tunnelprofile Benutzer Optionen

Globale Optionen	
UDP-Zielport	<input style="width: 90%;" type="text" value="1701"/>
UDP-Quellportauswahl	<input type="checkbox"/> Fest eingestellt
OK Abbrechen	

Abb. 128: VPN->L2TP->Optionen

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

Felder im Menü Globale Optionen

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

15.3 PPTP

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

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

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

15.3.1 PPTP-Tunnel

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

15.3.1.1 Neu

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

PPTP-Tunnel
Optionen
IP Pools

PPTP Partner Parameter													
Beschreibung	<input style="width: 90%;" type="text"/>												
PPTP-Modus	<input checked="" type="radio"/> PNS <input type="radio"/> Windows-Client-Modus												
Benutzername	<input style="width: 90%;" type="text"/>												
Passwort	<input style="width: 90%;" type="password"/>												
Immer aktiv	<input type="checkbox"/> Aktiviert												
Timeout bei Inaktivität	<input style="width: 50%;" type="text" value="300"/> Sekunden												
Entfernte PPTP-IP-Adresse	<input style="width: 90%;" 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 style="width: 90%;" 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 style="width: 90%;" type="text"/></td> <td><input style="width: 90%;" 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 style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	1	▼	Hinzufügen			
Entfernte IP-Adresse	Netzmaske	Metrik											
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	1	▼										
Hinzufügen													
Erweiterte Einstellungen													
Blockieren nach Verbindungsfehler für	<input style="width: 50%;" type="text" value="300"/> Sekunden												
Authentifizierung	<input style="width: 90%;" type="text" value="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. 129: 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>Beispiel: 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 hier einen im Menü VPN->PPTP->IP Pools konfigurierten IP-Pool aus.</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 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 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.

Feld	Beschreibung
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, 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>

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.

Feld	Beschreibung
	<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-Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom PPTP-Partner erhalten soll oder diese zum PPTP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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>

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

Feld	Beschreibung
Ausgewählte Ports	<p>Geben Sie die ISDN-Ports an, über die der Callback ausgeführt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle Ports</i>: Der Callback wird über einen der verfügbaren ISDN-Ports ausgeführt. • <i>Port angeben</i>: In Spezifische Ports können Sie die gewünschten ISDN-Ports auswählen.
Spezifische Ports	<p>Nur für Ausgewählte Ports = <i>Port angeben</i> können Sie mit Hinzufügen weitere Ports auswählen.</p>

15.3.2 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. 130: 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 elmeg-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 verwendet seit der Version XP ein höheres initiales Empfangs-Window im GRE, weshalb die maximale Sendewindow-Größe 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	

15.3.3 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.

15.3.3.1 Bearbeiten oder Neu

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

PPTP-Tunnel Optionen IP Pools

Basisparameter	
IP-Poolname	<input type="text"/>
IP-Adressbereich	<input type="text"/> - <input type="text"/>
DNS-Server	Primär <input type="text"/>
	Sekundär <input type="text"/>
OK Abbrechen	

Abb. 131: VPN->PPTP->IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

15.4 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.

15.4.1 GRE-Tunnel

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

15.4.1.1 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	<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: 15%;">Metrik</th> <th style="width: 15%;"></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;"><input type="button" value="Hinzufügen"/></td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	1	▼	<input type="button" value="Hinzufügen"/>					
Entfernte IP-Adresse	Netzmaske	Metrik													
<input type="text"/>	<input type="text"/>	1	▼												
<input type="button" value="Hinzufügen"/>															
MTU	<input type="text" value="1500"/>														
Schlüssel verwenden	<input type="checkbox"/> Aktiviert														

Abb. 132: 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 16 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen bintec elmeg Gateways über eine leistungsfähige Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann nicht nur aufgrund von Quell- und Zieladressen oder Ports, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung zu einem Partner gefällt werden.

Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören. Die Aushandlung einer FTP-Verbindung findet zum Beispiel über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

SIF und andere Sicherheitsfunktionen

Die Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der bintec elmeg-Geräte ein. Systemen wie Network Address Translation (NAT) und IP-Zugriffs-Listen (IPAL) gegenüber ist der Konfigurationsaufwand der SIF vergleichbar einfach.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muss man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, dass die Regeln der SIF generell global angewendet werden, d. h. nicht auf eine Schnittstelle beschränkt sind.

Grundsätzlich werden aber dieselben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske)
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)
- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der ein-

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).

16.1 Richtlinien

16.1.1 Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Deny-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

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



Abb. 133: **Firewall->Richtlinien->Filterregeln**

Mit der Schaltfläche  können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

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

16.1.1.1 Neu

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

Filterregeln QoS Optionen

Basisparameter	
Quelle	— INTERFACE ALIASES —
Ziel	— INTERFACE ALIASES —
Dienst	— SERVICES —
Aktion	Zugriff
QoS anwenden	<input type="checkbox"/> Aktiviert

OK Abbrechen

Abb. 134: Firewall->Richtlinien->Filterregeln->Neu

Das Menü **Firewall->Richtlinien->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.</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.</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 Dienstegruppen 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 Aktion = <i>Zugriff</i> und 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>

16.1.2 QoS

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

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

16.1.2.1 Neu

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

Filterregeln
QoS
Optionen

QoS-Schnittstelle konfigurieren

Schnittstelle	Eine auswählen ▾
Traffic Shaping	<input type="checkbox"/> Aktiviert
Filterregeln	Quelle Ziel Dienst Priorität Verwenden Bandbreite (Bit/s) Fest

OK
Abbrechen

Abb. 135: **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> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
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.

16.1.3 Optionen

In diesem Menü können Sie die Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wie vielen Sekunden Inaktivität eine Sitzung beendet werden soll.

Filterregeln QoS **Optionen**

Globale Firewall-Optionen	
Firewall Status	<input checked="" type="checkbox"/> Aktiviert
Protokollierte Aktionen	Alle <input type="button" value="v"/>
Vollständige Filterung	<input checked="" type="checkbox"/> Aktivieren
Sitzungstimer	
UDP-Inaktivität	180 <input type="text"/> Sekunden
TCP-Inaktivität	3600 <input type="text"/> Sekunden
PPTP-Inaktivität	86400 <input type="text"/> Sekunden
Andere Inaktivität	30 <input type="text"/> Sekunden

Abb. 136: 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".

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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> <p>Mit <i>Aktivieren</i> werden alle Pakete gefiltert (Standardwert).</p>

Felder im Menü Sitzungstimer

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

16.2 Schnittstellen

16.2.1 Gruppen

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

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

16.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere 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>LAN_EN1-4</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-0</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Schnittstelle	Auswahl	LOCAL	<input type="checkbox"/>	LAN_EN1-4	<input type="checkbox"/>	LAN_EN1-0	<input type="checkbox"/>
Schnittstelle	Auswahl								
LOCAL	<input type="checkbox"/>								
LAN_EN1-4	<input type="checkbox"/>								
LAN_EN1-0	<input type="checkbox"/>								
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>									

Abb. 137: Firewall->Schnittstellen->Gruppen->Neu

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

Felder im Menü Basisparameter

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

16.3 Adressen

16.3.1 Adressliste

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

16.3.1.1 Neu

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

Abb. 138: **Firewall->Adressen->Adressliste->Neu**

Das Menü **Firewall->Adressen->Adressliste->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adresse ein.
Adresstyp	Wählen Sie aus, welche Art von Adresse Sie angeben wollen. Mögliche Werte: <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 Adresstyp = <i>Adresse/Subnetz</i> 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 Adresstyp = <i>Adressbereich</i> Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein.

16.3.2 Gruppen

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

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

16.3.2.1 Neu

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

Basisparameter					
Beschreibung	<input type="text"/>				
Auswahl	<table border="1"> <thead> <tr> <th>Adressen</th> <th>Auswahl</th> </tr> </thead> <tbody> <tr> <td>ANY</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Adressen	Auswahl	ANY	<input type="checkbox"/>
Adressen	Auswahl				
ANY	<input type="checkbox"/>				

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

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

Felder im Menü Basisparameter

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

16.4 Dienste

16.4.1 Diensteliste

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

16.4.1.1 Neu

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

Abb. 140: **Firewall->Dienste->Diensteliste->Neu**

Das Menü **Firewall->Dienste->Diensteliste->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protokoll	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
Zielportbereich	Nur für Protokoll = <i>TCP, UDP/TCP</i> oder <i>UDP</i> Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll. Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen. Mögliche Werte sind 1 bis 65535.

Feld	Beschreibung
Quellportbereich	<p>Nur für Protokoll = <i>TCP, 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 (Standardwert)</i> • <i>Echo Reply</i> • <i>Destination Unreachable</i> • <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>

Feld	Beschreibung
	<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>

16.4.2 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.

16.4.2.1 Neu

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

Diensteliste Gruppen

Basisparameter																																															
Beschreibung																																															
Mitglieder	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #e0e0e0;">Dienst</th> <th style="background-color: #e0e0e0;">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-qt</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-qt	<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-qt	<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. 141: Firewall->Dienste->Gruppen->Neu

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

Felder im Menü Basisparameter

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

Kapitel 17 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.

17.1 SIP

SIP dient als Übersetzungsinstanz zwischen verschiedenen Telekommunikationsnetzen wie z. B. zwischen dem herkömmlichen Telefonnetz und den Next Generation Networks (IP-Netzwerken).

17.1.1 Optionen

Im Menü **VoIP->SIP->Optionen** können Sie globale Einstellungen für das SIP vornehmen.

Basisparameter	
SIP-Proxy	<input type="checkbox"/> Aktiviert
SIP Port	5060
SIP-Aufrufe priorisieren	<input type="checkbox"/> Aktiviert

Abb. 142: **VoIP->SIP->Optionen**

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

Felder im Menü Basisparameter

Feld	Beschreibung
SIP-Proxy	<p>Wählen Sie, ob Sie den SIP-Proxy aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
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>

17.2 RTSP

In diesem Menü konfigurieren Sie die Verwendung des Real-Time Streaming Protokolls (RTSP).

RTSP ist ein Netzwerkprotokoll zur Steuerung von Multimedia-Datenströmen in IP-basierten Netzwerken. Mittels RTSP werden keine Nutzdaten übertragen. Vielmehr wird damit eine Multimedia-Session zwischen Sender und Empfänger gesteuert.

Wenn Sie RTSP nutzen möchten, müssen Firewall und NAT entsprechend konfiguriert werden. Im Menü **VoIP->RTSP** können Sie den RTSP-Proxy aktivieren, um bei Bedarf angefragte RTSP-Sessions über den definierten Port zu ermöglichen.

17.2.1 RTSP-Proxy

Im Menü **VoIP->RTSP->RTSP-Proxy** konfigurieren Sie die Verwendung des Real-Time Streaming Protokolls.

RTSP-Proxy

Basisparameter	
RTSP-Proxy	<input type="checkbox"/> Aktiviert
RTSP-Port	<input style="width: 100%;" type="text" value="554"/>

Abb. 143: **VoIP->RTSP->RTSP-Proxy**

Das Menü **VoIP->RTSP->RTSP-Proxy** besteht aus den folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
RTSP-Proxy	<p>Wählen Sie aus, ob Sie RTSP-Sessions zulassen möchten.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
RTSP-Port	<p>Wählen Sie den Port aus, über den RTSP-Nachrichten ein- bzw. ausgehen sollen.</p> <p>Mögliche Werte sind 0 bis 65535.</p> <p>Der Standardwert ist 554.</p>

Kapitel 18 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- 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)
- Wake on LAN, um Netzwerkgeräte zu aktivieren, die aktuell ausgeschaltet sind.
- Verwendung eines redundanten Gateways (BRRP).

18.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.

- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste->DNS->Globale Einstellungen->Basisparameter** werden die IP-Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der globalen Name-Server kann Ihr Gerät auch dynamisch via PPP oder DHCP erhalten bzw. diese ggf. übermitteln.

Strategie zur Namensauflösung auf Ihrem Gerät

Eine DNS-Anfrage wird von Ihrem Gerät folgendermaßen behandelt:

- (1) Falls möglich, wird die Anfrage aus dem statischen oder dynamischen Cache direkt mit IP-Adresse oder negativer Antwort beantwortet.
- (2) Ansonsten wird, falls ein passender Forwarding-Eintrag vorhanden ist, der entsprechende DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (3) Ansonsten werden, falls Name-Server eingetragen sind, unter Berücksichtigung der konfigurierten Priorität und wenn der entsprechende Schnittstellenstatus "up" ist, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (4) Ansonsten werden, falls eine Internet- oder Einwählverbindung als Standard-Schnittstelle ausgewählt ist, die dazugehörigen DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (5) Ansonsten wird, falls im Menü **WAN->Internet + Einwählen** ein Eintrag angelegt wurde und das Überschreiben der Adressen der globalen Name-Server zulässig ist (**Schnittstellenmodus = Dynamisch**), eine Verbindung zur ersten Internet- bzw. Einwählverbindung ggf. kostenpflichtig aufgebaut, die so konfiguriert ist, dass DNS-Server-Adressen von DNS-Servern angefordert werden können (**DNS-Aushandlung = Aktiviert**) - soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung stehen diese Name-Server somit für weitere Anfragen zur Verfügung.

(6) Ansonsten wird die initiale Anfrage mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit `non-existent domain` antwortet, wird die initiale Anfrage sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache Ihres Geräts aufgenommen.

18.1.1 Globale Einstellungen

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	<input type="text" value="Automatisch"/> ↓					
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. 144: Lokale Dienste->DNS->Globale Einstellungen

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
WINS-Server	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.

18.1.2 DNS-Server

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

18.1.2.1 Bearbeiten oder Neu

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

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern über unterschiedliche Schnittstellen eingerichtet sind und Lastverteilung verwendet wird.



Abb. 145: Lokale Dienste->DNS->DNS-Server->Neu

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob der DNS-Server aktiv sein soll. Mit Auswahl von <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>

18.1.3 Statische Hosts

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

18.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

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. 146: Lokale Dienste->DNS->Statische Hosts->Neu

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DNS-Hostname	<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. *.bintec-elmeg.com.</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>

18.1.4 Domänenweiterleitung

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

18.1.4.1 Neu

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

Abb. 147: **Lokale Dienste->DNS->Domänenweiterleitung->Neu**

Das Menü **Lokale Dienste->DNS->Domänenweiterleitung->Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	Wählen Sie aus, ob 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. *.bintec-elmeg.com. 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. *.bintec-elmeg.com. 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.

18.1.5 Cache

Im Menü **Lokale Dienste->DNS->Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

Globale Einstellungen | DNS-Server | Statische Hosts | Domänenweiterleitung | **Cache** | Statistik

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. 148: **Lokale Dienste->DNS->Cache**

Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** markieren.

Durch Markieren eines Eintrags und Bestätigen mit **Als statisch festlegen** wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet aus dieser Liste und wird in der Liste im Menü **Statische Hosts** angezeigt. Die TTL wird übernommen.

18.1.6 Statistik

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. 149: Lokale Dienste->DNS->Statistik

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der Cache-Treffer pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

18.2 HTTPS

Die Benutzeroberfläche Ihres Geräts können Sie von jedem PC aus mit einem aktuellen Web-Browser auch über eine HTTPS-Verbindung bedienen.

HTTPS (HyperText Transfer Protocol Secure) ist hierbei das Verfahren, um zwischen dem Browser, der zur Konfiguration verwendet wird, und dem Gerät eine verschlüsselte und authentifizierte Verbindung mittels SSL aufzubauen.

18.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Abb. 150: **Lokale Dienste->HTTPS->HTTPS-Server**

Das Menü **Lokale Dienste->HTTPS->HTTPS-Server** besteht aus folgenden Feldern:

Felder im Menü HTTPS-Parameter

Feld	Beschreibung
HTTPS-TCP-Port	<p>Geben Sie den Port ein, über den die HTTPS-Verbindung aufgebaut werden soll.</p> <p>Möglich sind Werte von 0 bis 65535.</p> <p>Standardwert ist 443.</p>
Lokales Zertifikat	<p>Wählen Sie ein Zertifikat aus, das für die HTTPS-Verbindung verwendet werden soll.</p> <p>Mögliche Werte:</p> <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.

18.3 DynDNS-Client

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Hostnamens bei einem DynDNS-Provider
- Konfiguration Ihres Geräts

Registrierung

Bei der Registrierung des Hostnamens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Hostname für Ihr Gerät ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt für Sie die Aufgabe, alle DNS-Anfragen bezüglich des Hosts *dyn_client.provider.com* mit der dynamischen IP-Adresse Ihres Geräts zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Geräts informiert ist, kontaktiert Ihr Gerät beim Aufbau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse.

18.3.1 DynDNS-Aktualisierung

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

18.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

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. 151: Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internet Service Providers).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind. Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden. Weitere DynDNS-Provider können im Menü Lokale

Feld	Beschreibung
	<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>

18.3.2 DynDNS-Provider

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

18.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

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

OK
Abbrechen

Abb. 152: Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider. 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>

18.4 DHCP-Server

Sie können Ihr Gerät als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) konfigurieren.

Jeder Rechner in Ihrem LAN benötigt, wie auch Ihr Gerät, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie Ihr Gerät als DHCP-Server einrichten, vergibt es anfragenden Rechnern im LAN automatisch IP-Adressen aus einem definierten IP-Adress-Pool.

Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine DHCP-Anfrage (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server. Daraufhin erhält der Client (im Zuge einer kurzen Kommunikation) vom bintec elmeg seine IP-Adresse.

Sie müssen so den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem Ihr Gerät jeweils für einen definierten Zeitraum IP-Adressen an Hosts im LAN vergibt. Ein DHCP-Server übermittelt auch die Adressen des statisch oder per PPP-Aushandlung eingetragenen Domain-Name-Servers (DNS), des NetBIOS Name Servers (WINS) und des Standard-Gateways.

18.4.1 IP-Pool-Konfiguration

Im Menü **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration** wird eine Liste aller konfigurierten IP-Pools angezeigt. Diese Liste ist global und zeigt auch in anderen Menüs konfigurierte Pools an.

18.4.1.1 Bearbeiten oder Neu

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



Abb. 153: Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

18.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration** wird eine Liste aller konfigurierter IP-Adresspools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. deaktivieren.



Hinweis

Im Auslieferungszustand ist der DHCP-Pool mit den IP-Adressen 192.168.0.10 bis 192.168.0.49 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

18.4.2.1 Bearbeiten oder Neu

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

IP-Pool-Konfiguration
DHCP-Konfiguration
IP/MAC-Bindung
DHCP-Relay-Einstellungen

Basisparameter					
Schnittstelle	Eine auswählen ▾				
IP-Poolname	Noch nicht definiert ▾				
Pool-Verwendung	Lokal ▾				
Erweiterte Einstellungen:					
Gateway	Router als Gateway verwenden ▾				
Lease Time	120 Minuten				
DHCP-Optionen	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%; text-align: left; padding: 2px;">Option</th> <th style="width: 50%; text-align: left; padding: 2px;">Wert</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center; padding: 5px;"> <input type="button" value="Hinzufügen"/> </td> </tr> </tbody> </table>	Option	Wert	<input type="button" value="Hinzufügen"/>	
Option	Wert				
<input type="button" value="Hinzufügen"/>					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 154: **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu**

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	<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>
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
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 Subnetz 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.

Feld	Beschreibung
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	<p>Geben Sie an, welche zusätzlichen Daten dem DHCP Client 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 Zeitervers 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-Domänename</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 IP1x0-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form <i>http://<IP-Adresse des Provisionierungsservers>/eg_prov</i> 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. herstellerspezifische Informationen übermitteln. <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge</p>

Feld	Beschreibung
	mit der Schaltfläche Hinzufügen ein.

Bearbeiten

Im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Erweiterte Einstellungen** können Sie einen Eintrag im Feld **DHCP-Optionen** bearbeiten, wenn **Option = Herstellergruppe** gewählt ist.

Wählen Sie das Symbol , um einen vorhandenen Eintrag zu bearbeiten. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server zum Beispiel für bestimmte Telefone.

Felder im Menü Basisparameter

Feld	Beschreibung
Hersteller auswählen	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Siemens</i> (Standardwert) • <i>Sonstige</i>
Provisioning-Server	Nur für Hersteller auswählen = Siemens Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll. Für die Einstellung Hersteller auswählen = Siemens wird der Standardwert <i>sdlp</i> angezeigt. Sie können die IP-Adresse des gewünschten Servers ergänzen.
Herstellerbeschreibung	Nur für Hersteller auswählen = Sonstige Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Benutzerdefinierte DHCP-Optionen	Nur für Hersteller auswählen = Sonstige Fügen Sie mit Hinzufügen weitere Einträge hinzu. Sie können DHCP-Optionen hinzufügen.

18.4.3 IP/MAC-Bindung

Im Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.



Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste->DHCP-Server->DHCP-Konfiguration** IP-Adressbereiche konfiguriert wurden.

18.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

The screenshot shows a configuration window with four tabs: **IP-Pool-Konfiguration**, **DHCP-Konfiguration**, **IP/MAC-Bindung** (selected), and **DHCP-Relay-Einstellungen**. Below the tabs is a table with the following fields:

Basisparameter	
Beschreibung	<input type="text"/>
IP-Adresse	<input type="text"/>
MAC-Adresse	<input type="text"/>

At the bottom of the dialog are two buttons: **OK** and **Abbrechen**.

Abb. 155: **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu**

Das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen MAC-Adresse die IP-Adresse gebunden wird. Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse ein, die der in MAC-Adresse angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in IP-Adresse angegebene IP-Adresse zugewiesen werden soll.

18.4.4 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

Abb. 156: Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

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

18.5 Web-Filter

Im Menü **Lokale Dienste->Web-Filter** lässt sich ein URL-basierter Web-Filter-Dienst konfigurieren, der zur Laufzeit auf das Proventia Web Filter der Firma Internet Security Systems (www.iss.net) zugreift und überprüft, wie eine angeforderte Internet-Seite durch das Proventia Web Filter kategorisiert worden ist. Die Aktion, die sich aus der Kategorisierung ergibt, wird auf Ihrem Gerät konfiguriert.

18.5.1 Allgemein

In diesem Menü finden Sie die Konfiguration grundlegender Parameter für die Nutzung des Proventia Web Filters.

Allgemein		Filterliste	Black / White List	Verlauf
Web-Filter-Optionen				
Web-Filter-Status	<input checked="" type="checkbox"/> Aktiviert			
Gefilterte Eingangs-Schnittstelle(n):	<input type="button" value="Hinzufügen"/>			
Maximale Anzahl der Einträge im Verlauf	64			
URL Pfadtiefe	1			
Aktion wenn Server nicht erreichbar	<input checked="" type="radio"/> Alle zulassen <input type="radio"/> Alle blockieren <input type="radio"/> Alle protokollieren			
Aktion wenn Lizenz nicht registriert	<input checked="" type="radio"/> Alle zulassen <input type="radio"/> Alle blockieren <input type="radio"/> Alle protokollieren			
Lizenzinformation				
Lizenzschlüssel	B1BT			[Aktiviere 30-Tage-Demo-Lizenz]
Lizenzstatus				
				
Lizenz gültig bis	Nicht aktiviert			
<input type="button" value="Übernehmen"/>				

Abb. 157: Lokale Dienste->Web-Filter->Allgemein

Das Menü **Lokale Dienste->Web-Filter->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Web-Filter-Optionen

Feld	Beschreibung
Web-Filter-Status	<p>Aktivieren oder deaktivieren Sie das Filter.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Gefilterte Eingangs-Schnittstelle(n)	<p>Wählen Sie aus, für welche der vorhandenen Ethernet- und WLAN-Schnittstellen Web Filtering aktiviert werden soll.</p> <p>Drücken Sie die Hinzufügen-Schaltfläche, wenn Sie weitere Schnittstellen hinzufügen wollen. Die Anforderungen von http-Internetseiten, die Ihr Gerät über diese Schnittstellen erreichen, werden dann vom Web Filtering überwacht.</p>
Maximale Anzahl der Einträge im Verlauf	<p>Definieren Sie die Anzahl an Einträgen, die im Web Filtering Verlauf (Menü Verlauf) gespeichert werden sollen.</p> <p>Mögliche Werte sind <i>1</i> bis <i>512</i>.</p> <p>Standardwert ist <i>64</i>.</p>
URL Pfadtiefe	<p>Wählen Sie aus, bis zu welcher Pfadtiefe eine URL durch den Cobion Orange Filter geprüft werden soll.</p>
Aktion wenn Server nicht erreichbar	<p>Wählen Sie aus, wie mit URL-Anforderungen verfahren werden soll, wenn der Web-Filtering-Server nicht erreichbar ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle zulassen</i> (Standardwert): Der Aufruf wird zugelassen. • <i>Alle blockieren</i>: Der Aufruf der angeforderten Seite wird geblockt. • <i>Alle protokollieren</i>: Der Aufruf wird zugelassen, aber protokolliert.
Aktion wenn Lizenz nicht registriert	<p>Wählen Sie aus, wie mit URL-Anforderungen verfahren werden soll, wenn der Lizenzschlüsselstatus <i>Nicht gültig</i> ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle zulassen</i> (Standardwert): Der Aufruf wird zugelassen. • <i>Alle blockieren</i>: Der Aufruf der angeforderten Seite wird

Feld	Beschreibung
	geblockt. <ul style="list-style-type: none"> • <i>Alle protokollieren</i>: Der Aufruf wird zugelassen, aber protokolliert.

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

Felder im Menü Lizenzinformation

Feld	Beschreibung
Lizenzschlüssel	Tragen Sie die Nummer der erworbenen Proventia Web Filter-Lizenz ein. Die voreingestellte, von ISS vergebene, Kennung bezeichnet den Gerätetyp. Im Auslieferungszustand haben Sie die Möglichkeit eine 30-Tage-Demoversion des Proventia Web Filter zu aktivieren. Klicken Sie hierzu auf die Verknüpfung Aktiviere 30-Tage-Demo-Lizenz
Lizenzstatus	Zeigt das Ergebnis der letzten Gültigkeitsprüfung der Lizenz an. Die Gültigkeit der Lizenz wird alle 23 Stunden überprüft.
Lizenz gültig bis	Zeigt das Ablaufdatum der Lizenz (relativ zur eingestellten Zeit auf Ihrem Gerät) an und kann nicht editiert werden.

18.5.2 Filterliste

Im Menü **Lokale Dienste->Web-Filter->Filterliste** konfigurieren Sie, welche Kategorien von Internetseiten auf welche Weise behandelt werden sollen.

Hierfür konfigurieren Sie entsprechende Filter. Eine Liste der bereits konfigurierten Filter wird angezeigt.

Bei der Konfiguration der Filter gibt es grundsätzlich unterschiedliche Ansätze:

- Zum einen kann man eine Filterliste anlegen, die nur Einträge für solche Adressen enthält, die blockiert werden sollen. In diesem Fall ist es notwendig, am Ende der Filterliste einen Eintrag vorzunehmen, der alle Zugriffe, auf die kein Filter zutrifft, gestattet. (Einstellung dafür: **Kategorie** = *Default behaviour*, **Aktion** = *Zulassen* oder *Zulassen und Protokollieren*)
- Wenn Sie nur Einträge für solche Adressen anlegen, die zugelassen bzw. protokolliert werden sollen, ist eine Änderung des Standardverhaltens (=alle übrigen Aufrufe werden geblockt) nicht notwendig.

18.5.2.1 Neu

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

Allgemein **Filterliste** Black / White List Verlauf

Filtereinstellungen	
Kategorie	Anonymous Proxies
Tag	Täglich
Zeitplan (Start-/Stopzeit)	Von 00:00 bis 23:59
Aktion	<input type="radio"/> Zulassen <input type="radio"/> Zulassen und Protokollieren <input checked="" type="radio"/> Blockieren und Protokollieren

OK Abbrechen

Abb. 158: Lokale Dienste->Web-Filter->Filterliste->Neu

Das Menü **Lokale Dienste->Web-Filter->Filterliste->Neu** besteht aus folgenden Feldern:

Felder im Menü Filtereinstellungen

Feld	Beschreibung
Kategorie	<p>Wählen Sie aus, auf welche Kategorie von Adressen/URLs das Filter angewendet werden soll.</p> <p>Zur Auswahl stehen zum einen die Standardkategorien des Proventia Web Filters (Standardwert: <i>Anonymous Proxies</i>). Darüber hinaus können Aktionen für folgende Sonderfälle definiert werden, z. B.:</p> <ul style="list-style-type: none"> • <i>Default behaviour</i>: Diese Kategorie trifft auf alle Internet-Adressen zu. • <i>Other category</i>: Manche Adressen sind dem Proventia Web Filter bereits bekannt, aber noch nicht kategorisiert. Für derartige Adressen wird die mit dieser Kategorie verbundene Aktion angewendet. • <i>Unknown URL</i>: Wenn eine Adresse dem Proventia Web Filter nicht bekannt ist, wird die mit dieser Kategorie verbundene Aktion angewendet.
Tag	<p>Wählen Sie aus, an welchen Tagen das Filter aktiv sein soll.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Täglich</i> (Standardwert): Das Filter gilt für jeden Tag der Woche.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i><Wochentag></i>: Das Filter gilt für einen bestimmten Tag der Woche. Es kann pro Filter nur ein Tag ausgewählt werden, für mehrere einzelne Tage müssen mehrere Filter angelegt werden. • <i>Montag-Freitag</i>: Das Filter gilt montags bis freitags. <p>Standardwert ist <i>Täglich</i>.</p>
Zeitplan (Start-/Stopzeit)	<p>Geben Sie bei Von ein, zu welcher Uhrzeit das Filter aktiviert werden soll. Die Eingabe erfolgt nach dem Schema hh:mm. Geben Sie in das Feld nach dem bis ein, zu welcher Uhrzeit das Filter deaktiviert werden soll. Die Eingabe erfolgt nach dem Schema hh:mm. Standardwert ist 00:00 bis 23.59.</p>
Aktion	<p>Wählen Sie die Aktion, die ausgeführt werden soll, wenn das Filter auf einen Aufruf zutrifft.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Blockieren und Protokollieren</i> (Standardwert): Der Aufruf der angeforderten Seite wird unterbunden und protokolliert. • <i>Zulassen und Protokollieren</i>: Der Aufruf wird zugelassen, aber protokolliert. Einsicht in die protokollierten Ereignisse ist im Menü Lokale Dienste->Web-Filter->Filterliste möglich. • <i>Zulassen</i>: Der Aufruf wird zugelassen und nicht protokolliert.

18.5.3 Black / White List

Das Menü **Lokale Dienste->Web-Filter->Black / White List** enthält eine Liste mit URLs bzw. IP-Adressen. Die Adressen **Auf der White List** können auch dann aufgerufen werden, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im Proventia Web Filter blockiert würden. Die Adressen **Auf der Black List** sind auch dann blockiert, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im Proventia Web Filter aufgerufen werden könnten. In der Standardkonfiguration enthalten beide Listen keine Einträge.

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere URLs oder IP-Adressen der Liste hinzuzufügen.

[Allgemein](#) [Filterliste](#) [Black / White List](#) [Verlauf](#)

URL / IP-Adresse	Auf der Black List	Auf der White List	
<input style="width: 95%;" type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	
Hinzufügen OK Abbrechen			

Abb. 159: Lokale Dienste->Web-Filter->Black / White List->Hinzufügen

Das Menü **Lokale Dienste->Web-Filter->Black / White List->Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Black / White List

Feld	Beschreibung
URL / IP-Adresse	Geben Sie eine URL oder IP-Adresse ein. Die Länge des Eintrags ist auf 60 Zeichen begrenzt.
Auf der Black List Auf der White List	<p>Sie können wählen, ob eine URL oder IP-Adresse immer (<i>Auf der White List</i>) oder nie (<i>Auf der Black List</i>) aufgerufen werden kann.</p> <p>Standardmäßig ist <i>Auf der White List</i> aktiviert.</p> <p>Adressen, die in der White List geführt sind, werden automatisch zugelassen. Die Konfiguration eines entsprechenden Filters ist nicht notwendig.</p>

18.5.4 Verlauf

Im Menü **Lokale Dienste->Web-Filter->Verlauf** können Sie den aufgezeichneten Verlauf des Web Filters einsehen. Es werden alle Aufrufe protokolliert, die durch einen entsprechenden Filter dafür markiert werden (**Aktion** = *Zulassen und Protokollieren* oder *Blockieren und Protokollieren*), ebenso alle abgewiesenen Aufrufe.

[Allgemein](#) [Filterliste](#) [Black / White List](#) [Verlauf](#)

Ansicht	20	pro Seite	<input type="button" value="◀"/> <input type="button" value="▶"/>	Filtern in	Keiner	gleich	Los
Nr.	Datum	Zeit	Quelle	URL	Kategorie	Ergebnis	
Seite: 1							

Abb. 160: Lokale Dienste->Web-Filter->Verlauf

18.6 CAPI-Server

Mit der Funktion CAPI-Server können Sie an Nutzer der CAPI-Anwendungen Ihres Geräts Benutzernamen und Passwörter vergeben. So stellen Sie sicher, dass nur 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

Alle eingehenden Rufe an die CAPI werden allen registrierten und "lauschenden" CAPI-Applikationen im LAN angeboten.

Im Auslieferungszustand ist für das Subsystem CAPI ein Benutzer mit dem Benutzernamen *default* ohne Passwort eingetragen.

Wenn Sie Ihre gewünschten Benutzer mit Passwort angelegt haben, sollten Sie den Benutzer *default* ohne Passwort löschen.

18.6.1 Benutzer

Im Menü **Lokale Dienste->CAPI-Server->Benutzer** wird eine Liste aller konfigurierter CAPI Benutzer angezeigt.

18.6.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

Benutzer Optionen

Basisparameter	
Benutzername	<input type="text"/>
Passwort	<input type="password"/>
Zugriff	<input checked="" type="checkbox"/> Aktiviert

OK Abbrechen

Abb. 161: Lokale Dienste->CAPI-Server->Benutzer->Neu

Das Menü **Lokale Dienste->CAPI-Server->Benutzer->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, für den der Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll.
Passwort	Geben Sie das Passwort ein, mit dem sich der Benutzer Benutzername identifizieren muss, um Zugang zum CAPI Dienst zu erhalten.
Zugriff	Wählen Sie aus, ob der Zugriff auf den CAPI-Dienst für den Benutzer erlaubt oder gesperrt werden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

18.6.2 Optionen

Benutzer Optionen

Basisparameter	
Server aktivieren	<input checked="" type="checkbox"/> Aktiviert
Faxkopfzeile	<input type="checkbox"/> Aktiviert
TCP-Port des CAPI-Servers	<input type="text" value="2662"/>

OK Abbrechen

Abb. 162: 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>
Faxkopfzeile	<p>Nur für Geräte der RTxxx2-Serie</p> <p>Wählen Sie aus, ob am oberen Seitenrand von ausgehenden Faxen die Faxkopfzeile gedruckt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht 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>

18.7 Scheduling

Ihr Gerät verfügt über einen Aufgabenplaner, mit dem bestimmte Standardaktionen (beispielsweise Aktivierung bzw. Deaktivierung von Schnittstellen) durchgeführt werden können. Außerdem ist jede vorhandene MIB-Variable mit jedem beliebigen Wert konfigurierbar.

Sie legen die gewünschten **Aktionen** fest und definieren die **Auslöser**, die steuern, wann bzw. unter welchen Bedingungen die **Aktionen** durchgeführt werden sollen. Ein **Auslöser** kann ein einzelnes Ereignis sein oder eine Folge von Ereignissen, die in einer **Ereignisliste** zusammengefasst sind. Für ein einzelnes Ereignis legen Sie ebenfalls eine Ereignisliste an, die jedoch nur ein Element enthält.

Es ist möglich, zeitgesteuert Aktionen auszulösen. Außerdem kann der Status oder die Erreichbarkeit von Schnittstellen oder deren Datenverkehr zur Ausführung der konfigurierten Aktionen führen, oder aber auch die Gültigkeit von Lizenzen. Auch hier ist es möglich, jede beliebige MIB-Variable mit jedem beliebigen Wert als Auslöser einzurichten.

Um den Aufgabenplaner in Betrieb zu nehmen, aktivieren Sie das **Schedule-Intervall** unter **Optionen**. Dieses Intervall gibt den Zeitabstand vor, in dem das System prüft, ob mindestens ein Ereignis eingetreten ist. Dieses Ereignis dient als Auslöser für eine konfigurierte Aktion.



Achtung

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der bintec elmeg Gateways. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.



Hinweis

Voraussetzung für den Betrieb des Aufgabenplaners ist ein auf Ihrem Gerät eingestelltes Datum ab dem 1.1.2000.

18.7.1 Auslöser

Im Menü **Lokale Dienste->Scheduling->Auslöser** werden alle konfigurierten Ereignislisten angezeigt. Jede Ereignisliste enthält mindestens ein Ereignis, das als Auslöser für eine Aktion vorgesehen ist.

18.7.1.1 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;">Bedingungstyp</th> <th style="text-align: left;">Bedingungeinstellungen</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/> Wochentag</td> <td>Montag ▼</td> </tr> <tr> <td><input checked="" type="radio"/> Perioden</td> <td>Täglich ▼</td> </tr> <tr> <td><input type="radio"/> Tag des Monats</td> <td>1 ▼</td> </tr> </tbody> </table>	Bedingungstyp	Bedingungeinstellungen	<input type="radio"/> Wochentag	Montag ▼	<input checked="" type="radio"/> Perioden	Täglich ▼	<input type="radio"/> Tag des Monats	1 ▼
Bedingungstyp	Bedingungeinstellungen								
<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"/>								
Stoppzeit	Stunde <input style="width: 40px;" type="text"/> Minute <input style="width: 40px;" type="text"/>								
OK Abbrechen									

Abb. 163: 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>
Ereignistyp	<p>Wählen Sie den Typ des Ereignisses aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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. • <i>Status der GEO-Zone</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierten GEO-Zonen einen bestimmten Status annehmen.
Überwachte GEO-Zone	<p>Nur für Ereignistyp <i>Status der GEO-Zone</i></p> <p>Wählen Sie eine konfigurierte GEO-Zone aus.</p>
GEO Zone Status	<p>Nur für Ereignistyp <i>Status der GEO-Zone</i></p> <p>Wählen Sie den GEO Zone Status aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Wahr</i>: Die aktuelle Position liegt innerhalb der definierten Zone. • <i>Falsch</i>: Die aktuelle Position liegt außerhalb der definierten Zone.
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</p>

Feld	Beschreibung
	<p>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> <p>Geben Sie den Wert der MIB-Variable ein.</p>
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>

Feld	Beschreibung
	<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 Datenverkehr</i> angegebenen Wert sein muss, um die Aktion auszulösen.</p>
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 0.</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></p>

Feld	Beschreibung
	(Standardwert) oder <i>Nicht erreichbar</i> sein muss, um die Aktion auszulösen.
Intervall	Nur für Ereignistyp <i>Ping-Test</i> Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll. Standardwert ist <i>60</i> Sekunden.
Versuche	Nur für Ereignistyp <i>Ping-Test</i> Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis Ziel-IP-Adresse als <i>Nicht erreichbar</i> gilt. Standardwert ist <i>3</i> .
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 Bedin-

Feld	Beschreibung
	<p>gungstyp = <i>Wochentag</i>:</p> <p><i>Montag</i> (Standardwert) ... <i>Sonntag</i>.</p> <p>Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Perioden</i>:</p> <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. • <i>Samstag-Sonntag</i>: Der Auslöser wird Samstag und Sonntag aktiv. <p>Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Tag des Monats</i>:</p> <p><i>1... 31</i>.</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.

18.7.2 Aktionen

Im Menü **Lokale Dienste->Scheduling->Aktionen** wird eine Liste aller Aktionen angezeigt, die durch die in **Lokale Dienste->Scheduling->Auslöser** konfigurierten Ereignisse oder Ereignisketten ausgelöst werden sollen.

18.7.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Aktionen zu konfigurieren.

Auslöser
Aktionen
Optionen

Basisparameter	
Beschreibung	<input type="text"/>
Befehlstyp	Neustart ▼
Ereignisliste	Eine auswählen ▼
Bedingung für Ereignisliste	Alle ▼
Neustart des Geräts nach	60 Sekunden

OK
Abbrechen

Abb. 164: 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>WLAN-Status</i>: Nur für Geräte mit Wireless LAN. Der Status einer WLAN-SSID 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>5 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt. • <i>5,8 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless

Feld	Beschreibung
	<p>LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt.</p> <ul style="list-style-type: none"> • <i>WLC: Neuer Neighbor-Scanvorgang</i>: Nur für Geräte mit WLAN Controller. In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • <i>WLC: VSS-Status</i>: Nur für Geräte mit WLAN Controller. Der Status eines Drahtlosnetzwerkes wird verändert. • <i>Betriebsmodus</i>: Der Betriebsmodus eines WLAN-Radiomoduls 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 Ereignisse eintritt. • <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>

Feld	Beschreibung
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> <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 be-</p>

Feld	Beschreibung
	<p>schrieben.</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> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert) • <i>Inaktiv</i> • <i>Zurücksetzen</i>
Lokale WLAN-SSID	<p>Nur bei Befehlstyp = <i>WLAN-Status</i></p> <p>Wählen Sie das gewünschte Drahtlosnetzwerk aus, dessen Status verändert werden soll.</p>
Status festlegen	<p>Nur bei Befehlstyp = <i>WLAN-Status</i> oder <i>WLC: VSS-Status</i></p> <p>Wählen Sie den Status aus, den das Drahtlosnetzwerk erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert) • <i>Deaktivieren</i>

Feld	Beschreibung
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 Update-Server</i> (Standardwert): Die aktuelle Software wird vom Update-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> wenn Quelle nicht <i>Aktuelle Software vom Update-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> <p>Geben Sie den Dateinamen der Zertifikatsdatei ein.</p>
Aktion	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll.</p>

Feld	Beschreibung
	<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 Sie auf eine Zertifikatsdatei anwenden möchten.</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 werden 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>

Feld	Beschreibung
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> <p>Wählen Sie die Datei aus, die kopiert werden soll.</p>
Konfiguration enthält Zertifikate/Schlüssel	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren oder Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen.</p>

Feld	Beschreibung
Konfiguration verschlüsseln	<p>Standardmäßig ist die Funktion nicht aktiv.</p> <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 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.

Feld	Beschreibung
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 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>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
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.bintec-elmeg.com: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>
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>

Feld	Beschreibung
	Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.
Schlüsselgröße	<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 gestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Werte:</p> <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.
WLAN-Modul auswählen	Nur bei Befehlstyp = <i>5 GHz-WLAN-Bandscan</i> , <i>5,8 GHz-WLAN-Bandscan</i> und

Feld	Beschreibung
	<p><i>Betriebsmodus</i></p> <p>Wählen Sie das WLAN-Modul aus, auf dem ein Scan des Frequenzbands durchgeführt werden soll.</p>
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>
Betriebsmodus (Aktiv)	<p>Nur bei Befehlstyp = <i>Betriebsmodus</i></p> <p>Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand <i>Aktiv</i> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.</p>
	<p>Nur bei Befehlstyp = <i>Betriebsmodus</i></p> <p>Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand <i>Inaktiv</i> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.</p>

Feld	Beschreibung
)	

18.7.3 Optionen

Im Menü **Lokale Dienste->Scheduling->Optionen** konfigurieren Sie das Schedule-Intervall.

Abb. 165: **Lokale Dienste->Scheduling->Optionen**

Das Menü **Lokale Dienste->Scheduling->Optionen** besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

Feld	Beschreibung
Schedule-Intervall	<p>Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll.</p> <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).</p>

18.8 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Bei Geräten der **bintec WI**-Serie können Sie die Temperatur überwachen lassen.



Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

18.8.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

18.8.1.1 Bearbeiten oder Neu

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

Hosts Schnittstellen Ping-Generator

Hostparameter					
Gruppen-ID	<input type="text" value="Neue ID"/>				
Trigger					
Überwachte IP-Adresse	<input type="text" value="Standard-Gateway"/>				
Quell-IP-Adresse	<input type="text" value="Automatisch"/>				
Intervall	<input type="text" value="10"/> Sekunden				
Erfolgreiche Versuche	<input type="text" value="3"/>				
Fehlgeschlagene Versuche	<input type="text" value="3"/>				
Auszuführende Aktion	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Aktion</th> <th>Schnittstelle</th> </tr> </thead> <tbody> <tr> <td><input type="text" value="Deaktivieren"/></td> <td><input type="text" value="Eine auswählen"/></td> </tr> </tbody> </table>	Aktion	Schnittstelle	<input type="text" value="Deaktivieren"/>	<input type="text" value="Eine auswählen"/>
Aktion	Schnittstelle				
<input type="text" value="Deaktivieren"/>	<input type="text" value="Eine auswählen"/>				
<input type="button" value="Hinzufügen"/>					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 166: **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>

Feld	Beschreibung
	Die in Schnittstelle konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied erreichbar ist.

Felder im Menü Trigger

Feld	Beschreibung
Überwachte IP-Adresse	<p>Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.</p> <p>Mögliche Werte:</p> <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 1 bis 65536.</p> <p>Standardwert ist 10.</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>

Feld	Beschreibung
	<p>Mögliche Werte sind 1 bis 65536.</p> <p>Standardwert ist 3.</p>
<p>Fehlgeschlagene Versuche</p>	<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 1 bis 65536.</p> <p>Standardwert ist 3.</p>
<p>Auszuführende Aktion</p>	<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 = <i>Überwachen</i> 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>

18.8.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

18.8.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Hosts **Schnittstellen** Ping-Generator

Basisparameter	
Überwachte Schnittstelle	Eine auswählen ▾
Trigger	Schnittstelle wird aktiviert. ▾
Schnittstellenaktion	Aktivieren ▾
Schnittstelle	Eine auswählen ▾

OK Abbrechen

Abb. 167: 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

Feld	Beschreibung
	und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle IPSec-Schnittstellen</i> .

18.8.3 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

18.8.3.1 Bearbeiten oder Neu

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



Abb. 168: **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

Feld	Beschreibung
	erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in Entfernte IP-Adresse angegebene Adresse abgesetzt werden soll. Mögliche Werte sind <i>1</i> bis <i>65536</i> . Standardwert ist <i>10</i> .
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 <i>3</i> .

18.9 ISDN-Diebstahlsicherung

Mit der Funktion ISDN-Diebstahlsicherung können Sie verhindern, dass sich ein Dieb, der ein Gateway gestohlen hat, Zutritt zum LAN des Gateway-Besitzers verschafft. (Ohne Diebstahlsicherung könnte er sich über ISDN in das LAN einwählen, wenn unter **WAN->Internet + Einwählen->ISDN->** das Feld **Immer aktiv** aktiviert ist.)

18.9.1 Optionen

Alle Schnittstellen, für welche die Diebstahlsicherung aktiv ist, werden beim Booten des Gateways administrativ auf "down" gesetzt.

Anschließend ruft sich das Gateway über ISDN selbst an und überprüft seinen Standort. Wenn die konfigurierten ISDN Rufnummern von den gewählten Rufnummern abweichen, bleiben die Schnittstellen deaktiviert.

Stimmen die Nummern überein, geht das Gerät davon aus, dass es sich am ursprünglichen Standort befindet, und die Schnittstellen werden administrativ auf "up" gesetzt.

Um Kosten zu sparen, nutzt die Funktion den ISDN D-Kanal.



Hinweis

Beachten Sie, dass die Funktion ISDN-Diebstahlsicherung für Ethernet-Schnittstellen nicht zur Verfügung steht.

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	<div style="border: 1px solid gray; padding: 2px;"> Schnittstelle <input type="text"/> </div> <input type="button" value="Hinzufügen"/>
Erweiterte Einstellungen	
Anzahl der Wählversuche	<input type="text" value="3"/>
Timeout	<input type="text" value="5"/> Sekunden
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 169: Lokale Dienste->ISDN-Diebstahlsicherung->Optionen

Das Menü **Lokale Dienste->ISDN-Diebstahlsicherung->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
ISDN-Diebstahlsicherungsdienst	Aktivieren oder deaktivieren Sie die Funktion ISDN-Diebstahlsicherung. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Wählnummer	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Geben Sie die Rufnummer ein, die das Gateway wählt, wenn es sich selbst anruft.
Eingehende Nummer	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Geben Sie die Rufnummer ein, die mit der aktuellen Calling Party Number verglichen werden soll.
Ausgehende Nummer	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Geben Sie die Rufnummer ein, die als Calling Party Number ge-

Feld	Beschreibung
	setzt wird.
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>

18.10 UPnP

Universal Plug and Play (UPnP) ermöglicht die Nutzung aktueller Messenger-Dienste (z. B. Realtime-Video/Audiokonferenzen) als Peer-to-Peer Kommunikation, wobei einer der Peers hinter einem Gateway mit aktiver NAT-Funktion liegt.

UPnP befähigt (meist) Windows-basierte Betriebssysteme, die Kontrolle über andere Geräte im lokalen Netzwerk mit UPnP Funktionalität zu übernehmen und diese zu steuern. Dazu zählen u.a. Gateways, Access Points und Printserver. Es sind keine speziellen Gerätetreiber notwendig, da gemeinsame und bekannte Protokolle genutzt werden wie TCP/IP, HTTP und XML.

Ihr Gateway ermöglicht die Nutzung des Subsystems des Internet Gateway Devices (IGD) aus dem UPnP-Funktionsspektrum.

In einem Netzwerk hinter einem Gateway mit aktiver NAT Funktion agieren die UPnP-konfigurierten Rechner als LAN UPnP Clients. Dazu muss die UPnP Funktion auf dem PC aktiviert sein.

Der auf dem Gateway voreingestellte Port, über den die UPnP-Kommunikation zwischen LAN UPnP Clients und dem Gateway läuft, ist 5678. Der LAN UPnP Client dient hierbei als sogenannter Service Control Point, d.h. er erkennt und kontrolliert die UPnP-Geräte im Netzwerk.

Die z. B. vom MSN Messenger dynamisch 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.

18.10.1 Schnittstellen

In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Sie können festlegen, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle angenommen werden (für Anfragen aus dem lokalen Netzwerk) und/oder ob die Schnittstelle über UPnP-Anfragen kontrolliert werden kann.

Schnittstellen Allgemein

Schnittstelle	Auf Client-Anfrage antworten	Schnittstelle ist UPnP-kontrolliert
en1-4	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert
en1-0	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert

Seite: 1, Objekte: 1 - 2

Abb. 170: Lokale Dienste->UPnP->Schnittstellen

Das Menü **Lokale Dienste->UPnP->Schnittstellen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der Schnittstelle an, für welche die UPnP-Einstellungen vorgenommen werden. Der Eintrag kann nicht verändert werden.
Auf Client-Anfrage antworten	Legen Sie fest, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle (aus dem lokalen Netzwerk) beantwortet werden. Mit <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.

18.10.2 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. 171: Lokale Dienste->UPnP->Allgemein

Das Menü **Lokale Dienste->UPnP->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Allgemein

Feld	Beschreibung
UPnP-Status	Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt. Mit <i>Aktiviert</i> wird die Funktion aktiv. Das Gateway nimmt die UPnP-Freigaben gemäß der in der Anfrage des LAN UPnP Cli-

Feld	Beschreibung
	<p>ents beinhaltenen Parameter vor, unabhängig von der IP Adresse 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>

18.11 Hotspot-Gateway

Die **Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen (mittels WLAN oder kabelgebundenem Ethernet). Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **Hotspot Solution** besteht aus einem vor Ort installierten bintec elmeg Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

Ablauf der Anmeldeprozedur am Hotspot Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein bintec elmeg Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung**->**Remote Authentifizierung** ->**RADIUS**->**Neu** mit **Gruppenbeschreibung** *Standardgruppe 0*)
- bintec elmeg Hotspot Hosting (Artikelnummer 5510000198 bzw. 5510000197)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

- Gehen Sie auf www.bintec-elmeg.com zu **Service/Support** -> **Services** -> **Online Services**.

- Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

- Sie erhalten daraufhin die Login-Daten des Hotspot Servers.



Hinweis

Die Freischaltung kann etwa 2-3 Werktage in Anspruch nehmen.

Zugangsdaten zur Konfiguration des Gateways

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Wird von bintec elmeg GmbH festgelegt
Domain	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Network	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Server URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Terms & Condition URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt

Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Wird durch bintec elmeg individuell festgelegt
Password	Wird durch bintec elmeg individuell festgelegt



Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf www.bintec-elmeg.com zum Download zur Verfügung steht.

18.11.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte bintec elmeg Gateway für die **Hotspot Solution**.

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller konfigurierter Hotspot Netzwerke angezeigt.



Abb. 172: **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway**

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktivieren.

18.11.1.1 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	<input type="text" value="LAN_EN1-0"/>
Domäne am Hotspot-Server	<input type="text"/>
Walled Garden	<input type="checkbox"/> Aktiviert
Aufzurufende Seite nach Login	<input type="text"/>
Sprache für Anmeldefenster	<input type="text" value="English"/>

Erweiterte Einstellungen

Tickettyp	<input type="text" value="Benutzername/Passwort"/>
Zulässiger Hotspot-Client	<input type="text" value="Alle"/>
Anmeldefenster	<input checked="" type="checkbox"/> Aktiv
Pop-Up-Fenster für Statusanzeige	<input checked="" type="checkbox"/> Aktiviert
Standard-Timeout bei Inaktivität	<input checked="" type="checkbox"/> Aktiviert
	<input type="text" value="600"/> Sekunden

OK
Abbrechen

Abb. 173: **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="margin-top: 20px;"> <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</p> </div>

Feld	Beschreibung
	zur weiteren Konfiguration Ihres Geräts erneut anmelden.
Domäne am Hotspot-Server	Geben Sie den Domännennamen ein, der bei der Einrichtung des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.
Walled Garden	<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 IP-Adressen von 192.168.0.0 bis 19.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IP-Adresse 192.168.0.1 frei.</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, freizugängliche Domännennamen	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Fügen Sie mit Hinzufügen weitere URLs oder IP-Adressen hin-</p>

Feld	Beschreibung
	zu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.
Aufzurufende Seite nach Login	Hier können Sie eine URL angeben, zu der ein Benutzer umgeleitet wrd, wenn er sich bei der Hotspot-Lösung angemeldet hat.
Sprache für Anmeldefenster	<p>Hier können Sie die Sprache für die Start/Login-Seite auswählen.</p> <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 An-</p>

Feld	Beschreibung
	<p>melde-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>
Pop-Up-Fenster für Statusanzeige	<p>Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Standard-Timeout bei Inaktivität	<p>Aktivieren oder deaktivieren Sie den Standard-Timeout bei Inaktivität Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Standardwert ist 600 Sekunden.</p>

18.11.2 Optionen

Im Menü **Lokale Dienste->Hotspot-Gateway->Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

Abb. 174: **Lokale Dienste->Hotspot-Gateway->Optionen**

Das Menü **Lokale Dienste->Hotspot-Gateway->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Host für mehrere Standorte	Wenn für einen Kunden auf dem Hotspot Server mehrere Standorte (Filialen) eingerichtet wurden, geben Sie hier den

Feld	Beschreibung
	Wert des NAS-Identifiers (RADIUS-Server Parameter) ein, der für diesen Standort auf dem Hotspot Server eingetragen wurde.

18.12 Wake-On-LAN

Mit der Funktion **Wake-On-LAN (WOL)** können Sie ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten. Die Netzwerkkarte muss weiterhin mit Strom versorgt werden, auch wenn der Computer ausgeschaltet ist. Sie können die Bedingungen, die zum Versenden des sog. Magic Packets erfüllt sein müssen, über Filter und Regelketten definieren sowie diejenigen Schnittstellen auswählen, die auf die definierten Regelketten hin überwacht werden sollen. Die Konfiguration der Filter und Regelketten entspricht weitgehend der Konfiguration von Filtern und Regelketten im Menü **Zugriffsregeln**.

18.12.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

18.12.1.1 Bearbeiten oder Neu

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

Wake-on-LAN-Filter WOL-Regeln Schnittstellenzuweisung

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	any ▼
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 ▼

OK Abbrechen

Abb. 175: Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter->Neu

Das Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	<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>Beliebig</i>.</p>
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	<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 Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.
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> <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.
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).

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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.
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. Wertebereich 0 bis 7.</p> <p>Der Standardwert ist <i>Nicht beachten</i>.</p>

18.12.2 WOL-Regeln

Im Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln** wird eine Liste aller konfigurierten WOL-Regeln angezeigt.

18.12.2.1 Bearbeiten oder Neu

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

Wake-on-LAN-Filter
WOL-Regeln
Schnittstellenzuweisung

Basisparameter	
Wake-On-LAN-Regelkette	Neu <input type="button" value="v"/>
Beschreibung	<input type="text"/>
Wake-on-LAN-Filter	Eines auswählen <input type="button" value="v"/>
Aktion	WOL aufrufen, wenn Filter zutrifft <input type="button" value="v"/>
Typ	Ethernet <input type="button" value="v"/>
Sende WOL-Paket über Schnittstelle	Eine auswählen <input type="button" value="v"/>
Ziel-MAC-Adresse	<input type="text"/>
Passwort	<input type="text"/>

Abb. 176: Lokale Dienste->Wake-On-LAN->WOL-Regeln->Neu

Das Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Wake-On-LAN-Regelkette	<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>: Zeigt eine bereits angelegte Regelkette, die Sie auswählen und bearbeiten können.
Beschreibung	<p>Nur für Wake-On-LAN-Regelkette = <i>Neu</i></p> <p>Geben Sie die Bezeichnung der Regelkette ein.</p>
Wake-on-LAN-Filter	<p>Wählen Sie ein WOL-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> <p>Um ein Filter auswählen zu können, muss mindestens ein Filter</p>

Feld	Beschreibung
	im Menü Local Services->Wake-On-LAN->WOL-Regeln konfiguriert sein.
Aktion	<p>Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WOL aufrufen, wenn Filter zutrifft</i>: WOL ausführen, wenn der Filter zutrifft. • <i>Aufrufen, wenn Filter nicht zutrifft</i>: WOL ausführen, wenn der Filter nicht zutrifft. • <i>WOL verweigern, wenn Filter zutrifft</i>: WOL nicht ausführen, wenn der Filter zutrifft. • <i>WOL verweigern, wenn Filter nicht zutrifft</i>: WOL nicht ausführen, wenn der Filter nicht zutrifft. • <i>Regel ignorieren und zu nächster Regel springen</i>: Diese Regel wird ignoriert und die in der Kette folgende wird überprüft.
Typ	Wählen Sie aus, ob das Wake on LAN Magic Packet als UDP-Paket oder als Ethernet Frame über die Schnittstelle gesendet werden soll, die in Sende WOL-Paket über Schnittstelle festgelegt wird.
Sende WOL-Paket über Schnittstelle	Wählen Sie die Schnittstelle aus, über die das Wake on LAN Magic Packet gesendet werden soll.
Ziel-MAC-Adresse	<p>Nur für Action = <i>WOL aufrufen, wenn Filter zutrifft</i> und <i>Aufrufen, wenn Filter nicht zutrifft</i></p> <p>Geben Sie die MAC-Adresse desjenigen Netzwerkgerätes ein, das mittels WOL aktiviert werden soll.</p>
Passwort	<p>Nur für Action = <i>WOL aufrufen, wenn Filter zutrifft</i> und <i>Aufrufen, wenn Filter nicht zutrifft</i></p> <p>Wenn das Netzwerkgerät, das aktiviert werden soll, die Funktion "SecureOn" unterstützt, geben Sie hier das entsprechende Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.</p>

18.12.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten einzelnen Schnittstellen zugeordnet, die auf diese Regelketten hin überwacht werden.

Im Menü **Lokale Dienste->Wake-On-LAN->Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

18.12.3.1 Bearbeiten oder Neu

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



Abb. 177: **Lokale Dienste->Wake-On-LAN->Schnittstellenzuweisung->Neu**

Das Menü **Lokale Dienste->Wake-On-LAN->Schnittstellenzuweisung ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.

18.13 BRRP

Im Menü **BRRP** können Sie eine Redundanz für Ihr Gateway konfigurieren.



Hinweis

Für Geräte der R23x-Serie und der RS-Serie benötigen Sie eine Lizenz.

BRRP (Bintec Router Redundancy Protocol) ist eine bintec elmeg-spezifische Implementierung des VRRP (Virtual Router Redundancy Protocol). Ein Router-Redundanzverfahren dient hauptsächlich dazu, die Verfügbarkeit eines physikalischen Gateways im LAN oder WAN sicherzustellen.

Begriffe und Definitionen

Zur Beschreibung der Funktion werden einige spezielle Begriffe verwendet. Folgende Begriffe werden im entsprechenden RFC und im Internet-Entwurf definiert.

BRRP Begriffe

Feld	Beschreibung
VRRP-Router	"Ein Router, der das Virtual Router Redundancy Protocol benutzt. Er kann in einen oder in mehrere "virtuelle Router" integriert sein."
Virtueller Router	"Ein abstraktes, von VRRP gesteuertes Objekt, das als Standard-Router für Hosts eines LAN verwendet wird. Es besteht aus einem Virtual Router Identifier (ID des virtuellen Routers) und einer IP-Adresse bzw. einer Gruppe zugehöriger IP-Adressen innerhalb eines gemeinsamen LAN. Ein VRRP-Router kann den Datenverkehr eines einzelnen virtuellen Routers oder mehrerer virtueller Router absichern."
IP Address Owner	"Der VRRP-Router, der die IP-Adresse(n) des virtuellen Routers als echte Schnittstellen-Adresse(n) besitzt. Es handelt sich um den Router, der, wenn er aktiv ist, auf Pakete für ICMP-Pings, TCP-Verbindungen etc. an eine dieser IP-Adressen antwortet."
Primary IP Address	"Eine IP-Adresse, die aus der Gruppe der echten Schnittstellenadressen gewählt wird. Eine mögliche Algorithmusoption ist die Auswahl der ersten Adresse. VRRP Advertisements werden immer mit der Primary IP-Adresse als Quelle des IP-Pakets verschickt."
VRRP Advertisement	Ein Keepalive, das der Master zu den Backup-Gateways schickt, um seine Erreichbarkeit zu signalisieren.
Virtual Router Master	"Der VRRP-Router, der das Weiterleiten der Pakete übernimmt, die an die mit dem "virtuellen Router" verbundenen IP-Adressen geschickt wurden, und der für die Beantwortung von ARP (Address Resolution Protocol) Requests an diese IP-Adressen zuständig ist."

Feld	Beschreibung
Virtual Router Backup	"Die Gruppe der VRRP-Router, welche die Verantwortung für das Weiterleiten übernehmen, falls der Master ausfallen sollte." Im Backup-Status sind diese VRRP-Router inaktiv, d.h. beantworten keine ARP-Requests."

18.13.1 Virtuelle Router

Bei der Verwendung eines Router-Redundanzprotokolls werden mehrere Router zu einer logischen Einheit zusammengefasst. Das Router-Redundanzprotokoll BRRP verwaltet die beteiligten Router und organisiert im einzelnen Folgendes:

Es stellt sicher, dass jeweils nur ein Router innerhalb des logischen Verbunds aktiv ist.

Es gewährleistet, dass bei Ausfall des aktiven Routers ein anderer Router die Funktion des ausgefallenen Geräts übernimmt. Wann welcher Router aktiv ist, wird über eine dem Router zugeordnete Priorität bestimmt.

Nehmen wir als Beispiel ein einfaches Szenario, in dem Gateway A den Internetzugang der Hosts in einem LAN ermöglicht. Wenn dieses Gateway ausfällt, haben alle Hosts keinen Zugang zum Internet, deren Routen statisch konfiguriert sind. Um den Hosts weiterhin Zugang zum Internet zu ermöglichen, bietet Gateway B allen Hosts im LAN den Dienst an, den vorher Gateway A durchgeführt hat. Alle Aufgaben eines virtuellen Routers und das Umschalten von Diensten von einem Gateway auf das andere werden von dem BRRP-Redundanzprotokoll gesteuert.

Das BRRP folgt den Spezifikationen in RFC 2338 und dem entsprechenden Internet- Entwurf (siehe www.ietf.org).

Die Konfiguration des Router-Redundanzverfahrens wird in folgenden Schritten durchgeführt:

- Konfiguration der Schnittstelle, über welche die BRRP-Advertisement-Datenpakete geschickt werden.



Hinweis

Diese Schnittstelle wird zur Übertragung der BRRP-Advertisement-Datenpakete sowie eventuell zur Übertragung von Keepalive-Monitoring-Datenpaketen verwendet. Zur Übertragung der Nutzdaten muss eine andere Schnittstelle im nächsten Schritt konfiguriert werden.

Die Konfiguration der Advertisement-Schnittstelle wird im Menü **Lokale Dienste->BRRP-**

>**Virtueller Router**->**Neu** unter **BRRP Advertisement-Schnittstelle** vorgenommen.

Nur der aktive Router des Routerverbunds sendet Advertisement-Datenpakete. Die IPv4-Multicast-Adresse 224.0.0.18 dient als Zieladresse für alle Router, die Bestandteil des Routerverbundes sind. Alle passiven Router des Verbundes müssen diese Adresse überwachen, damit sie bei Ausbleiben der Advertisement-Datenpakete entsprechend ihrer Priorität und der sonstigen BRRP-Konfiguration reagieren können.

- Konfiguration der Schnittstelle zur Übertragung von Nutzdaten (Konfiguration der virtuellen Schnittstelle).

Eine virtuelle Schnittstelle wird über die Zuweisung zu einem virtuellen Router über das BRRP-Router-Redundanzprotokoll aktiviert bzw. deaktiviert.

Die Konfiguration wird im Menü **Lokale Dienste**->**BRRP**->**Virtueller Router**->**Neu**->**Ethernet-Schnittstelle** vorgenommen.

In diesem Schritt konfigurieren Sie die IP-Adresseinstellungen und ordnen die Schnittstelle einem virtuellen Router zu. Darüber hinaus werden die Eigenschaften des virtuellen Routers (z. B. die Priorität) festgelegt.



Hinweis

Das System vergibt die MAC-Adresse der virtuellen Schnittstelle nach folgendem Schema automatisch: 00:00:5E:00:01:<ID des virtuellen Routers>. Die ID des virtuellen Routers bestimmt somit die MAC-Adresse der Schnittstelle, die zur Übertragung der Nutzdaten verwendet wird.

Die Konfiguration der virtuellen Schnittstelle (MAC-Adresse, IP-Adresse) sowie die Konfiguration des virtuellen Routers (Sendeintervall für Advertisements, 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.)

18.13.1.1 Neu

Wählen Sie die Schaltfläche **Neu** um weitere Virtuelle Router zu konfigurieren.

Virtuelle Router		VR-Synchronisation	Optionen
BRRP Advertisement-Schnittstelle			
Ethernet-Schnittstelle	Eine auswählen ▾		
IP-Adresse	IP-Adresse <input type="text"/> Netzmaske <input type="text"/>		
BRRP Überwachte Schnittstelle			
Schnittstelle des virtuellen Routers	Keine Advertisement-Schnittstelle ausgewählt!		
Router-IP-Adresse	IP-Adresse <input type="text"/>	Netzmaske <input type="text"/>	<input type="text"/>
	<input type="button" value="Hinzufügen"/>		
ID des virtuellen Routers	1 ▾		
Priorität des virtuellen Routers	100 ▾		
Erweiterte Einstellungen			
Sendintervall 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. 178: **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> <p>Hinweis: Die Ethernet-Schnittstelle zur Versendung der Advertisements ist immer up and running und kann daher nicht als Schnittstelle des virtuellen Routers verwendet werden.</p>
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>

Feld	Beschreibung
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> <p>Der Standardwert ist 100.</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
Sendeintervall für Advertisements	<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 1 und 255. Der Wert wird in Sekunden angegeben, Standardwert ist 1.</p> <p>Basierend auf diesem Sendeintervall für Advertisements läuft routerintern ein Advertisement Timer, nach dessen Ablauf ein Advertisement-Paket gesendet wird.</p>
Master down trials	<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 errech-</p>

Feld	Beschreibung
	<p>net 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> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 255, Standardwert ist 10.</p>
<p>Pre-Empt-Modus (zurück in Master-Status)</p>	<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 derzeitig aktiven 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>
<p>Authentisierung aktivieren</p>	<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>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

18.13.2 VR-Synchronisation

Im Menü **Lokale Dienste->BRRP->VR-Synchronisation** wird der Watchdog Daemon konfiguriert, d. h. Sie legen fest, wie Statusänderungen gehandhabt werden.

Nach Öffnen des Menüs **Lokale Dienste->BRRP->VR-Synchronisation** wird eine Liste aller Synchronisationen angezeigt. Sie können entweder virtuelle Router untereinander synchronisieren oder Schnittstellen. Neue Synchronisationen können im Menü **Neu** hinzugefügt werden.

Sie können z. B. die beiden virtuellen Router R1 und R2 über BRRP synchronisieren. Dazu müssen Sie zwei Einträge anlegen. Für den ersten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R1 und als **Synchronisations-VR/Schnittstelle** R2 verwenden. Für den zweiten Eintrag müssen Sie als **Monitoring-VR/Schnittstelle** R2 und als **Synchronisations-VR/Schnittstelle** R1 konfigurieren.

18.13.2.1 Neu

Wählen Sie die Schaltfläche **Neu** um neue Synchronisationen hinzuzufügen.

Virtuelle Router
VR-Synchronisation
Optionen

Basisparameter	
Monitoring-VR/Schnittstelle	
Monitoring-Modus	BRRP ▾
ID des virtuellen Routers	Eine auswählen ▾
Synchronisations-VR/Schnittstelle	
Synchronisationsmodus	BRRP ▾
ID des virtuellen Routers	Eine auswählen ▾

OK
Abbrechen

Abb. 179: **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.)
ID des virtuellen Routers	<p>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.</p>

Felder im Menü Synchronisations-VR/Schnittstelle

Feld	Beschreibung
Synchronisationsmodus	<p>Zeigt an, mit welchem Mechanismus virtuelle Router bzw. Schnittstellen synchronisiert werden:</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>BRRP</i>: BRRP wird für die Synchronisierung der virtuellen Router verwendet.
ID des virtuellen Routers	<p>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.</p>

18.13.3 Optionen

Im Menü **Lokale Dienste->BRRP->Optionen** können Sie die Funktion BRRP ein- oder ausschalten.

The screenshot shows a web interface with three tabs: 'Virtuelle Router', 'VR-Synchronisation', and 'Optionen'. The 'Optionen' tab is active. Below the tabs is a 'Basisparameter' section containing a table with one row: 'BRRP aktivieren' with an unchecked checkbox and the label 'Aktiviert'. At the bottom of the section are two buttons: 'OK' and 'Abbrechen'.

Abb. 180: 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.

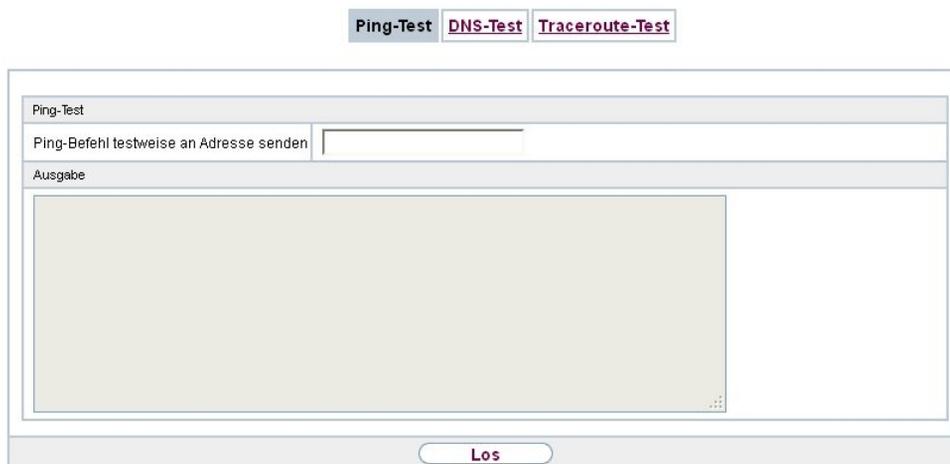
Kapitel 19 Wartung

Im diesem Menü werden Ihnen zahlreiche Funktionen zur Wartung Ihres Geräts zur Verfügung gestellt. So finden Sie zunächst eine Menü zum Testen der Erreichbarkeit innerhalb des Netzwerks. Sie haben die Möglichkeit Ihre Systemkonfigurationsdateien zu verwalten. Falls aktuellere Systemsoftware zur Verfügung steht, kann die Installation über dieses Menü vorgenommen werden. Falls Sie weitere Sprachen der Konfigurationsoberfläche benötigen, können Sie diese importieren. Auch ein System-Neustart kann in diesem Menü ausgelöst werden.

19.1 Diagnose

Im Menü **Wartung**->**Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

19.1.1 Ping-Test



The screenshot shows a web interface for network diagnostics. At the top, there are three buttons: "Ping-Test" (highlighted in blue), "DNS-Test", and "Traceroute-Test". Below these is a main container with a header "Ping-Test". Inside, there is a label "Ping-Befehl testweise an Adresse senden" followed by an empty text input field. Below that is a label "Ausgabe" followed by a large, empty rectangular area for displaying test results. At the bottom of the container is a button labeled "Los".

Abb. 181: **Wartung**->**Diagnose**->**Ping-Test**

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an. Durch Eingabe der IP-Adresse, die getestet werden soll, in **Ping-Befehl testweise an Adresse senden** und Klicken auf die **Los**-Schaltfläche wird der Ping-Test gestartet.

19.1.2 DNS-Test

The screenshot shows a web interface for a DNS test. At the top, there are three buttons: 'Ping-Test', 'DNS-Test', and 'Traceroute-Test'. The 'DNS-Test' button is highlighted. Below the buttons is a form with a header 'DNS-Test'. It contains a text input field labeled 'DNS-Adresse', an empty output area labeled 'Ausgabe', and a 'Los' button at the bottom.

Abb. 182: **Wartung->Diagnose->DNS-Test**

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domänennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

19.1.3 Traceroute-Test

The screenshot shows a web interface for a Traceroute test. At the top, there are three buttons: 'Ping-Test', 'DNS-Test', and 'Traceroute-Test'. The 'Traceroute-Test' button is highlighted. Below the buttons is a form with a header 'Traceroute-Test'. It contains a text input field labeled 'Traceroute-Adresse', an empty output area labeled 'Ausgabe', and a 'Los' button at the bottom.

Abb. 183: **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. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an. Durch Eingabe der Adresse, die getestet werden soll, in **Traceroute-Adresse** und Klicken auf die **Los**-Schaltfläche wird der Traceroute-Test gestartet.

19.2 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

19.2.1 Optionen

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Daher müssen Sie gegebenenfalls ein Software-Update durchführen.

Jede neue Systemsoftware beinhaltet neue Funktionen, bessere Leistung und bei Bedarf Fehlerkorrekturen der vorhergehenden Version. Die aktuelle Systemsoftware finden Sie unter www.bintec-elmeg.com. Hier finden Sie auch aktuelle Dokumentationen.



Wichtig

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörigen Release Notes. Hier sind alle Änderungen beschrieben, die mit der neuen Systemsoftware eingeführt werden.

Die Folge von unterbrochenen Update-Vorgängen (z. B. Stromausfall während des Updates) könnte sein, dass Ihr Gerät nicht mehr bootet. Schalten Sie Ihr Gerät nicht aus, während die Aktualisierung durchgeführt wird.

In seltenen Fällen ist zusätzlich eine Aktualisierung von BOOTmonitor und/oder Logic empfohlen. In diesem Fall wird ausdrücklich in den entsprechenden Release Notes darauf hingewiesen. Führen Sie bei BOOTmonitor oder Logic nur ein Update durch, wenn bintec elmeg GmbH eine explizite Empfehlung dazu ausspricht.

Flash

Ihr Gerät speichert seine Konfiguration in Konfigurationsdateien im Flash EEPROM (electrically erasable programmable read-only memory). Auch wenn Ihr Gerät ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

RAM

Im Arbeitsspeicher (RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf Ihrem Gerät einstellen. Der Inhalt des RAM geht verloren, wenn Ihr Gerät ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start Ihres Geräts beibehalten wollen, müssen Sie die geänderte Konfiguration im Flash speichern: Schaltfläche **Konfiguration speichern** über dem Navigationsbereich des **GUIs**. Dadurch wird die Konfiguration in eine Datei mit dem Namen *boot* im Flash gespeichert. Beim Starten Ihres Geräts wird standardmäßig die Konfigurationsdatei *boot* verwendet.

Aktionen

Die Dateien im Flash-Speicher können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen Ihrem Gerät und einem Host per HTTP zu transferieren.

Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden. So können Sie mit den Aktionen "Konfiguration exportieren", "Konfiguration mit Statusinformationen exportieren" und "Konfiguration laden" Dateien sichern bzw. einspielen. Wenn Sie mit der Aktion "Konfiguration exportieren" oder "Konfiguration mit Statusinformationen exportieren" eine Konfigurationsdatei sichern wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll.



Achtung

Sollten Sie über die SNMP-Shell mit dem Kommando `put` eine Konfigurationsdatei in einem alten Format gesichert haben, kann ein Wiedereinspielen auf das Gerät nicht garantiert werden. Daher wird das alte Format nicht mehr empfohlen.

Optionen

Aktuell Installierte Software	
BOSS	V.9.1 Rev. 8 (Beta 1) from 2014/01/16 00:00:00
Systemlogik	1.1
Optionen zu Software und Konfiguration	
Aktion	Keine Aktion <input type="button" value="v"/>

Abb. 184: **Wartung->Software & Konfiguration ->Optionen**

Das Menü **Wartung->Software & Konfiguration ->Optionen** besteht aus folgenden Feldern:

Felder im Menü Aktuell Installierte Software

Feld	Beschreibung
BOSS	Zeigt die aktuelle Softwareversion an, die auf Ihrem Gerät geladen ist.
Systemlogik	Zeigt die aktuelle Systemlogik an, die auf Ihrem Gerät geladen ist.
ADSL-Logik	Zeigt die aktuelle Version der ADSL-Logik an, die auf Ihrem Gerät geladen ist.

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	<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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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. Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben! • <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>Sicherung wiederherstellen</i>: Nur, wenn unter Konfiguration speichern mit der Einstellung <i>Konfiguration speichern und 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. • <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.bintec-elmeg.com 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>Voice Mail Wave-Dateien importieren</i> (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist.): Wählen Sie in Dateiname die Datei <i>vms_wavfiles.zip</i> aus, die Sie importieren wollen. • <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

Feld	Beschreibung
	Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.
Aktueller Dateiname im Flash	Für Aktion = <i>Konfiguration exportieren</i> Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.
Zertifikate und Schlüssel einschließen	Für Aktion = <i>Konfiguration exportieren</i> Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Verschlüsselung der Konfiguration	Nur für Aktion = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i> Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Passwort eingeben.
Dateiname	Nur für Aktion = <i>Konfiguration importieren, Sprache importieren, Systemsoftware aktualisieren</i> Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.
Name der Quelldatei	Nur für Aktion = <i>Konfiguration kopieren</i> Wählen Sie die Quelldatei aus, die kopiert werden soll.
Name der Zieldatei	Nur für Aktion = <i>Konfiguration kopieren</i> Geben Sie den Namen der Kopie ein.

Feld	Beschreibung
Datei auswählen	Nur für Aktion = <i>Konfiguration löschen, Konfiguration umbenennen</i> oder <i>Software/Firmware löschen</i> Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.
Neuer Dateiname	Nur für Aktion = <i>Konfiguration umbenennen</i> Geben Sie den neuen Namen der Konfigurationsdatei ein.
Quelle	Nur für Aktion = <i>Systemsoftware aktualisieren</i> Wählen Sie die Quelle der Aktualisierung aus. Mögliche Werte: <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 Update-Server</i>: Die Datei liegt auf dem offiziellen Update-Server.
URL	Nur für Aktion = <i>Systemsoftware aktualisieren</i> und Quelle = <i>HTTP-Server</i> Geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.

19.3 Neustart

19.3.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **GUI** neu aufrufen und sich wieder anmelden.

Beobachten Sie dazu die LEDs an Ihrem Gerät. Für die Bedeutung der LEDs lesen Sie bitte in dem Handbuch-Kapitel **Technische Daten**.

**Hinweis**

Stellen Sie vor einem Neustart sicher, dass Sie Ihre Konfigurationsänderungen durch Klicken auf die Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.



Abb. 185: **Wartung->Neustart->Systemneustart**

Wenn Sie Ihr Gerät neu starten wollen, klicken Sie auf die **OK**-Schaltfläche. Der Neustart wird ausgeführt.

Kapitel 20 Externe Berichterstellung

In diesem Menü legen Sie fest, welche Systemprotokoll-Nachrichten auf welchem Rechner gespeichert werden und ob der Systemadministrator bei bestimmten Ereignissen eine Email erhalten soll. Informationen über den IP-Datenverkehr können - bezogen auf die einzelnen Schnittstellen - ebenfalls gespeichert werden. Darüber hinaus können im Fehlerfall SNMP-Traps an bestimmte Hosts versandt werden. Außerdem können Sie Ihr Gerät für die Überwachung mit dem Activity Monitor vorbereiten.

20.1 Systemprotokoll

Ereignisse in den verschiedenen Subsystemen Ihres Geräts (z. B. PPP) werden in Form von Systemprotokoll-Nachrichten (Syslog) protokolliert. Je nach eingestelltem Level (acht Stufen von *Notfall* über *Informationen* bis *Debug*) werden dabei mehr oder weniger Meldungen sichtbar.

Zusätzlich zu den intern auf Ihrem Gerät protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf Ihrem Gerät intern gespeicherte Systemprotokoll-Nachrichten gehen bei einem Neustart verloren.



Warnung

Achten Sie darauf, die Systemprotokoll-Nachrichten nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, dass jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

Syslog-Daemon

Die Erfassung der Systemprotokoll-Nachrichten wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (abrufbar im Download-Bereich unter www.bintec-elmeg.com).

20.1.1 Syslog-Server

Konfigurieren Sie Ihr Gerät als Syslog-Server, sodass die definierten Systemmeldungen an geeignete Hosts im LAN geschickt werden können.

In diesem Menü definieren Sie, welche Meldungen mit welchen Bedingungen zu welchem Host geschickt werden.

Im Menü **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** wird eine Liste aller konfigurierten Systemprotokoll-Server angezeigt.

20.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.

Syslog-Server

Basisparameter	
IP-Adresse	<input type="text"/>
Level	Informationen <input type="button" value="v"/>
Facility	local0 <input type="button" value="v"/>
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. 186: **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** -> **Neu**

Das Menü **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität)

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <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 (Standardwert)</p> <p><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>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System &Accounting</i> (Standardwert) • <i>System</i> • <i>Accounting</i>

20.2 IP-Accounting

In modernen Netzwerken werden häufig aus kommerziellen Gründen Informationen über Art und Menge der Datenpakete gesammelt, die über die Netzwerkverbindungen übertragen und empfangen werden. Für Internet Service Provider, die ihre Kunden nach Datenvolumen abrechnen, ist das von entscheidender Bedeutung.

Aber auch nicht-kommerzielle Zwecke sprechen für ein 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.

20.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

The screenshot shows the 'Schnittstellen' menu with the following table:

Nr.	Schnittstelle	IP-Accounting
1	en1-4	<input type="checkbox"/>
2	en1-0	<input type="checkbox"/>

Additional interface elements include: 'Ansicht 20 pro Seite', 'Filtern in Keiner', 'gleich', 'Los', and 'Seite: 1, Objekte: 1 - 2'.

Abb. 187: Externe Berichterstellung->IP-Accounting->Schnittstellen

Im Menü **Externe Berichterstellung->IP-Accounting->Schnittstellen** wird eine Liste aller auf Ihrem Gerät konfigurierten Schnittstellen angezeigt. Für jeden Eintrag kann durch Setzen eines Hakens die Funktion IP-Accounting aktiviert werden. In der Spalte **IP-**

Accounting müssen Sie nicht jeden Eintrag einzeln anklicken. Über die Optionen **Alle auswählen** oder **Alle deaktivieren** können Sie die Funktion IP-Accounting für alle Schnittstellen gleichzeitig aktivieren bzw. deaktivieren.

20.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

The screenshot shows a software interface with two tabs: 'Schnittstellen' and 'Optionen'. The 'Optionen' tab is selected. Below the tabs is a text input field labeled 'Protokollformat' containing the text 'INET: %d %t %a %c %i:%r%f-> %l:%R/%F %p %o %P %O [%s]'. At the bottom of the window are two buttons: 'OK' and 'Abbrechen'.

Abb. 188: 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

Feld	Beschreibung
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen:

```
INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

20.3 Benachrichtigungsdienst

Bisher war es schon möglich Syslog-Meldungen vom Router an einen beliebigen Syslog-Host übertragen zu lassen. Mit dem Benachrichtigungsdienst werden dem Administrator je nach Konfiguration E-Mails gesendet, sobald relevante Syslog-Meldungen auftreten.

20.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

20.3.1.1 Neu

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

Benachrichtigungsempfänger Benachrichtigungseinstellungen

Benachrichtigungsempfänger hinzufügen/bearbeiten	
Benachrichtigungsdienst	E-Mail
Empfänger	<input type="text"/>
Nachrichtenkomprimierung	<input checked="" type="checkbox"/> Aktiviert
Betreff	<input type="text"/>
Ereignis	Systemmeldung enthält Zeichenfolge <input type="button" value="v"/>
Enthaltene Zeichenfolge	<input type="text"/> (Wildcards zulässig)
Schweregrad	Notfall <input type="button" value="v"/>
Überwachte Subsysteme	<input type="text"/> Subsystem <input type="button" value="Hinzufügen"/>
Timeout für Nachrichten	<input type="text" value="60"/>
Anzahl Nachrichten	<input type="text" value="1"/>

Abb. 189: Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungsempfänger -> Neu

Das Menü **Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungs-**

empfänger->Neu besteht aus folgenden Feldern:

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungsdienst	<p>Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • E-Mail • SMS
Empfänger	<p>Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.</p>
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	<p>Sie können einen Betreff eingeben.</p>
Ereignis	<p>Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar.</p> <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 Rough 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 unkonfigurierter AP hat sich beim WLAN Controller gemeldet. • <i>Verwalteter AP offline</i>: Ein managed AP ist nicht mehr

Feld	Beschreibung
	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 Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.</p>
Schweregrad	<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>
Überwachte Subsysteme	<p>Wählen Sie die Subsysteme aus, die überwacht werden sollen.</p> <p>Fügen Sie mit Hinzufügen neue Subsysteme hinzu.</p>
Timeout für Nachrichten	<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. Standardwert ist 60.</p>
Anzahl Nachrichten	<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>

20.3.2 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. 190: 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>Keine</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 600 Sekunden.</p>

Felder im Menü SMS Parameter (nur für Geräte mit UMTS)

Feld	Beschreibung
SMS-Gerät	Sie können sich über Systemmeldungen per SMS informieren

Feld	Beschreibung
	lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
Maximale SMS pro Tag	<p>Begrenzen Sie hier die Anzahl der an einem Tag versendeten SMS.</p> <p>Die Aktivierung von <i>Uneingeschränkt</i> erlaubt eine beliebige Anzahl an versendeten SMS.</p> <p>Der Standardwert beträgt 10 SMS pro Tag.</p> <p>Hinweis: Die Eingabe des Wertes 0 ist gleichbedeutend mit der Aktivierung von <i>Uneingeschränkt</i>.</p>

20.4 SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll in der IP-Protokollfamilie für den Transport von Managementinformationen über Netzwerkkomponenten.

Zu den Bestandteilen eines jeden SNMP-Managementsystems zählt u. a. eine MIB. Über SNMP sind verschiedene Netzwerkkomponenten von einem System aus zu konfigurieren, zu kontrollieren und zu überwachen. Mit Ihrem Gerät haben Sie ein solches SNMP-Werkzeug erhalten, den Konfigurationsmanager. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HPOpenView verwenden.

Weitergehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

20.4.1 SNMP-Trap-Optionen

Zur Überwachung des Systems wird im Fehlerfall unaufgefordert eine Nachricht gesendet, ein sogenanntes Trap-Paket.

Im Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Optionen** können Sie das Senden von Traps konfigurieren.

SNMP-Trap-Optionen SNMP-Trap-Hosts

Basisparameter	
SNMP Trap Broadcasting	<input checked="" type="checkbox"/> Aktiviert
SNMP-Trap-UDP-Port	<input type="text" value="162"/>
SNMP-Trap-Community	<input type="text" value="snmp-Trap"/>

OK Abbrechen

Abb. 191: 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>

20.4.2 SNMP-Trap-Hosts

In diesem Menü geben Sie an, an welche IP-Adressen Ihr Gerät die SNMP-Traps schicken soll.

Im Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Hosts** wird eine Liste aller konfigurierten SNMP-Trap-Hosts angezeigt.

20.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

Abb. 192: **Externe Berichterstellung ->SNMP->SNMP-Trap-Hosts->Neu**

Das Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

20.5 Activity Monitor

Im diesem Menü finden Sie die Einstellungen, die nötig sind, um Ihr Gerät mit dem Windows-Tool **Activity Monitor** (Bestandteil von **BRICKware** for Windows) überwachen zu können.

Zweck

Mit dem **Activity Monitor** können Windows-Nutzer die Aktivitäten ihres Geräts überwachen. Wichtige Informationen über den Status von physikalischen Schnittstellen (z. B. ISDN-Leitung) und virtuellen Schnittstellen sind leicht mit einem einzigen Tool erreichbar. Ein permanenter Überblick über die Auslastung der Schnittstellen Ihres Geräts ist damit

möglich.

Funktionsweise

Ein Status-Daemon sammelt Informationen über Ihr Gerät und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse der ersten LAN-Schnittstelle (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro Zeitintervall, das individuell einstellbar ist auf Werte von 1 - 60 Sekunden, wird gesendet. Bis zu 100 physikalische und virtuelle Schnittstellen können überwacht werden, soweit die Paketgröße von 4096 Bytes nicht überschritten wird. Der **Activity Monitor** auf Ihrem PC empfängt die Pakete und kann die enthaltenen Informationen je nach Konfiguration auf verschiedene Arten darstellen.

Um den **Activity Monitor** zu aktivieren, müssen Sie:

- das/die zu überwachende(n) Gerät(e) entsprechend konfigurieren
- die Windows-Anwendung auf Ihrem PC starten und konfigurieren (**BRICKware** for Windows, können Sie vom Download-Bereich auf www.bintec-elmeg.com auf Ihren PC herunterladen und von da aus in Ihr Gerät einspielen).

20.5.1 Optionen

Optionen

Basisparameter	
Überwachte Schnittstellen	<input checked="" type="radio"/> Keine <input type="radio"/> Physikalisch <input type="radio"/> Physikalisch/WAN/VPN
Informationen senden an	Alle IP-Adressen (Broadcast) ▾
Aktualisierungsintervall	5 Sekunden
UDP-Zielport	2107
Passwort	••••••••
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 193: Externe Berichterstellung ->Activity Monitor->Optionen

Das Menü **Externe Berichterstellung ->Activity Monitor->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstellen	Wählen Sie die Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden soll.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Deaktiviert das Senden von Informationen an den Activity Monitor. • <i>Physikalisch</i>: Nur Informationen über physikalische Schnittstellen werden gesendet. • <i>Physikalisch/WAN/VPN</i>: Informationen über physikalische und virtuelle Schnittstellen werden gesendet.
Informationen senden an	<p>Wählen Sie aus, an wen Ihr Gerät die UDP Pakete schicken soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle IP-Adressen (Broadcast)</i> (Standardwert): Mit dem Standardwert <i>255.255.255.255</i> wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet. • <i>Einzelner Host</i>: Die UDP-Pakete werden an die im nebenstehenden Eingabefeld eingetragene IP-Adresse geschickt.
Aktualisierungsintervall	<p>Geben Sie das Aktualisierungsintervall (in Sekunden) ein.</p> <p>Mögliche Werte sind <i>0</i> bis <i>60</i></p> <p>Standardwert ist <i>5</i>.</p>
UDP-Zielport	<p>Geben Sie die Port-Nummer für die Windows-Anwendung Activity Monitor ein.</p> <p>Standardwert ist <i>2107</i> (registriert durch IANA - Internet Assigned Numbers Authority).</p>
Passwort	<p>Geben Sie das Passwort für den Activity Monitor ein.</p>

Kapitel 21 Monitoring

Dieses Menü enthält Informationen, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten, z. B. an der WAN-Schnittstelle Ihres Geräts, ermöglichen.

21.1 Internes Protokoll

21.1.1 Systemmeldungen

Im Menü **Monitoring->Internes Protokoll->Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die konfigurierten Werte der Felder **Maximale Anzahl der Syslog-Protokolleinträge** und **Maximales Nachrichtenlevel von Systemprotokolleinträgen**. Diese Werte können im Menü **Systemverwaltung->Globale Einstellungen->System** verändert werden.

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="text" value="gleich"/> <input type="button" value="Los"/>					
Nr.	Datum	Zeit	Level	Subsystem	Nachricht
1	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
2	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
3	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
4	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
5	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas5Ghz not found
6	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas5Ghz
7	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanVSSTable
8	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanIFTable
9	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
10	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
11	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
12	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
13	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas5Ghz not found
14	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas5Ghz
15	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanVSSTable
16	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanIFTable
17	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
18	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
19	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
20	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
Seite: 1, Objekte: 1 - 20, Summe der Objekte: 43					

Abb. 194: 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.

21.2 IPsec

21.2.1 IPSec-Tunnel

Im Menü **Monitoring->IPSec->IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.



Abb. 195: **Monitoring->IPSec->IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

Durch Klicken auf die -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der IPSec-Verbindung geändert.

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

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. 196: Monitoring->IPSec->IPSec-Tunnel-> 

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Peers an.
Lokale IP-Adresse	Zeigt die WAN-IP-Adresse Ihres Geräts an.
Entfernte IP-Adresse	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
Lokale ID	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
Entfernte ID	Zeigt die ID des Peers an.
Aushandlungsmodus	Zeigt den Aushandlungsmodus an.
Authentifizierungsmethode	Zeigt die Authentifizierungsmethode an.
MTU	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
Erreichbarkeitsprüfung	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
NAT-Erkennung	Zeigt die NAT-Erkennungsmethode an.
Lokaler Port	Zeigt den lokalen Port an.
Entfernter Port	Zeigt den entfernten Port an.
Pakete	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
Bytes	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
Fehler	Zeigt die Anzahl der Fehler an.

Feld	Beschreibung
IKE (Phase-1) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IKE (Phase 1) SAs an.
IPSec (Phase-2) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

21.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

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. 197: **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.

21.3 ISDN/Modem

21.3.1 Aktuelle Anrufe

Im Menü **Monitoring->ISDN/Modem->Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.



Abb. 198: **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>

21.3.2 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

 gleich
Los

#	Dienst	Entfernte Nummer	Schnittstelle	Richtung	Kosten	Startzeit	Dauer
Seite: 1							

Abb. 199: 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.

21.4 Schnittstellen

21.4.1 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. 200: Monitoring->Schnittstellen->Statistik

Durch Klicken auf die -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert.

Werte in der Liste Statistik

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der Schnittstelle an.
Beschreibung	Zeigt den Namen der Schnittstelle an.
Typ	Zeigt den Schnittstellentyp an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.
Rx-Fehler	Zeigt die Gesamtzahl der erhaltenen Fehler an.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Nicht geändert seit	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt 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:a0f9:21: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. 201: Monitoring->Schnittstellen->Statistik-> 

Werte in der Liste Statistik

Feld	Beschreibung
Beschreibung	Zeigt den Namen der Schnittstelle an.
MAC-Adresse	Zeigt den Schnittstellentyp an.
IP-Adresse/Netzmaske	Zeigt die IP-Adresse und die Netzmaske an.
NAT	Zeigt an, ob NAT für diese Schnittstelle aktiviert ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.

Feld im Menü TCP-Verbindungen

Feld	Beschreibung
Status	Zeigt den Status einer aktiven TCP-Verbindung an.
Lokale Adresse	Zeigt die lokale IP-Adresse der Schnittstelle für eine aktive TCP-Verbindung an.
Lokaler Port	Zeigt den lokalen Port der IP-Adresse für eine aktive TCP-Verbindung an.
Remote-Adresse	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

21.5 WLAN

21.5.1 WLANx

Im Menü **Monitoring->WLAN->WLAN** werden die aktuellen Werte und Aktivitäten der WLAN-Schnittstelle angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1 WLAN2 VSS Client-Verwaltung Bridge-Links Client Links		
Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen		
WLAN1Statistik		
Mbit/s	Tx-Pakete	Rx-Pakete
802.11a/b/g		
54	0	0
48	0	0
36	0	0
24	0	0
18	0	0
12	0	0
11	0	0
9	0	0
6	0	0
5	0	0
2	0	0
1	0	0
802.11n		
144,4	0	0
139	0	0
115,6	0	0
86,7	0	0
72,2	0	0
65	0	0
57,8	0	0
43,3	0	0
28,9	0	0
21,7	0	0
14,4	0	0
7,2	0	0
Gesamt	0	0
Erweitert		

Abb. 202: **Monitoring->WLAN->WLAN**

Werte in der Liste WLAN

Feld	Beschreibung
Mbit/s	Zeigt die möglichen Datenraten auf diesem Funkmodul an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete für die in Mbit/s

Feld	Beschreibung
	angezeigte Datenrate an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete für die in Mbit/s angezeigte Datenrate an.

Über die Schaltfläche **Erweitert** gelangen Sie in eine Übersicht über weitere Details.

[WLAN1](#) [WLAN2](#) [VSS](#) [Client-Verwaltung](#) [Bridge-Links](#) [Client Links](#)

Automatisches Aktualisierungsintervall Sekunden [Übernehmen](#)

#	Beschreibung	Wert
1	Unicast MSDUs erfolgreich übertragen	0
2	Erfolgreich übertragene Multicast-MSDUs	0
3	Übertragene MPDUs	0
4	Erfolgreich empfangene Multicast-MSDUs	0
5	Unicast MPDUs erfolgreich erhalten	0
6	MSDUs, die nicht übertragen werden konnten	0
7	Frame-Übertragungen ohne ACK	0
8	Doppelte empfangene MSDUs	0
9	CTS Frames als Antwort auf RTS empfangen	0
10	Nicht entschlüsselbare MPDUs erhalten	0
11	RTS Frames ohne CTS	0
12	Fehlerhafte Erhaltene Pakete	0

[Zurück](#)

Abb. 203: Monitoring->WLAN->WLAN->Erweitert

Werte in der Liste Erweitert

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des angezeigten Werts an.
Wert	Zeigt den entsprechenden statistischen Wert an.

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Unicast MSDUs erfolgreich übertragen	Zeigt die Anzahl der erfolgreich an Unicast-Adressen versandten MSDUs seit dem letzten Reset an. Zu jedem dieser Pakete wurde ein Acknowledgement empfangen.
Erfolgreich übertragene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich an Multicast-Adressen (inklusive der Broadcast MAC-Adresse) versandten MSDUs an.
Übertragene MPDUs	Zeigt die Anzahl der erfolgreich empfangenen MPDUs an.
Erfolgreich empfangene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Multicast-Adresse versandt wurden.
Unicast MPDUs erfolg-	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die

Beschreibung	Bedeutung
reich erhalten	mit einer Unicast-Adresse versandt wurden.
MSDUs, die nicht übertragen werden konnten	Zeigt die Anzahl der MSDUs an, die nicht gesendet werden konnten.
Frame-Übertragungen ohne ACK	Zeigt die Anzahl der gesendeten Frames an, für die kein Acknowledgement-Frame empfangen wurde.
Doppelte empfangene MSDUs	Zeigt die Anzahl von doppelt empfangenen MSDUs an.
CTS Frames als Antwort auf RTS empfangen	Zeigt die Anzahl der empfangenen CTS (Clear to send)-Frames an, die als Antwort auf RTS (Request to send) empfangen wurden.
Nicht entschlüsselbare MPDUs erhalten	Zeigt die Anzahl der empfangenen MPDUs an, die nicht entschlüsselt werden konnten. Ein Grund dafür könnte sein, dass kein passender Schlüssel eingetragen wurde.
RTS Frames ohne CTS	Zeigt die Anzahl der RTS-Frames an, für die kein CTS empfangen wurde.
Fehlerhafte Erhaltene Pakete	Zeigt die Anzahl der Frames an, die unvollständig oder fehlerhaft empfangen wurden.

21.5.2 VSS

Im Menü **Monitoring->WLAN->VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.

WLAN1 WLAN2 VSS Client-Verwaltung Bridge-Links Client Links

Automatisches Aktualisierungsintervall Sekunden Übernehmen

Client-Node-Tabelle

MAC-Adresse	IP-Adresse	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s	
Funkwerk-ec (vss1-0)								
00:d:f0:67:55:f3	0.0.0.0	0 Tag(e) 0:1:57	1	3	-99(0,0,0)	-98	1	🔍

Abb. 204: Monitoring->WLAN->VSS

Werte in der Liste VSS

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der je-

Feld	Beschreibung
	weilige Client angemeldet ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	<p>Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an.</p> <p>Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s.</p> <p>Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.</p>

VSS - Details für Verbundene Clients

Im Menü **Monitoring->WLAN->VSS-><Verbundener Client>->**  werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1 WLAN2 VSS Client-Verwaltung Bridge-Links Client Links						
Automatisches Aktualisierungsintervall		60	Sekunden		Übernehmen	
Client-MAC-Adresse	IP-Adresse	Uptime	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	SNR dB	Datenrate Mbit/s
00:01:cd:06:1a:b4	10.0.0.234	0 Tag(e) 0:0:27	-88(-90,-88,-88)	-87	-1	12
Rate		Tx-Pakete	Rx-Pakete			
802.11 a/b/g						
54		0	0			
48		0	0			
36		0	0			
24		0	518			
18		0	89.27k			
12		0	8.39k			
11		4	0			
9		0	0			
6		0	519			
5.5		0	0			
2		2	0			
1		0	75			
802.11n						
300		0	0			
270		0	0			
240		0	0			
180		0	0			
150		0	0			
135		0	0			
120		0	0			
90		0	0			
60		0	701			
45		0	0			
30		0	0			
15		0	0			
Gesamt		6	215.36k			
Zurück						

Abb. 205: **Monitoring->WLAN->VSS-><Verbundener Client>->** 

Werte in der Liste <Verbundener Client>

Feld	Beschreibung
Client-MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen

Feld	Beschreibung
	<p>Indikator für die Qualität der Verbindung im Funk dar.</p> <p>Werte:</p> <ul style="list-style-type: none"> • > 25 dB exzellent • 15 – 25 dB gut • 2 – 15 dB grenzwertig • 0 – 2 dB schlecht.
Datenrate Mbit/s	<p>Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.</p>
Rate	<p>Zeigt die möglichen Datenraten auf dem Funkmodul an.</p>
Tx-Pakete	<p>Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.</p>
Rx-Pakete	<p>Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.</p>

21.5.3 Client Links

Im Menü **Monitoring->WLAN->Client Links** werden die aktuellen Werte und Aktivitäten der Client Links angezeigt.

[WLAN1](#)
[WLAN2](#)
[VSS](#)
[Client-Verwaltung](#)
[Bridge-Links](#)
[Client Links](#)

Automatisches Aktualisierungsintervall | 60 Sekunden [Übernehmen](#)

Client Links

Beschreibung des Client Links	AP-MAC-Adresse	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s	
WLAN1 (SSID1)								
sta7-90		36d 5h 8m 1s	0	0	0(0,0,0)	0	0	

Abb. 206: **Monitoring->WLAN->Client Links**

Werte in der Liste Client Links

Feld	Beschreibung
Beschreibung des Client Links	<p>Zeigt den Namen des Client Links an.</p>

Feld	Beschreibung
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.

Client Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Client Links.

[WLAN1](#)
[WLAN2](#)
[VSS](#)
[Client-Verwaltung](#)
[Bridge-Links](#)
[Client Links](#)

Automatisches Aktualisierungsintervall		60 Sekunden		Übernehmen		
AP-MAC-Adresse	Uptime	Signal dBm(RSSI1, RSSI2, RSSI3)		Rauschen dBm	SNR dB	Datenrate Mbit/s
	36d 5h 10m 41s	0(0,0,0)		0	0	0
Rate		Tx-Pakete		Rx-Pakete		
802.11a/b/g						
54		0		0		
48		0		0		
36		0		0		
24		0		0		
18		0		0		
12		0		0		
11		0		0		
9		0		0		
6		0		0		
5		0		0		
2		0		0		
1		0		0		
802.11n						
144,4		0		0		
139		0		0		
115,6		0		0		
86,7		0		0		
72,2		0		0		
65		0		0		
57,8		0		0		
43,3		0		0		
28,9		0		0		
21,7		0		0		
14,4		0		0		
7,2		0		0		
Gesamt		0		0		

Zurück

Abb. 207: Monitoring->WLAN->Client Links->

Werte in der Liste Client Links

Feld	Beschreibung
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Zeigt die Qualität des Signals in dB an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrates der auf diesem Client Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-

Feld	Beschreibung
	Pakete und Rx-Pakete einzeln an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

21.6 Bridges

21.6.1 br<x>

Im Menü **Monitoring->Bridges->br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

br0

Automatisches Aktualisierungsintervall	60	Sekunden	Übernehmen
MAC-Adresse	00:a0:f9:0b:08:98		Port
			en1-0

Abb. 208: **Monitoring->Bridges**

Werte in der Liste br<x>

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adressen der assoziierten Bridges an.
Port	Zeigt den Port an, auf dem die Bridge aktiv ist.

21.7 Hotspot-Gateway

21.7.1 Hotspot-Gateway

Im Menü **Monitoring->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

Hotspot-Gateway

Automatisches Aktualisierungsintervall Sekunden

Authentifizierter Hotspot-Benutzer

Benutzername	IP-Adresse	Physische Adresse	Anmeldung	Schnittstelle

Abb. 209: **Monitoring->Hotspot-Gateway->Hotspot-Gateway**

Werte in der Liste Hotspot-Gateway

Feld	Beschreibung
Benutzername	Zeigt den Namen des Benutzers an.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Physische Adresse	Zeigt die Physische Adresse des Benutzers an.
Anmeldung	Zeigt den Zeitpunkt der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

21.8 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

21.8.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

QoS

QoS

Schnittstelle	QoS-Gueue	Senden	Verworfen	Queued

Abb. 210: **Monitoring->QoS->QoS**

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.

Feld	Beschreibung
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

Glossar

2G	Siehe GSM.
3DES	Siehe DES.
3G	Siehe UMTS.
4G	Siehe LTE.
802.11	Die Norm 802.11 beschreibt Wireless LAN (WLAN). Es existieren verschiedene Erweiterungen: 802.11a: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 5 GHz, 802.11b: Brutto-Datentransferrate: 11 Mbit/s, Frequenzband: 2,4 GHz, 802.11g: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 2,4 GHz, 802.11n: Brutto-Datentransferrate: 600 Mbit/s, Frequenzband: 2,4 GHz (optional: 5 GHz)
Access Client	Der Client Mode ist eine Betriebsart eines Wireless Access Points (AP), bei dem sich dieser gegenüber dem übergeordneten AP wie ein Wireless Adapter verhält. Mit einem im Client Mode betriebenen AP können einzelne Rechner oder ganze Subnetze an übergeordnete Netze angebunden werden.
Access Point	Ein Access Point (AP) ist ein Gerät zur drahtlosen Verbindung von Clients (Computern). Der AP dient somit zum Aufbau eines Funknetzwerks (WLAN) sowie der Verbindung dieses WLANs mit einem kabelgebundenen Ethernet-Netzwerk (Bridging).
Accounting	Beim Accounting werden Verbindungsdaten aufgezeichnet, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.
Activity Monitor	Mithilfe des Activity Monitors kann der Status physikalischer und virtueller Geräteschnittstellen überwacht werden.
Ad-Hoc-Netzwerk	In einem Ad-Hoc-Netzwerk verbinden sich einzelne Clients über einen Wireless Adapter zu einem unabhängiges Wireless LAN. Ad-Hoc-Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer-Basis. Der Ad-Hoc-Modus wird auch als IBSS-Modus (Independent Basic Service Set) bezeichnet und ist in kleinsten Netzen sinnvoll, z. B. bei der Vernetzung zweier Notebooks ohne Access Point.
ADSL	Asymmetric Digital Subscriber Line. Siehe DSL.

AES	Advanced Encryption Standard (AES, Rijndael) ist ein Verschlüsselungsverfahren (siehe Cipher). AES verwendet eine feste Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit. AES ist ein sehr schneller und sicherer Algorithmus.
Aggressive Mode	Beim Aufbau einer IPSec-Verbindung wird der Aggressive Mode zur Realisierung eines Phase-1-Austausches verwendet. Der Aggressive Mode bietet keinen Schutz der Identität für aushandelnde Knoten, da sie ihre Identitäten übertragen müssen, bevor sie einen sicheren Kanal aufbauen können. Siehe auch Main Mode.
AH	Der Authentication Header (AH) wird bei IPSec verwendet, um die Authentizität und Integrität der übertragenen Pakete sicherzustellen sowie den Sender zu authentisieren.
Anlagenanschluss	Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...) Siehe auch Mehrgeräteanschluss.
Anlagenanschluss-Rufnummer	Siehe Anlagenanschluss.
Annex A	Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.
Annex B	Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.
Annex J	Annex J ist eine DSL-Variante zur reinen Datenübertragung, ohne Sprachinformationen (entbundelter Anschluss). Annex J ist eine Ergänzung zur Spezifikation G.992. Diese DSL-Anschlüsse benötigen keinen Splitter und haben eine höhere Reichweite und eine schnellere Übertragungsgeschwindigkeit.
Annex L	Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrate vergrößert.
Annex M	Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.

ANSI T1.413	ANSI T1.413 ist eine ADSL-Variante.
ARP	Das Address Resolution Protocol (ARP) liefert zu IPv4-Adressen die zugehörigen MAC-Adressen. Die notwendigen Informationen werden zwischen den Netzwerkknoten ausgetauscht, im Cache des Geräts gespeichert und nach Ablauf der ARP Lifetime wieder gelöscht. Für IPv6 wird diese Funktionalität durch das Neighbor Discovery Protocol (NDP) bereitgestellt.
ATM	Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge kodiert und über asynchrones Zeitmultiplexing übertragen wird.
Authentifikation	Überprüfung der Identität des Nutzers (Authentisierung).
Autorisierung	Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
AUX	AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.
B-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.
Backbone Area	Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.
Basisanschluss	Der Basisanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Basic Rate Interface (BRI). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle) mit je 64 kbit/s und einen Steuerkanal (D-Kanal) mit 16 kbit/s. Für den Basisanschluss existieren zwei Betriebsarten: Anlagenanschluss und Mehrgeräteanschluss. Für größere Installationen wird der Primärmultiplexanschluss verwendet.
Beacon	Zum Aufbau eines Wireless LAN im Infrastruktur-Modus versendet der zentrale Access Point Beacons. Diese Mitteilungen enthalten den Netzwerknamen (SSID), eine Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung.
Bit	Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.
Black / White List	Einträge in der Black List werden blockiert, Einträge in der White List werden durchgelassen. (Beispiel: Alle Telefonnummern, die mit 01234 beginnen, werden in der Black List blockiert. Die Telefonnum-

mer 01234987 kann trotzdem in der White List freigegeben werden.)

Blowfish	Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.
BootP	Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Siehe Basisanschluss.
Bridge	Eine Bridge ist eine Netzwerkkomponente zum Verbinden gleichartiger Netze auf Schicht 2 des OSI-Modells. Datenpakete werden anhand von MAC-Adressen übertragen. Durch Bridges wird das Netzwerk aufgeteilt und entlastet.
Broadcast	Bei einem Broadcast werden Datenpakete von einem Punkt an alle Teilnehmer eines Netzes übertragen, z. B. falls der Empfänger noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP und DHCP. Die Kommunikation erfolgt über Broadcast-Adressen: MAC-Netzwerke: FF:FF:FF:FF:FF:FF, IPv4-Netzwerke: 255.255.255.255, IPv6-Netzwerke: ff00::/8
BRRP	BRRP ist eine Implementierung des Virtual Router Redundancy Protocol (VRRP). Ziel des Verfahrens ist es den Ausfall des Standardgateways zu kompensieren. Mehrere Router werden zu einem virtuellen Router zusammengefasst. Fällt einer dieser Router aus, können die Restlichen diesen ersetzen.
CA	Certificate Authority. Siehe Zertifikat.
Cache	Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.
Called Party's Number	Rufnummer des angerufenen Teilnehmers.
Calling Party's Number	Rufnummer des Anrufers.
CAPI	Das Common ISDN Application Programming Interface (CAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch TAPI.

CAPWAP	Das Control And Provisioning of Wireless Access Points Protocol (CAPWAP) dient zur Überwachung von Wireless Access Points (Slaves) durch einen WLAN-Controller (Master). Es verwendet die UDP-Ports 5246 zur Kontrolle und 5247 zur Datenübertragung.
CAST	CAST ist ein Verschlüsselungsverfahren (siehe Cipher). CAST verwendet eine fixe Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 40 und 128 Bit gewählt werden. Alternative Bezeichnungen sind CAST-128 oder CAST5.
CHAP	Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentifizierungsprotokoll für PPP-Verbindungen. Neben dem Standard-CHAP existieren noch die Varianten MS-CHAPv1 und MS-CHAPv2 der Firma Microsoft. Man wählt sich über PPP in ein Netzwerk ein und authentifiziert sich mit Benutzername und Passwort. Benutzername und Passwort werden verschlüsselt übertragen. Siehe auch PAP.
Cipher	Eine Blockchiffre (Block Cipher) ist ein Verschlüsselungsalgorithmus. In diesem Verschlüsselungsverfahren wird ein Datenblock mit fester Größe (normalerweise 64 Bit) mithilfe eines sogenannten Schlüssels zu einem Block derselben Größe umgeschrieben. Je länger der Schlüssel ist, umso sicherer ist der Algorithmus.
Client	Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.
CoS	Der Begriff Class of Service (CoS) hat je nach Anwendungsgebiet verschiedene Bedeutungen. In der Telekommunikation wird unter CoS die dem Benutzer zugewiesene Berechtigungsklasse verstanden. Die Berechtigungsklasse legt die Rechte des Benutzers fest, wie z. B. Amtsberechtigung, nutzbare Leistungsmerkmale, Zugriff auf Anwendungen, ... In der Netzwerktechnologie versteht man unter CoS die Klassifizierung bestimmter Dienste gemäß IEEE 802.1p. CoS ermöglicht eine gezielte Priorisierung, während mit Quality of Service (QoS) explizite Bandbreitengarantien oder -beschränkungen eingerichtet werden. Die Einteilung der Datenpakete erfolgt mittels eines DSCP-Werts (Differentiated Services Code Point).
CRC	Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.
CRL	Siehe Zertifikat.
D-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.

Daemon	Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.
Datagramm	Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.
Datenkompression	Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.
Dead Peer Detection	In IPsec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.
Default Gateway	An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.
Default Route	Siehe Standardroute.
Diffie-Hellman	Diffie-Hellman ist ein Public-Key-Algorithmus zur Aushandlung und Etablierung von Schlüsseln. Da Daten weder verschlüsselt noch signiert werden, ist das Verfahren nur sicher, falls sich die Verbindungspartner über andere Mechanismen, wie RSA oder DSA, authentifizieren.
Denial-Of-Service Attack	Bei einem Denial-of-Service-Angriff (DoS) wird eine Netzwerkkomponente mit Anfragen überflutet, sodass diese völlig überlastet wird. Das System oder ein bestimmter Dienst ist in Folge dessen nicht mehr funktionsfähig.
DES	Data Encryption Standard (DES) ist ein Verschlüsselungsverfahren (siehe Cipher). DES verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge beträgt 56 Bit. Triple-DES oder 3DES basiert auf der dreimaligen Anwendung von DES (drei verschiedene unabhängige Schlüssel).
DFÜ	DFÜ steht für Datenfernübertragung.
DHCP	Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die dynamische Zuweisung von IP-Adressen. Ein DHCP-Server vergibt an jeden Client im Netzwerk eine IP-Adresse aus einem definierten Adress-Pool. Die Clients müssen dazu entsprechend konfiguriert sein.
DIME	Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.
DNS	Mithilfe des Domain Name System (DNS) wird der Domänenname

(z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).

Domäne	Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).
Downstream	Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.
DSA	Mithilfe des Digital Signature Algorithm (DSA) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über Signaturen können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. DSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch RSA. DSA ist schneller in der Schlüsselerzeugung aber langsamer in der Schlüsselverarbeitung als RSA.
DSCP	Datenpakete können mit einem Differentiated Services Codepoint (DSCP) ausgezeichnet werden. DSCP-Werte teilen Datenpakete in Klassen ein, sodass wichtige Pakete schneller durch das Netzwerk geleitet werden können. Siehe auch QoS.
DSL-Modem	Siehe Modem.
DSS1	Digital Subscriber Signalling System No. 1 (DSS1) ist ein Signalisierungsprotokoll für den D-Kanal des ISDN. Es ist auch bekannt als Euro-ISDN.
DTIM	Eine Delivery Traffic Indication Message informiert die Clients über auf dem Access Point vorhandene Multicast- bzw. Broadcast-Daten.
Durchwahl (VoIP)	Beim Durchwahl-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer IP-TK-Anlage. Man erhält eine Basisrufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Basisrufnummer: 1234, Rufnummernblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...)
Durchwahlausnahme	Siehe Anlagenanschluss und Durchwahl (VoIP).
Durchwahlbereich	Siehe Rufnummernblock bei Anlagenanschluss und Durchwahl (VoIP).
Durchwahlnummer	Siehe Anlagenanschluss und Durchwahl (VoIP).

Dynamische IP-Adresse	Im Gegensatz zu einer statischen IP-Adresse wird die dynamische IP-Adresse temporär per DHCP zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
DynDNS	Mithilfe eines DynDNS-Providers kann ein Domänenname auch mit einer dynamisch wechselnden IP-Adresse verknüpft werden.
Einzelrufnummer (VoIP)	Beim Einzelrufnummer-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von VoIP-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Durchwahl (VoIP).
Encapsulation	Encapsulation (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.
Encryption	Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.
ESP	Encapsulating Security Payload (ESP) ist ein Protokoll für IPSec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.
Ethernet	Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.
Euro-ISDN	In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.
Eurofile-Transfer	EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.
Filter	Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Treffen diese Kriterien für ein Datenpaket zu, kann das Datenpaket einer bestimmten Aktion (weiterleiten, ablehnen, ...) unterworfen werden. Dadurch entsteht eine Filterregel.
Filterregel	Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.
Firmware	Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts

bereitgestellt.

Fragmentierung	Falls die Gesamtlänge des Datenpakets größer als die Maximum Transmission Unit (MTU) der Netzwerkschnittstelle ist, muss das Datenpaket durch IP-Fragmentierung auf mehrere physikalische Datenblöcke aufgeteilt werden. Der umgekehrte Prozess wird Reassembly genannt.
Frame	Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells
Frame Relay	Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.
FTP	Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.
Full-Duplex	Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.
G.991.1	Datenübertragungsempfehlung für HDSL.
G.991.2	Datenübertragungsempfehlung für SHDSL.
G.992.1	Datenübertragungsempfehlung für ADSL (G.DMT). Es existieren zwei länderspezifische Ausprägungen G.992.1 Annex A und G.992.1 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.2	Datenübertragungsempfehlung für ADSL (G.LITE / ADSL-Lite). Es existieren zwei Varianten G.992.2 Annex A und G.992.2 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.3	Datenübertragungsempfehlung für xDSL2. Es existieren drei Varianten: G.992.3 Annex A/B (G.DMT bis ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.3 Annex L (RE-ADSL2) mit Datenübertragungsraten von 5 Mbit/s im Downstream und 0,8 Mbit/s im Upstream und G.992.3 Annex M (ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 2,5 Mbit/s im Upstream.
G.992.4	Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)
G.992.5	Datenübertragungsempfehlung für xDSL2+. Es existieren drei Vari-

anten: G.992.5 Annex A/B (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.5 Annex L (RE-ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream und G.992.5 Annex M (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 3,5 Mbit/s im Upstream.

G.993.1	Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)
G.993.2	Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)
G.DMT	Siehe F.992.1.
G.Lite	Siehe F.992.2.
G.SHDSL	Siehe G.991.2.
Gateway	Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.
GPRS	General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.
GRE	Generic Routing Encapsulation (GRE) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. GRE verwendet die Protokollnummer 47.
GSM	Das Global System for Mobile Communications (GSM), auch als 2G bezeichnet, ist ein Mobilfunkstandard. Dieser erreicht zusammen mit GPRS eine spezifizierte max. Datenübertragungsrate von 171,2 kbit/s.
Half-Duplex	Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.
Hash	Zur Sicherstellung der Datenintegrität muss die Information vor unautorisierter Manipulation während der Übertragung geschützt werden. Um dies zu gewährleisten, muss jede empfangene Kommunikation mit der ursprünglich gesendeten Information übereinstimmen. Deshalb werden mathematische Streuwertfunktionen (Hashfunktionen) zur Berechnung von Prüfsummen (Hashwerten) verwendet. Diese werden verschlüsselt und mit der Nachricht als digitale Signatur versendet. Der Empfänger prüft wiederum die Signatur, bevor er das Paket öffnet. Falls sich die Signatur und damit der

Inhalt des Datenpakets geändert hat, wird das Paket verworfen. Die am häufigsten verwendeten Hash-Algorithmen sind Message Digest Version 5 (MD5) und Secure Hash Algorithm (SHA1).

HDSL	High Data Rate Digital Subscriber Line. Siehe DSL.
Heartbeat	Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.
Hop	Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.
Host	Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.
Host-Name	Domänenname eines Host. Siehe DNS.
Hostroute	Eine Hostroute bezeichnet die Route zu einem einzelnen Host.
Hotspot	Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.
HSDPA	High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.
HTTP	Das HyperText Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. Es verwendet standardmäßig den Port 80.
HTTPS	Das HyperText Transfer Protocol Secure (HTTPS) ist ein Protokoll zur abhörsicheren Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. HTTPS ist schematisch identisch zu HTTP. Für die zusätzliche Verschlüsselung der Daten wird SSL / TLS verwendet. Der Standard-Port für HTTPS-Verbindungen ist 443.
Hyperchannel	Beim Hyperchannel haben mehrere Teilnehmer Zugriff auf das Übertragungsmedium. Ein Teilnehmer kann seine Informationen nur übertragen, wenn kein anderer Teilnehmer das Medium belegt. Ein Hyperchannel-Netzwerk dient hauptsächlich für Kurzstreckenbetrieb mit höchsten Datenraten.
ICMP	Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.

IGMP	Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.
IKE	Das Internet-Key-Exchange-Protokoll (IKE) dient der automatischen Schlüsselverwaltung bei IPSec-Verbindungen. Der IKE-Prozess verläuft in zwei Phasen. Während Phase 1 authentifizieren sich die IKE-Teilnehmer gegenseitig und etablieren einen sicheren Kanal. In Phase 2 handeln die beiden IPSec-Teilnehmer die SAs aus. Es existieren zwei Versionen des IKE-Mechanismus.
Infrastruktur-Netzwerk	In einem Infrastruktur-Netz bilden die einzelnen Endgeräte (Clients) über einen zentralen Knotenpunkt (Access Point) ein Wireless LAN. Dieser zentrale Access Point kann dabei auch ein Vermittler in weitere Netze sein.
IP	Das Internet Protocol (IP) ist ein Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es arbeitet auf der Vermittlungsschicht des OSI-Modells. Auf IP bauen die Protokolle TCP und UDP auf. Es existieren zwei Versionen Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6).
IP-Adresse	IP-Adressen werden zur Navigation in einem IP-Netzwerk verwendet, um Quelle und Ziel eindeutig zu bestimmen. IPv4-Adressen bestehen aus 32 Bits, IPv6-Adressen aus 128 Bits. Damit sind bei IPv4 232, also 4.294.967.296 Adressen darstellbar, bei IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen. Für IPv4 wird die Dezimaldarstellung (dotted decimal notation) verwendet, z. B. 192.168.0.250. Für IPv6 wird die Hexadezimaldarstellung verwendet, z. B. 2001:db8:85a3::8a2e:370:7344. Siehe auch Netzmaske.
IPCP	Das Internet Protocol Control Protocol (IPCP) dient, analog zu DHCP, zur Konfiguration eines Host mit IP-Adresse, Gateway und DNS-Server, falls eine PPP-Netzwerkverbindung verwendet wird. Mithilfe der Erweiterung Robust Header Compression over PPP kann der Header für eine schnellere Datenübertragung komprimiert werden. Analog wird in IPv6-Netzwerken die Funktionalität durch das Internet-Protocol-Version-6-Control-Protokoll (IPv6CP) bereitgestellt.
IPSec	IPSec (Internet Protocol Security) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. Die Protokollnummer für IPSec ist dabei vom verwendeten Protokoll abhängig. Der Authentication-Header (AH) verwendet die Protokollnummer 51, das Encapsulating-Security-Payload (ESP) die Nummer 50.

IPv6	Siehe IP.
ISDN	Integrated Services Digital Network (ISDN) ist ein Datenübertragungsstandard, der Telefonie, Telefax und Datenübertragung umfasst. Es existieren zwei ISDN-Anschluss-Varianten: Basisanschluss und Primärmultiplexanschluss.
ISDN-Adresse	Die ISDN-Adresse eines ISDN-Geräts setzt sich zusammen aus einer ISDN-Nummer gefolgt von weiteren Ziffern, die sich auf das spezifische Endgerät beziehen.
ISDN-Login	Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.
ISDN-Nummer	Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.
ISDN-Router	Siehe Router.
ISP	Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.
ITU	Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.
Kanal	Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.
Kanalbündelung	Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.
Keepalive	Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.
Keepalive	Keepalive ist ein Mechanismus zur Aufrechterhaltung der Netzwerkverbindung und zur Überprüfung der Erreichbarkeit der Kommunikationspartner. Dazu werden in der Regel spezifische Pakete ins Netzwerk gesendet.
Konfiguration	Alle Einstellungen des Geräts werden als Konfiguration bezeichnet. Diese Konfiguration ist intern in MIB-Tabellen gespeichert. Diese Informationen können extern gespeichert, von extern geladen oder gelöscht werden. Bearbeitet wird die Konfiguration über die HTTP(S)-Benutzeroberfläche, einen SNMP-Client oder angeschlossene Telefone.

L2TP	Das Layer 2 Tunneling Protocol (L2TP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über verschiedene Protokolle zu transportieren. L2TP verwendet standardmäßig die Protokollnummer 1701. Die Architektur eines L2TP-Netzwerks besteht aus einem L2TP-Access-Concentrator (LAC), der auch fest in den Client integriert sein kann, und dem L2TP-Network-Server (LNS). Der LAC stellt die Verbindungen zum LNS her und verwaltet diese. Die Autorisierung wird über einen Network-Access-Server (NAS), der im LAC oder LNS implementiert sein kann, geregelt. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Die eigentlichen Nutzdaten werden unverschlüsselt ausgetauscht, während Kontrollnachrichten zur Aufrechterhaltung der Erreichbarkeit der Tunnelendpunkte abgesichert übertragen werden.
LAC	Siehe L2TP.
LAN	Ein Local Area Network (LAN) bezeichnet ein räumlich eng begrenztes Netzwerk und umspannt meist ein Gebäude oder einen Firmensitz.
Lastverteilung	Bei der Lastverteilung werden Daten über unterschiedliche Schnittstellen gesendet, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. Im Unterschied zu Multilink funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.
Layer	Ein Layer bezeichnet eine Schicht im OSI-Modell.
LCP	Das Link Control Protocol (LCP) wird in PPP-Verbindungen verwendet, um die Einkapsulierung automatisch auszuhandeln, Grenzen für variierende Paketgrößen zu verarbeiten, den Verbindungspartner zu authentifizieren, einen defekten Link zu bestimmen, Verbindungsfehler zu erkennen und die Verbindung zu beenden.
LDAP	Das Lightweight Directory Access Protocol (LDAP) regelt die Kommunikation zwischen einem Client und dem Directory-Server. LDAP wird für den Austausch und die Aktualisierung von Verzeichnissen, z. B. ein Telefonbuch, verwendet.
Lease Time	Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.
Leased Line	Siehe Standleitung.
LLC	Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.

LNS	Siehe L2TP.
Loopback	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
LTE	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
MAC-Adresse	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
Main Mode	Beim Aufbau einer IPSec-Verbindung wird der Main Mode zur Realisierung eines Phase-1-Austausches verwendet, indem ein sicherer Kanal eingerichtet wird. Siehe auch Aggressive Mode.
Man-in-the-Middle Attack	Im Man-in-the-middle-Angriff befindet sich der Angreifer physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kann somit den Datenverkehr einsehen und sogar manipulieren.
MD5	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Media Gateway	Ein Media Gateway wandelt den Netzwerktyp von digitalen Sprach-, Audio- oder Bildinformationen um. Beispielsweise können die Signale eines ISDN-Netzwerks auf ein IP-Netzwerk umgesetzt werden.
Mehrfachrufnummer (MSN)	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
Mehrgeräteanschluss	Beim Mehrgeräteanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von ISDN-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Anlagenanschluss.
Metrik	Die Metrik ist eine Maß für die Güte der Route. Die schnellste Route weist dabei die geringste Metrik (costs, »Kosten«) auf. Vereinfacht ist dies die Verbindung mit der kleinsten Anzahl an Knotenpunkten (Routern).
MIB	Die Management Information Base (MIB) beschreibt die Informationen, die über ein Netzwerk-Management-Protokoll (z. B. SNMP) abgefragt oder modifiziert werden können. Die MIB ist eine Datenbank, die alle Geräte und Funktionen im Netzwerk beschreibt.

MLP	Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.
Modem	Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.
MPDU	Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.
MPPC	Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.
MPPE	Microsoft Point-To-Point Encryption (MPPE) wird zur Verschlüsselung von Daten, die über PPP übertragen werden, eingesetzt. Es wurde von Microsoft und Cisco entwickelt und als RFC 3078 spezifiziert.
MS-CHAP	Das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) ist ein Authentisierungsverfahren. MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für PPTP-Verbindungen (VPN).
MSDU	Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.
MSN	Siehe Mehrfachrufnummer.
MSS	Die Maximum Segment Size (MSS) definiert die maximale Anzahl an Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Die MSS muss kleiner als die Maximum Transmission Unit (MTU) sein, um eine Fragmentierung der IP-Pakete zu vermeiden.
MSS Clamping	Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.
MTU	Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.
Multicast	Bei einem Multicast werden Datenpakete von einem Punkt an bestimmte Teilnehmer eines Netzes übertragen. In IPv4 wird dies über den Adress-Bereich 224.0.0.0 bis 239.255.255.255 und das Protokoll IGMP gesteuert, in IPv6 über ff00::8-Adressen und ICMPv6.

Multilink	Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, ...) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.
NAPT	Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.
NAT	Mithilfe von Network Address Translation (NAT) werden die Quell- und Ziel-IP-Adressen eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch PAT.
NBNS	NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.
Netzabschluss	Der Netzabschluss (Network Termination, NT) bezeichnet einen Anschluss bzw. eine Betriebsart. Am NT-Anschluss (Anschlussdose) wird einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt. Beim analogen Anschluss wird die Steckdose TAE genannt, beim ISDN-Basisanschluss NTBA und beim ISDN-Primärmultiplexanschluss NTPMGF. Im NT-Betrieb wird das Gateway am externen S0 der Telefonanlage angeschlossen und stellt für diese einen externen Amtsanschluss dar. Siehe auch TE.
Netzmaske	Die Netzmaske, auch Netzwerkmaske oder Subnetzmaske, definiert bei IPv4 in Verbindung mit der IP-Adresse das Netzwerk, indem sie die IP-Adresse in einen Netzwerk- und einen Geräteanteil aufteilt und somit bestimmt, welche Adressen geroutet werden müssen. Beispiel einer Netzmaske: 255.255.255.0. Bei IPv6 spricht man von der Präfixlänge.
Netzwerkadresse	Eine Netzadresse (Präfix) bezeichnet die Adresse des gesamten Netzwerks. Die Netzwerkmaske bzw. Präfixlänge unterteilt die IP-Adresse in die Netzadresse und Host-Adresse (Geräteadresse). Beispiel für eine Netzadresse: 192.168.0.250/24
Netzwerkroute	Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.
NT	Siehe Netzabschluss.
NTP	Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.
OAM	OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.
OSI-Modell	Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen

physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.

OSPF	OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.
PAP	Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.
PAT	Mithilfe von Port and Address Translation (PAT) werden die Quell- und Ziel-IP-Adressen sowie die Quell- und Ziel-Ports eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch NAT.
Peer	Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.
Phase-1/2	Siehe IKE.
PIM	Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.
Ping	Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist. Daneben wird die Zeitspanne zwischen dem Aussenden eines Datenpakets (ICMP(v6)-Echo-Request-Paket) und dem Empfangen eines daraufhin unmittelbar zurückgeschickten Antwortpakets gemessen. Dadurch kann die Qualität der Verbindung ermittelt werden.
PKCS	Die Public-Key Cryptography Standards (PKCS) beinhalten Standards für Public-Key-Kryptografie. Die PKCS sind konzipiert für binäre und ASCII-Daten und sind kompatibel mit dem X.509-Standard. Die veröffentlichten Standards sind PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, und #15. PKCS #10 beschreibt die Syntax für Zertifizierungsanfragen.
PKI	Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.
PMTU	Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.
Point-to-Multipoint	Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).

Point-to-Point	Siehe Anlagenanschluss und Durchwahl (VoIP).
Pool	Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.
POP3	Das Post Office Protocol Version 3 (POP3) ist ein Übertragungsprotokoll, um den E-Mail-Abruf von einem E-Mail-Server durch einen Client zu steuern.
Port	Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, ...) ein ankommendes Datenpaket weitergeleitet wird.
PPP	Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.
PPPoA	Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.
PPPoE	Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.
PPTP	Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. PPTP verwendet die Protokollnummer 1723. Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP-Access-Concentrator (PAC) und den PPTP-Network-Server (PNS). Der PAC ist üblicherweise in den Windows Client integriert. Er stellt die Verbindung zum PNS her und verwaltet diese. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.
Präfix	Siehe Netzwerkadresse.
Präfixdelegation	In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.
Präfixlänge	Siehe Netzmaske.
Preshared Key	Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.
PRI	Siehe Primärmultiplexanschluss.

Primärmultiplexanschluss	Der Primärmultiplexanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Primary Rate Interface (PRI) oder S2M-Anschluss. Ein Primärmultiplexanschluss bietet in Europa 30 und in den USA 23 Nutzkanäle (B-Kanäle) mit je 64 kbit/s, einen Steuerkanal (D-Kanal) mit 64 kbit/s und einen Synchronisationskanal mit 64 kbit/s in Europa und 8 kbit/s in den USA. Siehe auch Basisanschluss.
Proposal	Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.
Protokoll	Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP
Proxy	Ein Proxy ist eine Netzwerkkomponente. Der Proxy ist ein Vermittler. Er leitet eine Anfrage der Quelle mit seiner eigenen IP-Adresse an das Ziel weiter.
PVID	Der Port VLAN Identifier (PVID) ist die Standard-VLAN-ID des jeweiligen Ports. Ein Paket, das ohne VLAN-Tag diesen Port erreicht, wird mit dieser ID versehen.
Q-SIG	Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.
QoS	Quality of Service (QoS) beschreibt die Qualität (Güte) des Kommunikationsdienstes. Diese wird anhand von Bandbreite, Verzögerung, Paketverlusten und Jitter definiert. Um zeitkritische Datenpakete für VoIP oder Videostreaming möglichst schnell zu übertragen, werden alle Datenpakete bei QoS in Gruppen sortiert und entsprechend ihrer Priorität im Netzwerk schneller oder langsamer weitergeleitet.
Queue	In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen. Der RADIUS-Server authentifiziert den Client z. B. mittels der Überprüfung von Benutzername und Kennwort. Siehe auch TACACS+.
RE-ADSL2	Siehe G.992.5.

Real Time Jitter Control	Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.
Regelkette	In einer Regelkette sind unterschiedliche Filterregeln zusammengefasst. Eine Filterregel wählt einen Teil des Datenverkehrs aufgrund bestimmter Merkmale, z. B. der Quell-IP-Adresse, aus und wendet auf diese Teilmenge eine Aktion an, z. B. blockieren.
Registrar	Der SIP-Server (Registrar) muss eingesetzt werden, falls die Teilnehmer eines VoIP-Gesprächs keine statischen IP-Adressen verwenden. Der SIP-Server registriert die IP-Adressen der Clients und sendet diese Informationen an den SIP-Proxy, der die Anrufe vermittelt. Meistens sind SIP-Proxy und SIP-Registrar identisch.
Repeater	Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.
Reset	Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.
RFC	Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.
Rijndael	Siehe AES.
RIP	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
RJ45	RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.
Roaming	Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.
Router	Ein Router ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze auf der Vermittlungsschicht des OSI-Modells. Datenpakete werden anhand von IP-Adressen übertragen. Über Routing-Tabellen werden die besten Wege (Routen) durch das Netzwerk festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle, z. B. OSPF oder RIP, aus.

Router Advertisement	Router Advertisements sind Nachrichten, die der Router ins Netzwerk sendet. Diese verkünden die Anwesenheit des Routers im Netz. Ferner werden mithilfe von Router Advertisements Präfixe verteilt, die Autokonfiguration organisiert und der Standardrouter festgelegt.
Routing	Routing bezeichnet das Festlegen von Wegen für die Nachrichtenübermittlung.
RSA	Mithilfe des RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über die Signatur können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. RSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch DSA. RSA ist langsamer in der Schlüsselerzeugung aber schneller in der Schlüsselverarbeitung als DSA.
RTP	Mit dem Real-Time Transport Protocol (RTP) werden Audio- und Video-Daten (Streams) über IP-basierte Netzwerke übertragen.
RTS Threshold	Sobald die Anzahl der Frames im Datenpaket über der RTS-Schwelle (RTS Threshold) liegt, wird vor dem Senden eines Datenpakets eine Verbindungsüberprüfung (RTS/CTS-Handshake) durchgeführt.
RTSP	Das Real-Time Streaming Protocol (RTSP) steuert die Übertragung von Audio- und Videodaten (Streams) über IP-basierte Netzwerke. Während das Real-Time Transport Protocol (RTP) zur Übertragung der Nutzdaten dient, besteht die Funktion von RTSP hauptsächlich in der Steuerung der Datenströme.
S2M-Anschluss	Siehe Primärmultiplexanschluss.
SA	Eine sogenannte Sicherheitsverbindungen (Security Associations, SA) enthält Informationen über die Maßnahmen zur Sicherung der Kommunikationsverbindung. Mindestens eine SA ist die Voraussetzung für den Aufbau einer gesicherten Verbindung. Eine SA enthält die IP-Adresse des Teilnehmers, das verwendete Authentifizierungsprotokoll, den verwendeten Verschlüsselungsalgorithmus, den Sicherheits-Parameter-Index (SPI), den Selektor und die Gültigkeitsdauer.
SAD	Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die SAD enthält Informationen über

jede Sicherheitsverbindung. Also welche Verschlüsselungsalgorithmen, Schlüssel, Protokolle, Sitzungsnummern oder Gültigkeitszeiträumen verwendet werden sollen. Für eine ausgehende Verbindung zeigt ein Eintrag der SPD auf einen Eintrag der SAD. Dadurch kann die SPD festlegen, welcher SA für ein bestimmtes Paket verwendet wird. Bei einer eingehenden Verbindung wird die SAD angesprochen, um festzulegen, wie das Paket verarbeitet wird.

SCEP	Das Simple Certificate Enrollment Protocol (SCEP) dient zur Verwaltung digitaler Zertifikate.
Scheduling	Unter Scheduling versteht man einen Aufgabenplan. Bestimmte Aktionen (z. B. Deaktivierung einer Schnittstelle) werden durch Ereignisse (z. B. Zeit oder Änderung einer MIB-Variablen) ausgelöst.
Serielle Schnittstelle	Die serielle Schnittstelle dient dem Datenaustausch zwischen Computern und Peripheriegeräten. Sie kann zur Konfiguration des Geräts oder zur Datenübertragung über eine IP-Infrastruktur verwendet werden (Serial over IP).
Server	Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden.
SFP	Small Form-factor Pluggable (SFP) ist eine Steckverbindung, die für extrem schnelles Ethernet entwickelt wurde.
SHA1	Secure-Hash-Algorithm Version 1 (SHA1) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
SHDSL	Symmetrical High-bit-rate Digital Subscriber Line. Siehe DSL.
Shell	Die Shell ist eine Eingabeschnittstelle (z. B. Kommandozeile oder grafische Benutzerschnittstelle) zwischen Computer und Benutzer.
Shorthold	Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.
SIF	Bei einer Stateful Inspection Firewall (SIF) wird die Weiterleitung eines Datenpakets nicht nur durch Quell- und Zieladressen oder Port bestimmt, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung.
SIP	Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das Protokoll wird für IP-Telefonie (VoIP) verwendet.

SIP-Provider	Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.
SNMP	Mithilfe des Simple Network Management Protocol (SNMP) werden verschiedene Netzwerkkomponenten (z. B. Router, Server, usw.) von einem zentralen System aus konfiguriert, kontrolliert und überwacht. Die änderbaren Einstellungen der Netzwerkkomponenten sind dabei in einer Datenbank gespeichert – der Management Information Base (MIB). SNMP verwendet UDP. Die Netzwerkkomponente empfängt dabei Anfragen (Requests) auf Port 161, während das verwaltende System Bestätigungsmeldungen (TRAPs) auf Port 162 entgegennimmt.
Spatial Streams	Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der Übertragungsrates.
SPD	Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die Security-Policy-Datenbank führt die Formen des Datenverkehrs auf, die gesichert werden sollen. Dazu werden Faktoren wie Quell- und Zieladresse des Datenpakets verwendet.
SRTP	Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die mithilfe von AES verschlüsselte Variante des Real-Time Transport Protocol (RTP).
SSH	Secure Shell (SSH) ist ein Netzwerkprotokoll mit dem man eine verschlüsselte Verbindung zur Shell eines Geräts herstellen kann.
SSID	Der Service Set Identifier (SSID) definiert ein Funknetzwerk, das auf IEEE 802.11 basiert. Der SSID ist der Netzwerkname des Wireless LAN. Alle Access Points und Clients, die zum gleichen Netzwerk gehören, verwenden denselben SSID. Die SSID-Zeichenfolge kann bis zu 32 Zeichen lang sein und wird allen Paketen unverschlüsselt vorangestellt. Mithilfe der SSID ANY kontaktiert ein Client alle erreichbaren Access Points. Dem Anwender werden daraufhin alle verfügbaren WLANs angezeigt und er kann das passende Netz auswählen. Wenn ein Access Point für verschiedene Netze verwendet wird, erhält jedes Funknetzwerk eine eigene MSSID (Multi Service Set Identifier).
SSL	Secure Sockets Layer (SSL) ist ein Protokoll zur Datenverschlüsselung. Seit Version 3.1 wird die neue Bezeichnung Transport Layer

Security (TLS) verwendet. SSL wird hauptsächlich für HTTPS verwendet, um die Datenübertragung zwischen Web-Server und Web-Browser zu verschlüsseln.

STAC	Mithilfe von STAC wird die übertragene Datenmenge verringert (Datenkompression).
Standardroute	Die Standardroute (Default Route) wird verwendet, falls keine andere passende Route vorhanden ist.
Standardrouter	Siehe Default Gateway.
Standleitung	Eine Standleitung (Leased Line) ist eine permanente Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz.
Statische IP-Adresse	Im Gegensatz zu einer dynamischen IP-Adresse wird die statische IP-Adresse fest vom Anwender zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
STUN-Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Ein STUN-Server ermöglicht VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Netzwerk.
Subadressierung	Neben der ISDN-Telefonnummer kann eine Subadresse beim Verbindungsaufbau übertragen werden. Diese Subadresse überträgt eine beliebige Zusatzinformation. Diese kann genutzt werden, um z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt anzusprechen oder bestimmte Programme auf einem PC aufzurufen.
Subnetz	Ein Teilnetz eines IP-Netzes wird als Subnetz bezeichnet. Ein Teilnetz wird wie ein normales Netzwerk über IP-Adresse und (Sub-)Netzmaske (IPv4) bzw. Präfixlänge (IPv6) definiert. Beispiel: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 mögliche IP-Adressen) ist ein Subnetz von 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 mögliche IP-Adressen).
Switch	Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerkkomponenten miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells betrieben werden. Das dem

	Switch vergleichbare Gerät der Bitübertragungsschicht wird als Hub bezeichnet.
SWYX	SwyxWare ist eine softwarebasierte Kommunikationslösung für VoIP.
Syslog	Das Syslog-Protokoll wird zur Übermittlung von Status-Meldungen in einem IP-Netzwerk verwendet. Verschiedene Netzwerkkomponenten können somit von einem zentralen System aus überwacht werden. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP-Port 514 gesendet.
T.38	T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.
TACACS+	Das Terminal Access Controller Access Control System Plus (TACACS+) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern. Der TACACS+-Server authentifiziert den Client mittels der Überprüfung von z. B. Benutzername und Kennwort. Im Gegensatz zum UDP-basierten RADIUS-Protokoll verwendet TACACS+ TCP auf Port 49 und überträgt die gesamte Kommunikation verschlüsselt.
TAPI	Telephony Applications Programming Interface (TAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch CAPI.
TCP	Beim Transmission Control Protocol (TCP) handelt es sich um ein verbindungsorientiertes Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungsorientierten Protokoll wird vor der Übertragung eine logische Verbindung aufgebaut und aufrechterhalten. Dies ermöglicht eine zuverlässige Übertragung der Daten. Allerdings werden ständig Kontrollinformationen neben dem eigentlichen Datenpaketen übertragen. Dies führt zu einem Anstieg des übertragenen Datenvolumens. Siehe auch UDP.
TCP-ACK-Paket	Ein ACK-Signal (Acknowledgement = Bestätigung) wird bei einer Datenübertragung verwendet, um den Erhalt oder die Verarbeitung von Daten oder Befehlen zu bestätigen. TCP verwendet ACK-Signale zur Kommunikation.
TE	Der Endgeräteanschluss (Terminal Equipment, TE) bezeichnet einen Anschluss bzw. eine Betriebsart. Der TE-Anschluss ist der Anschluss eines Endgeräts. Im TE-Betrieb wird das Gateway am internen S0 der Telefonanlage angeschlossen und stellt damit ein

ISDN-Endgerät dar. Siehe auch NT.

Telnet	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
TFTP	Das Trivial File Transfer Protocol (TFTP) regelt die Übertragung von Dateien. Im Vergleich zu FTP fehlen eine Möglichkeit zur Dateianzeige, eine Rechtevergabe und eine Benutzerauthentifizierung.
Tiger 192	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
TLS	Siehe SSL.
TOS	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
Traceroute	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpakete bis zum abgefragten Ziel-Host vermittelt werden.
Trigger	Unter Trigger versteht man einen Auslöseimpuls.
Triple DES	Siehe DES.
TTL	Die Time to live (TTL) ist die konfigurierte Gültigkeitsdauer eines Datenpakets. Beim Internet Protocol (IP) legt die TTL fest, wie viele Hops ein Datenpaket passieren darf. Der Maximalwert beträgt 255 Hops. Mit jedem Hop wird die TTL um 1 reduziert. Falls ein Datenpaket nach Ablauf seiner TTL noch nicht sein Ziel erreicht hat, wird es verworfen.
Twofish	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) ist eine DSL-Variante. Sie wurde als ANSI T1.413 entwickelt und als G.992.2 standardisiert. U-ADSL erlaubt die parallele Nutzung verschiedener Kommunikationstechniken, z. B. ISDN und POTS, und benötigt keinen Splitter.
Überprüfung der Rückroute	Falls bei einer Schnittstelle "Überprüfung der Rückroute" (Back Route Verify) aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden.

UDP	Beim User Datagram Protocol (UDP) handelt es sich um ein verbindungsloses Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungslosen Protokoll ist keine Kontrolle für die Auslieferung des Pakets integriert. Die Kontrolle muss in der Anwendungsschicht erfolgen. Im Gegenzug ist UDP schneller als verbindungsorientierte Protokolle.
ULA	Unique Local Addresses (ULA) sind IPv6-Adressen, die nicht geroutet werden. Sie können in privaten Netzen (z. B. einem LAN) verwendet werden. ULAs beginnen mit dem Präfix fd.
UMTS	Das Universal Mobile Telecommunications System (UMTS), auch als 3G bezeichnet, ist ein Mobilfunkstandard mit einer spezifizierten max. Datenübertragungsrate von 384 kbit/s bzw. 21 Mbit/s in Verbindung mit HSPA+.
Unicast	Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertragen.
UPnP	Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.
Upstream	Das Gateway leitet die Daten des eigenen Netzwerks weiter.
URL	Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: http://www.example.org/index.htm (Web-Seite im Internet)
V.110	V.110 beschreibt ein Verfahren zur Anpassung von Bitströmen mit 0,6, 1,2, 2,4, 2,8, 7,2, 9,6, 12, 14,4, 19,2 und 38,4 kbit/s in den ISDN-Bitstrom von 64 kbit/s.
VDSL	Very High Speed Digital Subscriber Line. Siehe DSL.
VID	Siehe VLAN.
VLAN	Ein Netzwerk kann in eines oder mehrere logische Teilnetze – sogenannte Virtual-Local-Area-Networks (VLAN) – aufgespalten werden, indem die Netzwerkkomponenten das Datenpaket eines definieren Teilnetzes nicht mehr in andere Teilnetze weiterleiten. Jedem VLAN wird eine eindeutige Nummer zugeordnet. Diese Nummer wird VLAN ID (VID) genannt und den Datenpaketen im VLAN-Tag zugeordnet.
VoIP	Voice over IP (VoIP), auch IP-Telefonie genannt, bezeichnet die Übertragung von Sprache über ein IP-Netzwerk. Der Auf- und Ab-

bau der Telefonverbindung erfolgt dabei über Signalisierungsprotokolle, wie z. B. SIP.

VPN	Mithilfe eines virtuellen privaten Netzwerks (VPN) werden private Datenpakete durch ein öffentliches Netzwerk transportiert. Die Informationen werden dabei durch Einkapselung in neue Protokolle von den öffentlich zugänglichen Daten getrennt, um sie an den vorgesehenen Empfänger zu leiten. Man spricht in diesem Zusammenhang auch von einem Tunnel, der zwischen den privaten Netzen der beiden Verbindungsteilnehmer aufgebaut wird. VPN-Protokolle sind IP-Sec, PPTP, L2TP und GRE.
VSS	Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.
Wählverbindung	Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.
Walled Garden	Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.
WAN	Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausgehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.
WDS	Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.
Web-Server	Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.
WEP	Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.
WINS	Der Windows Internet Name Service (WINS) ist eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft. Wie DNS dient WINS der zentralen Namensauflösung. Siehe auch DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.
WMM	Wi-Fi Multimedia (WMM) priorisiert die Datenpakete unterschiedlicher Anwendungen und verbessert damit die Übertragung von Sprach-, Musik- und Videodaten in WLAN-Netzwerken. Dazu stellt WMM Quality-of-Service-Merkmale (QoS) für IEEE 802.11-basierte Netzwerke bereit.

WPA	Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.
WPA - Enterprise	WPA - Enterprise bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmer durch das Extensible Authentication Protocol (EAP). Nach erfolgreicher Authentisierung übermittelt der Server dem Client und dem Access Point einen gemeinsamen Schlüssel für die Datenübertragung im WLAN.
WPA - PSK	WPA - PSK bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmern über Preshared Keys. Dabei nutzen Access Point und Client die gleiche Zeichenfolge für die Schlüsselberechnung im WLAN. Diese Zeichenfolge muss von den Anwendern konfiguriert werden.
WPA 2	Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.
X.25	X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.
X.31	Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.
X.500	Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.
X.509	Der X.509-Standard beschreibt die Erstellung der Zertifikate für eine Public-Key-Infrastruktur (PKI).
X.75	X.75 ist eine standardisierte Protokollfamilie für ISDN-Netzwerke mit einer Übertragungsrate von 64 kbit/s.
XAuth	Mithilfe von XAUTH (Extended Authentication) wird IKE um weitere Authentifizierungsmechanismen ergänzt. Nach einer erfolgreichen IKE-Phase-1-Authentifizierung kann der Benutzer noch einmal separat identifiziert werden. Die Identifizierung erfolgt über Benutzername und Passwort, PAP, CHAP oder Hardware-basierte Systeme.
Zeitschlitz	Ein Zeitschlitz ist ein fest zugeordneter Zeitabschnitt innerhalb eines Übertragungsrahmens und entspricht meist einem Übertragungskanal.
Zertifikat	Ein Zertifikat identifiziert eine Person, eine Institution, ein Gerät oder eine Anwendung. Ein Public-Key-Zertifikat ist ein digitales Zertifikat und stellt eine Verbindung zwischen der Identität und einem öffentli-

chen Schlüssel her. Zertifikate mit öffentlichem Schlüssel werden von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt. Nicht mehr vertrauenswürdige Zertifikate können über Zertifikatsperrlisten (Certificate Revocation List, CRL) deaktiviert werden.

Index

- Benutzerdefinierte DHCP-Optionen 426
 - Herstellerbeschreibung 426
 - ISDN-Zeitserver 85
 - Systemadministrator-Passwort 81
 - Zeit bis zum Abschalten 80
- #
- #1 #2, #3 129
- A**
- Abfrage Intervall 266
- ACCESS_ACCEPT 103
- ACCESS_REJECT 103
- ACCESS_REQUEST 103
- ACCOUNTING_START 103
- ACCOUNTING_STOP 103
- Action 479
- Activity Monitor 513
- Admin-Status 224
- Administrativer Status 323 , 409
- Administrativer Zugriff 96
- Adressbereich 395
- Adresse des Service-Centers 157
- Adresse/Subnetz 395
- Adressen 394
- Adressliste 395
- Adressmodus 160 , 309
- Adresstyp 395
- ADSL-Leitungsprofil 147
- ADSL-Logik 496
- Ähnliches Zertifikat überschreiben 445
- Airtime Fairness 175
- Aktion 197 , 197 , 213 , 248 , 388 , 432 , 445 , 496 , 518 , 524
- Aktion wenn Lizenz nicht registriert 429
- Aktion wenn Server nicht erreichbar 429
- Aktionen 444
- Aktive IPSec-Tunnel 76
- Aktive Sitzungen (SIF, RTP, etc...) 76
- Aktiviert 383
- Aktualisierung aktivieren 418
- Aktualisierungsintervall 420 , 514
- Aktualisierungspfad 420
- Aktualisierungstimer 260
- Aktuelle Ortszeit 84
- Aktuelle Anrufe 522
- Aktuelle Geschwindigkeit / Aktueller Modus 136 , 137
- Aktueller Dateiname im Flash 496
- Aktuelles Netzwerk 149 , 157
- Alle Multicast-Gruppen 271
- Allgemein 265 , 429 , 467
- Allgemeiner Name 127
- Als DHCP-Server 408
- Als IPCP-Server 408
- Alternative Schnittstelle, um DNS-Server zu erhalten 407
- Andere Inaktivität 393
- Ankommende Rufnummer 337
- Anmeldefenster 473
- Anmeldung 535
- Anrufliste 522
- Antwort 411
- Antwortintervall (Letztes Mitglied) 266
- Anzahl Nachrichten 507
- Anzahl der Wählversuche 465
- Anzahl der Spatial Streams 171
- Anzahl erlaubter Verbindungen 330
- Anzahl Verwendeter Ports 297
- AP-MAC-Adresse 197 , 531 , 533
- APN (Access Point Name) 149
- Arbeitsspeichernutzung 76
- ARP Lifetime 252
- ARP Processing 187
- Art des Datenverkehrs 212
- Assistenten 73
- ATM 305
- ATM PVC 286
- ATM-Dienstkategorie 312

- ATM-Schnittstelle 307
- Auf Client-Anfrage antworten 466
- Auf der Black List 434
- Auf der White List 434
- Aufzurufende Seite nach Login 471
- Ausgehende ISDN-Nummer 378
- Ausgehende Rufnummer 337
- Ausgehende Schnittstelle 238
- Ausgehende Nummer 464
- Ausgewählte Ports 379
- Ausgewählte Kanäle 177
- Ausgewählter Kanal 171
- Ausgewähltes PLMN 157
- Aushandlungsmodus 519
- Auslöser 438
- Ausstehende Ende-
zu-Ende-Anforderungen 315
- Ausstehende
Segment-Anforderungen 315
- Auswahl 396
- Auszuführende Aktion 459
- Authentifizierung 278 , 283 , 288 ,
294 , 302 , 369 , 376
- Authentifizierung für PPP-Einwahl
113
- Authentifizierungsmethode 156 , 323 ,
340 , 519
- Authentifizierungstyp 105 , 110
- Authentisierung aktivieren 487
- Automatische Konfiguration beim
Start 139
- Autospeichermodus 129 , 445
- B**
- Bandbreite 171
- Bandbreite angeben 391
- Basierend auf Ethernet-Schnittstelle
160
- Beacon Period 177
- Bedingung des Schnittstellenverkehrs
439
- Bedingung für Ereignisliste 445
- Befehlsmodus 445
- Befehlstyp 445
- Benachrichtigungsdienst 506 , 507 ,
509
- Benachrichtigungseinstellungen 509
- Benachrichtigungsempfänger 506
- Benutzer 117 , 120 , 354 , 365 , 435
- Benutzer muss das Passwort ändern
120
- Benutzerdefiniert 127
- Benutzerdefinierter Kanalplan 180
- Benutzername 156 , 276 , 281 , 286 ,
291 , 300 , 366 , 373 , 418 , 436 ,
509 , 535
- Berichtsmethode 250
- Berücksichtigen 219
- Beschreibung 115 , 123 , 133 , 204 ,
212 , 224 , 228 , 231 , 238 , 244 ,
248 , 276 , 281 , 286 , 291 , 300 ,
307 , 323 , 329 , 340 , 348 , 354 ,
362 , 366 , 373 , 383 , 394 , 395 ,
396 , 397 , 400 , 409 , 427 , 439 ,
445 , 475 , 518 , 519 , 524 , 525 ,
527
- Beschreibung - Verbindungsinformation
- Link 77
- Beschreibung des Client Links 531
- Beschreibung des Client Links 197
- Betreff 507
- Betreibermodus 105
- Betriebsmodus 171
- Betriebsmodus (Aktiv) 445
- Betriebsmodus (Inaktiv) 445
- Bevorzugter Netzwerktyp 149
- Black / White List 433
- Blockieren nach Verbindungsfehler
für 278 , 283 , 288 , 294 , 302 ,
369 , 376
- Blockzeit 111 , 345
- BOSS 496
- BOSS-Version 75
- Bridges 534
- BRRP 481
- BRRP aktivieren 491
- Burst-Größe 238
- Burst-Mode 175

- Bytes 519
- C**
- CA-Name 445
- CA-Zertifikat 125
- CA-Zertifikate 345
- Cache 414
- Cache-Größe 407
- Cache-Treffer 415
- Cache-Trefferrate (%) 415
- Callback 378
- Callback-Modus 294
- CAPI-Server 435
- Cell ID 157
- Certificate Revocation List 131
- Channel Sweep 180
- Client Links 531
- Client Link 194
- Client-MAC-Adresse 530
- Client-Modus 171
- Client-Typ 311
- Code 397
- Continuity Check (CC) Ende-zu-Ende 317
- Continuity Check (CC) Segment 317
- COS-Filter (802.1p/Layer 2) 228 , 244 , 475
- CPU-Nutzung 76
- CRL verwenden 445
- CRLs 131
- CRLs senden 360
- CSV-Dateiformat 445
- CTS Frames als Antwort auf RTS empfangen 527
- D**
- Datei auswählen 496
- Dateikodierung 130 , 131
- Dateiname 445 , 496
- Dateiname auf Server 445
- Dateiname in Flash 445
- Datenrate Mbit/s 528 , 530 , 531 , 533
- Datum 517
- Datum einstellen 84
- Datum und Uhrzeit 82
- Dauer 522 , 523
- Description 479
- Details 518
- DH-Gruppe 340
- DHCP Broadcast Flag 162
- DHCP Client an Schnittstelle 252
- DHCP-Hostname 162 , 309
- DHCP-Konfiguration 423
- DHCP-MAC-Adresse 162 , 309
- DHCP-Optionen 424
- DHCP-Relay-Einstellungen 428
- DHCP-Server 421
- Diagnose 492
- Dienst 143 , 213 , 224 , 228 , 244 , 388 , 475 , 522 , 523
- Dienste 396
- Diensteliste 397
- Dienstmerkmal 143
- Dienstkategorien 311
- DNS 404
- DNS-Anfragen 415
- DNS-Aushandlung 278 , 283 , 288 , 298 , 302 , 370 , 377
- DNS-Hostname 411
- DNS-Server 304 , 356 , 381 , 408 , 412 , 422
- DNS-Test 493
- DNS-Zuweisung über DHCP 252
- Domäne 412
- Domäne am Hotspot-Server 471
- Domänenname 406
- Domänenweiterleitung 412
- Doppelte empfangene MSDUs 527
- Downstream 146
- Drahtloser Modus 175
- Drahtlosnetzwerke (VSS) 184
- Dritter Zeitserver 85
- Drop-In 251
- Drop-In-Gruppen 251
- Dropping-Algorithmus 241
- DSA-Schlüsselstatus 99
- DSCP-/TOS-Wert 204

DSCP/TOS-Filter (Layer 3) 228 , 244
 , 475
 DSL-Chipsatz 145
 DSL-Konfiguration 145
 DSL-Modem 145
 DSL-Modus 146
 DTIM Period 177
 Dynamische
 RADIUS-Authentifizierung 358
 DynDNS-Aktualisierung 417
 DynDNS-Client 417
 DynDNS-Provider 419

E

E-Mail 127
 E-Mail-Adresse 509
 EAP-Vorabauthentifizierung 188
 Eigene IP-Adresse per ISDN/GSM übertragen 337
 Eingehende ISDN-Nummer 378
 Eingehende Nummer 464
 Eingehender Diensttyp 149
 Einstellungen Funkmodul 169
 Eintrag aktiv 105 , 110
 Einträge 297
 Empfangene DNS-Pakete 415
 Empfänger 507
 Ende-zu-Ende-Sendeintervall 315
 Einkapsulierung 307
 Entfernte GRE-IP-Adresse 383
 Entfernte IP-Adresse 363
 Entfernte MAC-Adresse 194
 Entfernte PPTP-IP-Adresse 283 , 373
 Entfernte PPTP-IP-AdresseHostname 373
 Entfernte IP-Adresse 518 , 519
 Entfernte Netzwerke 518
 Entfernte Nummer 522 , 523
 Entfernte ID 519
 Entfernter Hostname 362
 Entfernter Port 519 , 525
 Entfernter Benutzer (nur Einwahl) 291
 Enthaltene Zeichenfolge 507
 Ereignis 507

Ereignisliste 439 , 445
 Ereignistyp 439
 Erfolgreich empfangene Multicast-MS-DUs 527
 Erfolgreich übertragene Multicast-MS-DUs 527
 Erfolgreich beantwortete Anfragen 415
 Erfolgreiche Versuche 459
 Ergebnis der automatischen Konfiguration 139
 Erlaubte Adressen 191
 Erreichbarkeitsprüfung 107 , 345 , 351 , 519
 Erster Zeitserver 85
 Erweiterte Route 207
 Ethernet-Ports 134
 Ethernet-Schnittstelle 486
 Ethernet-Schnittstellenauswahl 136 , 137
 Externe Berichterstellung 501
 Externer Dateiname 130 , 131

F

Facility 502
 Fallback-Nummer 149
 Faxkopfzeile 437
 Fehler 519 , 521
 Fehlerhafte Erhaltene Pakete 527
 Fehlgeschlagene Versuche 459
 Feste IP-Adresse 156
 Filter 231
 Filterliste 431
 Filterregeln 387 , 391
 Firewall 385
 Firewall Status 392
 Fragmentation Threshold 177 , 180
 Frame-Übertragungen ohne ACK 527
 Frames ohne Tag verwerfen 166
 Frequenzband 171
 Funkzellen Code 157

G

- Garbage Collection Timer 260
 - Gateway 207 , 424
 - Gateway-IP-Adresse 203
 - Gefilterte Eingangs-Schnittstelle(n) 429
 - GEO Zone Status 439
 - Gerät 157
 - Gesamt 521
 - Geschäftsbedingungen 471
 - Gewichtung 238
 - Globale Einstellungen 406
 - Globale Einstellungen 77
 - GRE 382
 - GRE-Tunnel 382
 - GRE-Window-Anpassung 380
 - GRE-Window-Größe 380
 - Größe der Zero Cookies 358
 - Größe des Protokoll-Headers unterhalb Layer 3 235
 - Gruppen 394 , 396 , 399
 - Gruppen-ID 458
 - Gruppenbeschreibung 105 , 219 , 221 , 252
- H**
- Hashing-Algorithmen 99
 - Hello-Intervall 364
 - Hersteller auswählen 426
 - High-Priority-Klasse 231
 - Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable 445
 - Hold Down Timer 261
 - Home PLMN 157
 - Host 412
 - Host für mehrere Standorte 474
 - Hostname 418
 - Hosts 458
 - Hotspot-Gateway 468 , 470 , 534
 - HTTP 96
 - HTTPS 96 , 416
 - HTTPS-Server 416
 - HTTPS-TCP-Port 416
- I**
- ICC ID 157
 - ID des virtuellen Routers 486 , 489 , 490
 - IEEE 802.11d-Konformität 171
 - IGMP 265
 - IGMP Proxy 268
 - IGMP-Status 269
 - IKE (Phase-1) 521
 - IKE (Internet Key Exchange) 323
 - IKE (Phase-1) SAs 519
 - IMEI 157
 - Immer aktiv 276 , 281 , 286 , 291 , 300 , 366 , 373
 - Indexvariablen 439 , 445
 - Informationen senden an 514
 - Initial Contact Message senden 358
 - Internes Protokoll 516
 - Internet + Einwählen 272
 - Intervall 439 , 445 , 459 , 462
 - Intra-cell Repeating 187
 - IP Address Owner 482
 - IP Pools 304 , 355 , 381
 - IP-Accounting 504
 - IP-Adressbereich 304 , 356 , 381 , 422
 - IP-Adresse 309 , 310 , 411 , 427 , 486 , 502 , 513 , 528 , 530 , 535
 - IP-Adresse / Netzmaske 160
 - IP-Adresse des virtuellen Routers 486
 - IP-Adresse zur Nachverfolgung 222
 - IP-Adresse/Netzmaske 258 , 525
 - IP-Adressenvergabe 326
 - IP-Adressmodus 277 , 282 , 287 , 293 , 301 , 367 , 375
 - IP-Komprimierung 351
 - IP-Konfiguration 159
 - IP-Pool-Konfiguration 422
 - IP-Poolname 304 , 356 , 381 , 422 , 424
 - IP-Zuordnungspool 293 , 326
 - IP-Zuordnungspool (IPCP) 367 , 375
 - IP/MAC-Bindung 427
 - IPSec 320 , 517
 - IPSec (Phase-2) 521

IPSec aktivieren 357
 IPSec (Phase-2) SAs 519
 IPSec über TCP 358
 IPSec-Debug-Level 357
 IPSec-Peers 321
 IPSec-Statistiken 520
 IPSec-Tunnel 518 , 520
 IPv4-Routing-Tabelle 207
 ISDN 290
 ISDN Verwendung Extern 76
 ISDN-Diebstahlsicherung 463
 ISDN-Diebstahlsicherungsdienst 464
 ISDN-Konfiguration 139
 ISDN-Konfigurationstyp 139
 ISDN-Login 96
 ISDN-Port 143
 ISDN-Ports 138
 ISDN/Modem 521

K

Kanal 171 , 197 , 522
 Kanalbündelung 297
 Kanäle scannen 180
 Kanalplan 177
 Kategorie 432
 Kennwort für geschütztes Zertifikat 445
 Key Hash Payloads senden 360
 Klassen-ID 231 , 238
 Klassenplan 231
 Komprimierung 100 , 376
 Konfiguration speichern 116
 Konfiguration verschlüsseln 445
 Konfiguration enthält Zertifikate/Schlüssel 445
 Konfiguration von IPv4-Routen 200
 Konfigurationsmodus 326
 Konfigurationsschnittstelle 92
 Konfigurationszugriff 114
 Konfigurierte Geschwindigkeit/konfigurierter Modus 136 , 137
 Kontakt 78
 Kontrollmodus 235 , 319
 Kosten 522 , 523

L

L2TP 361
 LAN 159
 Land 127
 Lastverteilung 218
 Lastverteilungsgruppen 218
 Layer 4-Protokoll 204
 LCP-Erreichbarkeitsprüfung 278 , 283 , 288 , 302 , 369 , 376
 LDAP-URL-Pfad 133
 Lease Time 424
 Lebensdauer 340 , 348
 LED-Modus 78
 Letzter Befehl 157
 Letzte Antwort 157
 Letzte gespeicherte Konfiguration 75
 Level 502 , 517
 Level Nr. 115
 Lizenz gültig bis 431
 Lizenzschlüssel 89 , 431
 Lizenzseriennummer 89
 Lizenzstatus 431
 Lokale GRE-IP-Adresse 383
 Lokale IP-Adresse 203 , 252 , 277 , 282 , 287 , 293 , 301 , 326 , 364 , 367 , 375 , 383
 Lokale PPTP-IP-Adresse 283
 Lokale Zertifikatsbeschreibung 130 , 131 , 445
 Lokale Adresse 525
 Lokale IP-Adresse 519
 Lokale Dienste 404
 Lokale ID 323 , 519
 Lokale WLAN-SSID 445
 Lokaler Dateiname 445
 Lokaler Hostname 362
 Lokaler ID-Typ 323 , 340
 Lokaler ID-Wert 340
 Lokaler Port 519 , 525
 Lokales Zertifikat 340
 Lokales Zertifikat 416
 Long Retry Limit 177 , 180
 Loopback Ende-zu-Ende 315

- Loopback aktiv 210
- Loopback-Segment 315
- Löschen 207
- M**
- MAC-Adresse 160 , 309 , 427 , 525 , 528 , 534
- Mail-Exchanger (MX) 419
- Manuelle IP-Adresse des WLAN-Controller 78
- Master down trials 487
- Max. Queue-Größe 241
- Max. Clients 187
- Max. eingehende Kontrollverbindungen über entfernte IP-Adresse 380
- Max. Übertragungsrate 175
- Max. Zeitraum aktiver Scan 180
- Max. Zeitraum passiver Scan 180
- Maximale Antwortzeit 266
- Maximale Anzahl der erneuten Einwählversuche 278 , 283 , 288 , 294 , 302
- Maximale Upload-Geschwindigkeit 235 , 238 , 319
- Maximale Anzahl der Accounting-Protokolleinträge 78
- Maximale Anzahl der Einträge im Verlauf 429
- Maximale Anzahl der Syslog-Protokolleinträge 78
- Maximale Gruppen 269
- Maximale Quellen 269
- Maximale Anzahl Wiederholungen 364
- Maximale Anzahl gleichzeitiger Verbindungen 98
- Maximale Anzahl der IGMP-Statusmeldungen 266
- Maximale Anzahl der IGMP-Statusmeldungen 269
- Maximale Burst-Größe (MBS) 312
- Maximale E-Mails pro Minute 509
- Maximale SMS pro Tag 510
- Maximale TTL für negative Cacheeinträge 407
- Maximale TTL für positive Cacheeinträge 407
- Maximale Upstream-Bandbreite 146
- Maximale Zeit zwischen Versuchen 364
- Maximales Nachrichtenlevel von Systemprotokolleinträgen 78
- Mbit/s 526
- Metrik 203 , 207 , 326
- Metrik-Offset für Inaktive Schnittstellen 258
- Metrik-Offset für Aktive Schnittstellen 258
- MIB-Variablen 445
- Min. Queue-Größe 241
- Min. Zeitraum aktiver Scan 180
- Min. Zeitraum passiver Scan 180
- Minimale Zeit zwischen Versuchen 364
- Mitglieder 394 , 400
- MoIKe 332
- Mobilfunk-Anbieter 149
- Mobilnetzbetreiber 154
- Modem-Status 149
- Modemmodell 157
- Modus 125 , 197 , 204 , 209 , 252 , 266 , 269 , 297 , 337 , 340 , 354
- Modus / Bridge-Gruppe 92
- Modus des D-Kanals 337
- Monitored GEO Zone 439
- Monitoring 516
- Monitoring-Modus 489
- MSDUs, die nicht übertragen werden konnten 527
- MSN 143
- MSN-Erkennung 143
- MSN-Konfiguration 142
- MTU 278 , 383 , 519
- Multicast 263
- Multicast-Gruppen-Adresse 271
- Multicast-Routing 265
- N**

- Nach Ausführung neu starten 445
 - Nachricht 517
 - Nachrichten 519
 - Nachrichtenkomprimierung 507
 - Nachrichtentyp 502
 - Name 158 , 354
 - Name der Quelldatei 496
 - Name der Zieldatei 496
 - NAT 210 , 525
 - NAT aktiv 210
 - NAT-Eintrag erstellen 277 , 282 , 287 , 293 , 301 , 367 , 375
 - NAT-Erkennung 519
 - NAT-Konfiguration 211
 - NAT-Methode 212
 - NAT-Schnittstellen 210
 - NAT-Traversal 345
 - Negativer Cache 407
 - Netzmaske 207 , 252 , 309 , 310
 - Netzwerk 200
 - Netzwerkadresse 252
 - Netzwerkconfiguration 252
 - Netzwerkname (SSID) 187 , 195 , 197
 - Netzwerkqualität 149 , 157
 - Neue Quell-IP-Adresse/Netzmaske 217
 - Neue Ziel-IP-Adresse/Netzmaske 217
 - Neuer Quell-Port 217
 - Neuer Ziel-Port 217
 - Neuer Dateiname 496
 - Neustart 499
 - Neustart des Geräts nach 445
 - Nicht entschlüsselbare MPDUs erhalten 527
 - Nicht geändert seit 524
 - Nicht-Mitglieder verwerfen 166
 - Nr. 209 , 517 , 524
 - Nutzungsart 294
 - Nutzungsbereich 171
- O**
- OAM-Fluss-Level 315
 - OAM-Regelung 314
 - Öffentliche Quell-IP-Adresse 332
 - Öffentliche Schnittstelle 332
 - Öffentlicher Schnittstellenmodus 332
 - Oper Status 157
 - Optionen 113 , 208 , 269 , 357 , 371 , 380 , 392 , 401 , 436 , 457 , 463 , 474 , 490 , 494 , 505 , 514
 - Organisation 127
 - Organisationseinheit 127
 - Original Quell-Port/Bereich 213
 - Original Ziel-IP-Adresse/Netzmaske 213
 - Original Ziel-Port/Bereich 213
 - Originale Quell-IP-Adresse/Netzmaske 213
 - Ort 127
 - OSPF-Modus 298 , 370 , 377
- P**
- Pakete 519
 - Password 479
 - Passwort 120 , 125 , 130 , 131 , 156 , 276 , 281 , 286 , 291 , 300 , 354 , 362 , 366 , 373 , 418 , 436 , 445 , 509 , 514
 - Passwörter 80
 - Passwörter und Schlüssel als Klartext anzeigen 82
 - Peak Cell Rate (PCR) 312
 - Peer-Adresse 323
 - Peer-ID 323
 - PFS-Gruppe verwenden 348
 - Phase-1-Profil 330
 - Phase-1-Profile 339
 - Phase-2-Profil 330
 - Phase-2-Profile 347
 - Physikalische Schnittstellen 134
 - Physikalische Verbindung 145
 - Physische Adresse 535
 - Ping 96
 - Ping-Generator 462
 - Ping-Test 492
 - PLMN 158
 - PMTU propagieren 351

- Poisoned Reverse 259
 - Pool-Verwendung 424
 - Pop-Up-Fenster für Statusanzeige 473
 - POP3-Server 509
 - POP3-Timeout 509
 - Port 420 , 534
 - Port-Verwendung 139
 - Portkonfiguration 135 , 166
 - Portname 139
 - Portweiterleitungen 210
 - Positiver Cache 407
 - PPPoA 285
 - PPPoE 275
 - PPPoE-Ethernet-Schnittstelle 276
 - PPPoE-Modus 276
 - PPPoE-Schnittstelle für Mehrfachlink 276
 - PPTP 280 , 372
 - PPTP-Adressmodus 283
 - PPTP-Ethernet-Schnittstelle 281
 - PPTP-Inaktivität 393
 - PPTP-Modus 373
 - PPTP-Passthrough 210
 - PPTP-Tunnel 372
 - Pre-Empt-Modus (zurück in Master-Status) 487
 - Preshared Key 323
 - Preshared Key 188 , 192 , 195
 - Primärer DNS-Server 409
 - Primärer DHCP-Server 428
 - Primary IP Address 482
 - Priorisierungsalgorithmus 235
 - Priorität 105 , 110 , 238 , 388 , 409
 - Priorität der virtuellen Schnittstelle 486
 - Priority Queueing 238
 - Privaten Schlüssel generieren 125
 - Profile 306
 - Proposals 340 , 348
 - Protokoll 207 , 213 , 224 , 228 , 244 , 329 , 397 , 420 , 445 , 475 , 502
 - Protokollformat 505
 - Protokollierte Aktionen 392
 - Protokollierungslevel 100
 - Provider 307 , 418
 - Providernamen 420
 - Provisioning-Server 426
 - Proxy ARP 162 , 332
 - Proxy-ARP-Modus 298 , 370 , 377
 - Proxy-Schnittstelle 268
 - PUK 149
 - PVID 166
- Q**
- QoS 227 , 390 , 535
 - QoS anwenden 388
 - QoS-Filter 227
 - QoS-Klassifizierung 231
 - QoS-Queue 535
 - QoS-Schnittstellen/Richtlinien 234
 - Quell-IP-Adresse 439 , 445 , 459 , 462
 - Quell-IP-Adresse/Netzmaske 204 , 213 , 224 , 228 , 244 , 329 , 475
 - Quell-Port 204 , 329
 - Quell-Port/Bereich 213 , 224 , 228 , 244 , 475
 - Quelle 388 , 445 , 496
 - Quellportbereich 397
 - Quellschnittstelle 204 , 224 , 271
 - Queued 535
 - Queues/Richtlinien 235
- R**
- RA-Signierungszertifikat 125
 - RA-Verschlüsselungszertifikat 125
 - RADIUS 103
 - RADIUS-Dialout 107
 - RADIUS-Passwort 105
 - RADIUS-Server Gruppen-ID 354
 - Rate 530 , 533
 - Rauschen dBm 528 , 530 , 531 , 533
 - Real Time Jitter Control 235
 - Real Time Jitter Control 318
 - Regelkette 248 , 250 , 481
 - Regelketten 247

- Region 198
- Regulierte Schnittstellen 318
- Remote Authentifizierung 103
- Remote-Adresse 525
- Retransmission Timer 261
- RFC 2091-Variabler Timer 259
- RFC 2453-Variabler Timer 259
- Richtlinie 107 , 111
- Richtlinien 387
- Richtung 231 , 258 , 522 , 523
- Richtung des Datenverkehrs 439
- RIP 254
- RIP-Filter 257
- RIP-Optionen 259
- RIP-Schnittstellen 254
- RIP-UDP-Port 259
- Roaming-Modus 154
- Roaming-Profil 180
- Robustheit 266
- Rolle 354
- Routen 200
- Routenankündigung 255
- Routeneinträge 277 , 282 , 287 , 293 ,
301 , 326 , 367 , 375 , 383
- Routenklasse 202
- Routenselektor 222
- Routentimeout 260
- Routentyp 202 , 207
- Routing-Protokolle 254
- RSA-Schlüsselstatus 99
- RTS Frames ohne CTS 527
- RTS Threshold 177 , 180
- RTSP 402
- RTSP-Port 403
- RTSP-Proxy 402 , 403
- RTT-Modus (Realtime-Traffic-Modus)
238
- Rufnummer 157 , 297
- Rx-Bytes 524 , 525
- Rx-Fehler 524
- Rx-Pakete 524 , 525 , 526 , 528 , 530
, 531 , 533
- SAs mit dem Status der ISP-
Schnittstelle synchronisieren 358
- Scan-Intervall 180
- Scan-Schwelle 180
- SCEP-Server-URL 445
- SCEP-URL 125
- Schedule-Intervall 457
- Scheduling 437
- Schlüsselgröße 445
- Schlüsselwert 383
- Schnittstelle 94 , 95 , 97 , 166 , 202 ,
207 , 209 , 212 , 221 , 235 , 250 ,
258 , 266 , 319 , 391 , 409 , 412 ,
418 , 424 , 445 , 461 , 466 , 471 ,
481 , 522 , 523 , 535 , 535
- Schnittstelle des virtuellen Routers
486
- Schnittstelle ist UPnP-kontrolliert 466
- Schnittstelle - Verbindungsinformation -
Link 76
- Schnittstellen 92 , 159 , 231 , 393 ,
460 , 466 , 504 , 523
- Schnittstellenaktion 461
- Schnittstellenauswahl 252
- Schnittstellenbeschreibung 92
- Schnittstellenmodus 160 , 409
- Schnittstellenmodus /
Bridge-Gruppen 90
- Schnittstellenstatus 439
- Schnittstellenstatus festlegen 445
- Schnittstellenzuweisung 249 , 481
- Schutz 192
- Schweregrad 507
- Segment-Sendeintervall 315
- Sekundärer DNS-Server 409
- Sekundärer DHCP-Server 428
- Sende WOL-Paket über Schnittstelle
479
- Sendeintervall für Advertisements
487
- Sendeleistung 171
- Senden 535
- Sequenznummern der Datenpakete
364

S

- Seriennummer 75
- Server 420
- Server Timeout 107
- Server aktivieren 437
- Server-IP-Adresse 105 , 110
- Server-URL 445
- Serveradresse 445
- Serverfehler 415
- Setze COS Wert (802.1p/Layer 2) 231
- Setze DSCP/TOS Wert (Layer 3) 231
- Short Guard Interval 177 , 180
- Short Retry Limit 177 , 180
- Sicherheitsalgorithmus 518
- Sicherheitsmodus 188 , 195
- Signal 197
- Signal dBm 528
- Signal dBm (RSSI1, RSSI2, RSSI3) 530 , 531 , 533
- SIM-Karte verwendet PIN 149
- SIP 401
- SIP Port 401
- SIP-Aufrufe priorisieren 401
- SIP-Proxy 401
- SMS-Gerät 510
- SMTP-Authentifizierung 509
- SMTP-Server 509
- SNMP 96 , 101 , 511
- SNMP Read Community 81
- SNMP Trap Broadcasting 512
- SNMP Write Community 81
- SNMP-Listen-UDP-Port 102
- SNMP-Trap-Community 512
- SNMP-Trap-Hosts 513
- SNMP-Trap-Optionen 511
- SNMP-Trap-UDP-Port 512
- SNMP-Version 102
- SNR dB 530 , 533
- Software & Konfiguration 494
- Special Handling Timer 224
- Special Session Handling 223
- Spezifische Ports 379
- Sprache für Anmeldefenster 471
- SSH 96 , 97
- SSH-Dienst aktiv 98
- SSH-Port 98
- Staat/Provinz 127
- Stack 522
- Standard-Benutzerpasswort 105
- Standard-Ethernet für PPPoE-Schnittstellen 309
- Standard-Timeout bei Inaktivität 473
- Standardeinstellungen wiederherstellen 96
- Standardmäßige Routenverteilung 259
- Standardroute 277 , 282 , 287 , 293 , 301 , 326 , 367 , 375 , 383
- Standort 78
- Startmodus 330
- Startzeit 443 , 523
- Statische Hosts 410
- Statistik 415 , 523
- Status 74 , 158 , 439 , 518 , 521 , 522 , 524 , 525
- Status festlegen 445
- Status des Auslösers 445
- Stoppzeit 443
- Subjektnamen 445
- Subsystem 517
- Sustained Cell Rate (SCR) 312
- Switch-Port 136
- Synchronisationsmodus 490
- Syslog-Server 502
- System 77
- System als Zeitserver 85
- Systemadministrator-Passwort bestätigen 81
- Systemdatum 75
- Systemlizenzen 88
- Systemlogik 496
- Systemmeldungen 516
- Systemname 78
- Systemneustart 499
- Systemprotokoll 501
- Systemverwaltung 74

T

- TACACS+ 109
 - TACACS+-Passwort 110
 - Tag 432
 - Target MAC-Address 479
 - TCP-ACK-Pakete priorisieren 278 ,
283 , 288 , 302 , 310 , 369
 - TCP-Inaktivität 393
 - TCP-Keepalives 100
 - TCP-MSS-Clamping 162
 - TCP-Port 111
 - TCP-Port des CAPI-Servers 437
 - Telnet 96
 - Tickettyp 473
 - Timeout 111 , 465
 - Timeout bei Inaktivität 276 , 281 , 286
, 291 , 300 , 366 , 373
 - Timeout für Nachrichten 507
 - Toleranzzeit beim Login 100
 - Traceroute-Test 493
 - Traffic Shaping 235 , 238 , 391
 - Transmit Shaping 146
 - Transparente MAC-Adresse 95
 - Trigger 461
 - TTL 411
 - Tunnelprofil 366
 - Tunnelprofile 361
 - Tx-Bytes 524 , 525
 - Tx-Fehler 524
 - Tx-Pakete 524 , 525 , 526 , 528 , 530
, 531 , 533
 - Typ 228 , 244 , 307 , 397 , 475 , 479 ,
524
- U**
- Überbuchen zugelassen 238
 - Überprüfung anhand einer Zertifi-
katsperrliste (CRL) 123
 - Überprüfung der Rückroute 332
 - Überprüfung der Rückroute 209
 - Übertragene MPDUs 527
 - Übertragener Datenverkehr 439
 - Übertragungsmodus 337
 - Übertragungsschlüssel 188 , 192 ,
195
 - Überwachte IP-Adresse 459
 - Überwachte Schnittstelle 439 , 461
 - Überwachte Subsysteme 507
 - Überwachte Variable 439
 - Überwachte Schnittstellen 464 , 514
 - Überwachtes Zertifikat 439
 - Überwachung 457
 - UDP-Inaktivität 393
 - UDP-Port 107
 - UDP-Quellport 363
 - UDP-Quellportauswahl 371
 - UDP-Zielport 363 , 371 , 514
 - UMTS/LTE 148 , 299
 - UMTS/LTE-Schnittstelle 300
 - UMTS/LTE-Status 149
 - Ungültige DNS-Pakete 415
 - Unicast MPDUs erfolgreich erhalten
527
 - Unicast MSDUs erfolgreich
übertragen 527
 - Unveränderliche Parameter 226
 - UPnP 465
 - UPnP TCP Port 467
 - UPnP-Status 467
 - Upstream 146
 - Uptime 75 , 528 , 530 , 531 , 533
 - URL 496
 - URL Pfadtiefe 429
 - URL / IP-Adresse 434
- V**
- Verbindungsstatus 228 , 244 , 475
 - Verbindungstyp 291 , 366
 - Verbleibende Gültigkeitsdauer 439
 - Verbunden 197
 - Vergleichsbedingung 439
 - Vergleichswert 439
 - Verlauf 434
 - Vermeidung von Datenstau (RED)
241
 - Verschlüsselt 521
 - Verschlüsselung 111 , 294 , 369 , 376
 - Verschlüsselung der Konfiguration
496

- Verschlüsselungsalgorithmen 99
- Verschlüsselungsmethode 235
- Version in Empfangsrichtung 255
- Version in Senderichtung 255
- Versionsprüfung 445
- Versuche 439 , 445 , 462
- Verteilungsmodus 219
- Verteilungsrichtlinie 219 , 221
- Verteilungsverhältnis 221
- Vertrauenswürdigkeit des Zertifikats erzwingen 123
- Verwaltung 167 , 198
- Verwaltungs-VID 167
- Verwerfen ohne Rückmeldung 250
- Verwerfen ohne Rückmeldung 210
- Verworfen 521 , 535
- Virtual Channel Identifier (VCI) 307
- Virtual Channel Connection (VCC) 312 , 315
- Virtual Path Connection (VPC) 315
- Virtual Path Identifier (VPI) 307
- Virtual Router Backup 482
- Virtual Router Master 482
- Virtuelle Router 483
- Virtueller Router 482
- VLAN 163 , 276
- VLAN Identifier 165
- VLAN aktivieren 167
- VLAN-ID 160 , 276
- VLAN-Mitglieder 165
- VLAN-Name 165
- VLANs 165
- VoIP 401
- Vollständige Filterung 392
- Vollständige IPSec-Konfiguration löschen 357
- Vom NAT ausnehmen (DMZ) 252
- VPN 320
- VR-Synchronisation 489
- VRRP Advertisement 482
- VRRP-Router 482
- VSS 528

W

- Wählnummer 464
- Wake-On-LAN 475
- Wake-On-LAN Filter 479
- Wake-On-LAN Rule Chain 479
- Wake-on-LAN-Filter 475
- Walled Garden 471
- Walled Garden URL 471
- Walled Network / Netzmaske 471
- WAN 272
- Wartung 492
- WDS-Beschreibung 192
- WDS-Links 191
- Web-Filter 429
- Web-Filter-Status 429
- Weitergeleitet 521
- Weitergeleitete Anfragen 415
- Weiterleiten 270 , 412
- Weiterleiten an 412
- WEP-Schlüssel 1 192
- WEP-Schlüssel 2 192
- WEP-Schlüssel 3 192
- WEP-Schlüssel 4 192
- WEP-Schlüssel 1-4 188 , 195
- Wert 527
- Wiederholungen 107
- Wildcard 419
- Wildcard-MAC-Adresse 95
- Wildcard-Modus 95
- WINS-Server 406
- Wireless LAN 168
- WLAN 169 , 526
- WLAN-Modul auswählen 445
- WLANx 526
- WLC-SSID 445
- WMM 187
- WOL-Regeln 478
- WPA Cipher 188 , 195
- WPA-Modus 188 , 195
- WPA2 Cipher 188 , 195

X

- X.31 (X.25 im D-Kanal) 141
- X.31 TEI-Dienst 141
- X.31 TEI-Wert 141

- XAUTH-Profil 330
- XAUTH-Profile 353
- Z**
- Zeit 517
- Zeit einstellen 84
- Zeitaktualisierungsintervall 85 , 87
- Zeitaktualisierungsrichtlinie 85
- Zeitbedingung 443
- Zeitplan (Start-/Stopzeit) 432
- Zeitstempel 502
- Zeitzone 84
- Zero Cookies verwenden 358
- Zertifikat in Konfiguration schreiben 445
- Zertifikat ist ein CA-Zertifikat 123
- Zertifikate 121
- Zertifikate und Schlüssel einschließen 496
- Zertifikatsanforderung 124
- Zertifikatsanforderungs-Payloads nicht beachten 360
- Zertifikatsanforderungs-Payloads senden 360
- Zertifikatsanforderungsbeschreibung 125 , 445
- Zertifikatsketten senden 360
- Zertifikatsliste 122
- Zertifikatsserver 132
- Ziel 388
- Ziel-IP-Adresse 207 , 439 , 445 , 462
- Ziel-IP-Adresse/Netzmaske 203 , 213 , 224 , 228 , 244 , 329 , 475
- Ziel-Port/Bereich 213 , 224 , 228 , 244 , 475
- Zielport 204 , 329
- Zielportbereich 397
- Zielschnittstelle 271
- Zugangs-Level 120
- Zugangstyp 158
- Zugriff 436
- Zugriffsfilter 243 , 248
- Zugriffskontrolle 191
- Zugriffsprofile 114
- Zugriffsregeln 242
- Zulässiger Hotspot-Client 473
- Zum SNMP Browser wechseln 116
- Zusammenfassend 127
- Zusätzliche, frei zugängliche Domänennamen 471
- Zusätzlicher Filter des Datenverkehrs 328 , 329
- Zweiter Zeitserver 85
- Zweiter Verwendeter Kanal 171