



Benutzerhandbuch be.IP

Copyright© Version 10.1.7 RC2 (SVN 5159) bintec elmeg GmbH

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

bintec elmeg GmbH gibt keinerlei Gewährleistung auf die in dieser Bedienungsanleitung enthaltenen Informationen. bintec elmeg GmbH übernimmt keine Haftung für mittelbare, unmittelbare, Neben-, Folge- oder andere Schäden, die mit der Auslieferung, Bereitstellung oder Benutzung dieser Bedienungsanleitung im Zusammenhang stehen.

Copyright © bintec elmeg GmbH

Alle Rechte an den hier beinhalteten Daten - insbesondere Vervielfältigung und Weitergabe - sind bintec elmeg GmbH vorbehalten.

Open Source Software in diesem Produkt

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

GEMA

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

Inhaltsverzeichnis

Kapitel 1	Inbetriebnahme	1
1.1	be.IP	1
1.1.1	Aufstellen und Anschließen	1
1.1.2	Anschlüsse	2
1.1.3	Anschlüsse (seitlich)	3
1.1.4	Montagewinkel	3
1.1.5	LEDs	3
1.1.6	Lieferumfang	6
1.1.7	Allgemeine Produktmerkmale	6
1.2	Reset	8
1.3	Voreinstellungen	8
1.4	Support-Information	9
Kapitel 2	Montage	10
2.1	Anschluss von Endgeräten	10
2.1.1	Interner ISDN-Anschluss	10
2.1.2	Terminierung der ISDN-Schnittstellen	10
2.2	Reset Taster	11
2.3	Wandmontage	11
2.4	Pin-Belegungen	12
2.4.1	Ethernet-Schnittstellen	12
2.4.2	ISDN-Schnittstelle	13
2.4.3	xDSL-Schnittstelle	13
2.4.4	Serielle Schnittstelle	14
2.4.5	USB-Schnittstelle	14
Kapitel 3	Grundkonfiguration	16

3.1	Vorbereitungen	16
3.1.1	Systemsoftware	16
3.1.2	System-Voraussetzungen	16
3.1.3	Daten sammeln	17
3.1.4	PC einrichten	18
3.2	Konfiguration des Systems.	19
3.2.1	Netzwerkeinstellung (LAN)	20
3.2.2	SIP-Provider eintragen	20
3.3	Internetverbindung einrichten.	20
3.3.1	Internetverbindung über das interne VDSL-Modem	20
3.3.2	Andere Internetverbindungen.	20
3.3.3	Konfiguration prüfen	21
3.4	Softwareaktualisierung be.IP	21
Kapitel 4	Zugang und Konfiguration	23
4.1	Zugang über LAN	23
4.1.1	HTTP/HTTPS	23
4.2	Konfiguration.	23
4.2.1	Konfigurationsoberfläche	23
Kapitel 5	Assistenten	32
Kapitel 6	Systemverwaltung	33
6.1	Status.	33
6.2	Globale Einstellungen	36
6.2.1	System	36
6.2.2	Passwörter	38
6.2.3	Datum und Uhrzeit	40
6.2.4	Systemlizenzen	44

6.3	Schnittstellenmodus / Bridge-Gruppen	46
6.3.1	Schnittstellen	48
6.4	Administrativer Zugriff	51
6.4.1	Zugriff	52
6.5	Remote Authentifizierung	53
6.5.1	RADIUS	53
6.5.2	Optionen	59
6.6	Konfigurationszugriff	59
6.6.1	Zugriffsprofile	60
6.6.2	Benutzer	62
6.7	Zertifikate	64
6.7.1	Zertifikatsliste	64
6.7.2	CRLs	72
6.7.3	Zertifikatsserver	73
Kapitel 7	Physikalische Schnittstellen	74
7.1	Ethernet-Ports	74
7.1.1	Portkonfiguration	75
7.2	ISDN-Ports	77
7.2.1	ISDN-Konfiguration	77
7.2.2	MSN-Konfiguration	79
7.3	DSL-Modem	82
7.3.1	DSL-Konfiguration	82
7.4	UMTS/LTE	84
7.4.1	UMTS/LTE	84
Kapitel 8	LAN	94
8.1	IP-Konfiguration	94
8.1.1	Schnittstellen	94

8.2	VLAN	107
8.2.1	VLANs	108
8.2.2	Portkonfiguration	109
8.2.3	Verwaltung	109
Kapitel 9	Wireless LAN Controller	111
9.1	Wizard	111
9.1.1	Grundeinstellungen	112
9.1.2	Funkmodulprofil	113
9.1.3	Drahtlosnetzwerk	113
9.1.4	Automatische Installation starten	115
9.2	Controller-Konfiguration	117
9.2.1	Allgemein	117
9.2.2	Slave-AP-Autoprofil	119
9.3	Slave-AP-Konfiguration	121
9.3.1	Slave Access Points	121
9.3.2	Funkmodulprofile	124
9.3.3	Drahtlosnetzwerke (VSS)	130
9.4	Monitoring	138
9.4.1	WLAN Controller	138
9.4.2	Slave Access Points	138
9.4.3	Aktive Clients	139
9.4.4	Drahtlosnetzwerke (VSS)	140
9.4.5	Client-Verwaltung	140
9.5	Umgebungs-Monitoring	140
9.5.1	Benachbarte APs	140
9.5.2	Rogue APs	141
9.5.3	Rogue Clients	142
9.6	Wartung	143
9.6.1	Firmware-Wartung	143

Kapitel 10	Netzwerk	145
10.1	Routen	145
10.1.1	Konfiguration von IPv4-Routen	145
10.1.2	Konfiguration von IPv6-Routen	151
10.1.3	IPv4-Routing-Tabelle	153
10.1.4	IPv6-Routing-Tabelle	154
10.1.5	Optionen	154
10.2	Allgemeine IPv6-Präfixe	156
10.2.1	Konfiguration eines Allgemeinen Präfixes	156
10.3	NAT	157
10.3.1	NAT-Schnittstellen	158
10.3.2	NAT-Konfiguration	159
10.3.3	NAT - Konfigurationsbeispiel	165
10.4	Lastverteilung	168
10.4.1	Lastverteilungsgruppen	168
10.4.2	Special Session Handling	172
10.4.3	Lastverteilung - Konfigurationsbeispiel.	176
10.5	QoS	178
10.5.1	IPv4/IPv6-Filter	179
10.5.2	QoS-Klassifizierung	182
10.5.3	QoS-Schnittstellen/Richtlinien	185
10.6	Zugriffsregeln	193
10.6.1	Zugriffsfiler	194
10.6.2	Regelketten	198
10.6.3	Schnittstellenzuweisung	199
Kapitel 11	Multicast.	201
11.1	Allgemein	203
11.1.1	Allgemein	203

11.2	IGMP	203
11.2.1	IGMP	203
11.2.2	Optionen	206
11.3	Weiterleiten	207
11.3.1	Weiterleiten	207
Kapitel 12	WAN.	209
12.1	Internet + Einwählen	209
12.1.1	PPPoE	210
12.1.2	PPTP	217
12.1.3	PPPoA	221
12.1.4	UMTS/LTE	227
12.1.5	IP Pools	230
12.2	ATM	231
12.2.1	Profile	232
12.2.2	Dienstkategorien	237
12.2.3	OAM-Regelung	239
12.3	Real Time Jitter Control	243
12.3.1	Regulierte Schnittstellen	243
Kapitel 13	VPN	245
13.1	IPSec	245
13.1.1	IPSec-Peers	246
13.1.2	Phase-1-Profile	264
13.1.3	Phase-2-Profile	271
13.1.4	XAUTH-Profile	276
13.1.5	IP Pools	278
13.1.6	Optionen	279
13.2	be.IP Secure Client	282

Kapitel 14	Firewall	283
14.1	Richtlinien	285
14.1.1	IPv4-Filterregeln	285
14.1.2	IPv6-Filterregeln	287
14.1.3	Optionen	290
14.2	Schnittstellen	292
14.2.1	IPv4-Gruppen	292
14.2.2	IPv6-Gruppen	293
14.3	Adressen	293
14.3.1	Adressliste	293
14.3.2	Gruppen	295
14.4	Dienste	295
14.4.1	Dienstliste	296
14.4.2	Gruppen	298
14.5	Konfiguration	298
14.5.1	SIF - Konfigurationsbeispiel	298
Kapitel 15	VoIP	303
15.1	Einstellungen	303
15.1.1	Teilnehmer	303
15.1.2	SIP-Konten	308
15.1.3	Standorte	315
15.1.4	ISDN-Trunks	318
15.1.5	Optionen	319
15.2	Media Gateway	323
15.2.1	Anrufkontrolle	324
15.2.2	CLID-Umwandlung	327
15.2.3	Rufnummertransformation	329

Kapitel 16	Lokale Dienste	332
16.1	DNS	332
16.1.1	Globale Einstellungen	334
16.1.2	DNS-Server	336
16.1.3	Statische Hosts	338
16.1.4	Domänenweiterleitung	339
16.1.5	Dynamische Hosts	341
16.1.6	Cache	341
16.1.7	Statistik	341
16.2	HTTPS	342
16.2.1	HTTPS-Server	342
16.3	DynDNS-Client	343
16.3.1	DynDNS-Aktualisierung	344
16.3.2	DynDNS-Provider	345
16.4	DHCP-Server	346
16.4.1	IP-Pool-Konfiguration	347
16.4.2	DHCP-Konfiguration	348
16.4.3	IP/MAC-Bindung	352
16.4.4	DHCP-Relay-Einstellungen	353
16.4.5	DHCP - Konfigurationsbeispiel	354
16.5	DHCPv6-Server	357
16.5.1	DHCPv6-Server	358
16.5.2	Globale DHCPv6-Optionen	360
16.5.3	Zustandsbehaftete Clients	362
16.5.4	Konfiguration von zustandsbehafteten Clients	362
16.6	CAPI-Server	363
16.6.1	Benutzer	363
16.6.2	Optionen	364
16.7	Scheduling	364

16.7.1	Auslöser	366
16.7.2	Aktionen	372
16.7.3	Optionen	384
16.7.4	Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling)	384
16.8	Überwachung	388
16.8.1	Hosts	388
16.8.2	Schnittstellen	390
16.8.3	Ping-Generator	392
16.9	UPnP	393
16.9.1	Schnittstellen	393
16.9.2	Allgemein	394
16.10	Wake-On-LAN	395
16.10.1	Wake-on-LAN-Filter	395
16.10.2	WOL-Regeln	399
16.10.3	Schnittstellenzuweisung	401
16.11	Trace-Schnittstelle	401
16.11.1	Trace-Schnittstelle	401
Kapitel 17	Wartung	403
17.1	Benutzer ausloggen	403
17.1.1	Benutzer ausloggen	403
17.2	Diagnose	404
17.2.1	Ping-Test	404
17.2.2	DNS-Test	404
17.2.3	Traceroute-Test	405
17.3	Software & Konfiguration	405
17.3.1	Optionen	405
17.4	Neustart	410
17.4.1	Systemneustart	410

17.5	Factory Reset	411
Kapitel 18	Externe Berichterstellung.	412
18.1	Systemprotokoll	412
18.1.1	Syslog-Server	412
18.2	IP-Accounting	414
18.2.1	Schnittstellen	415
18.2.2	Optionen	415
18.3	Benachrichtigungsdienst	416
18.3.1	Benachrichtigungsempfänger	416
18.3.2	Benachrichtigungseinstellungen	418
18.4	SIA	420
18.4.1	SIA	420
Kapitel 19	Monitoring	421
19.1	Internes Protokoll	421
19.1.1	Systemmeldungen	421
19.2	IPSec	421
19.2.1	IPSec-Tunnel	421
19.2.2	IPSec-Statistiken	423
19.3	ISDN/Modem	424
19.3.1	Aktuelle Anrufe	424
19.3.2	Anrufliste	425
19.4	Schnittstellen	425
19.4.1	Statistik	425
19.4.2	Netzwerk-Status	427
19.5	WLAN.	427
19.5.1	WLANx	427
19.5.2	VSS	428

- 19.5.3 Client-Verwaltung 430
- 19.5.4 Bridge-Links 431
- 19.6 Bridges 432
- 19.6.1 br<x> 432
- 19.7 QoS 433
- 19.7.1 QoS 433

- Glossar 434

- Index 475

Kapitel 1 Inbetriebnahme

1.1 be.IP

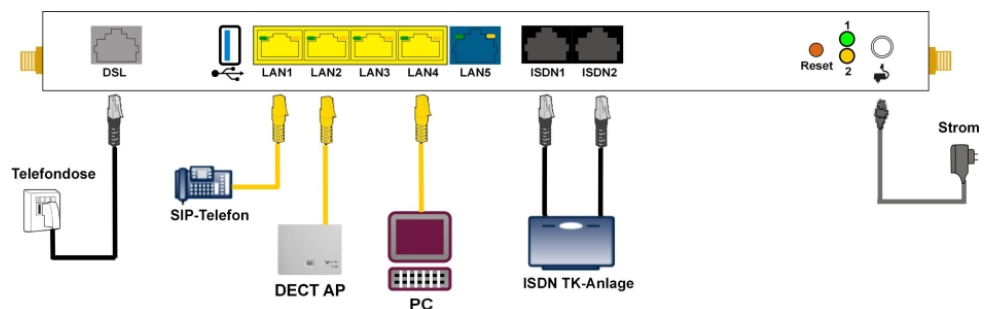
In diesem Kapitel erfahren Sie, wie Sie Ihr Gerät aufstellen, anschließen und in Betrieb nehmen.

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

Die PDF-Version dieses Dokuments enthält eine schlanke Version des Handbuchs. Sie beinhaltet alle Informationen zur Installation und Montage sowie die Beschreibung der Konfigurationsparameter, aber keine Screenshots. Eine HTML-basierte Version mit Screenshots ist im Downloadbereich Ihres Gerätes als ZIP-Datei verfügbar. Entpacken Sie die ZIP-Datei in einen Ordner Ihrer Wahl und rufen Sie die Datei "start.html" in einem Webbrowser auf.

1.1.1 Aufstellen und Anschließen

Die **be.IP** wird an einem reinen IP-Anschluss betrieben. Sie telefonieren ausschließlich über VoIP, sind aber beim Anschluss Ihrer Endgeräte nicht eingeschränkt: Sie können SIP- und ISDN-Endgeräte sowie PCs anschließen.



Achtung

Vor Installation und Inbetriebnahme Ihres Geräts lesen Sie bitte aufmerksam die beiliegenden Sicherheitshinweise.



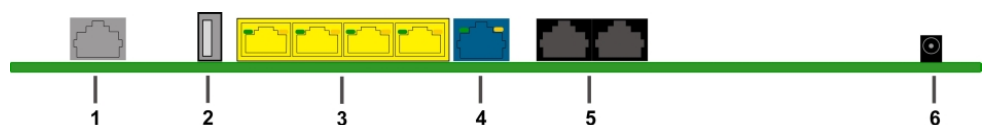
Achtung

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

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

- (1) Montage
Um einen störungsfreien Betrieb zu gewährleisten, sollte die **be.IP** aufrecht an einer Wand oder gut belüftet in einem Netzwerkschrank montiert sein (lesen Sie bitte aufmerksam das Kapitel *Montage* auf Seite 10).
- (2) Netzanschluss
Schließen Sie den Netzanschluss des Geräts mit dem mitgelieferten Steckernetzgerät an eine 230 V~ Steckdose an.
- (3) Antennen
Schrauben Sie die mitgelieferten Antennen auf die dafür vorgesehenen Anschlüsse.
- (4) DSL
Verbinden Sie den Anschluss **DSL** über das graue Kabel an die TAE-Buchse der Telefondose an.
- (5) ISDN-TK-Anlage
Schließen Sie eine ISDN-TK-Anlage an den internen ISDN-Anschluss der **be.IP** an.
- (6) SIP-Telefone
Schließen Sie Ihre SIP-Telefone an die 10/100/1000 Base-T Ethernet-Schnittstellen an.
- (7) PC
Schließen Sie einen geeigneten PC über ein Ethernet-Kabel an eine der Ethernet-Schnittstellen der **be.IP** an. Sollten Probleme bei der Verbindung zwischen PC und **be.IP** auftreten, lesen Sie bitte die entsprechenden Kapitel zur Grundkonfiguration.
- (8) VoIP
Für einen reinen IP-Anschluss ohne ISDN verwenden Sie die vom Provider bereitgestellte Anleitung.

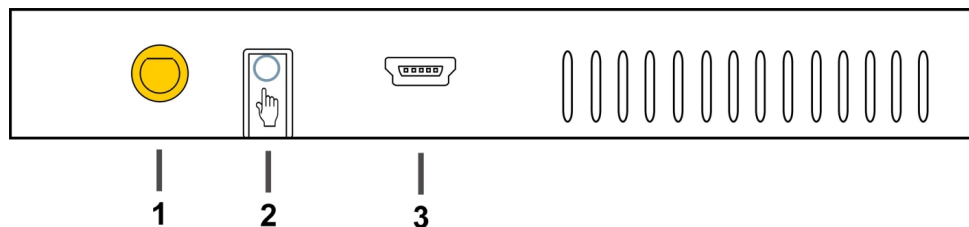
1.1.2 Anschlüsse



1	DSL-Schnittstelle Annex B/J
2	USB-Schnittstelle

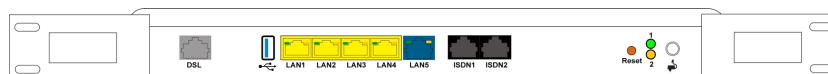
3	10/100/1000 Base-T Ethernet-Schnittstellen (LAN 1 - LAN4)
4	Ethernet-WAN-Schnittstelle (LAN5)
5	Schnittstelle für ISDN-Endgeräte oder eine ISDN-TK-Anlage (ISDN1, ISDN2)
6	Buchse für das Steckernetzteil

1.1.3 Anschlüsse (seitlich)



1	Antennenanschluss
2	Funktionstaste
3	Console

1.1.4 Montagewinkel



Aufgrund der Platzierung der Geräte im Netzwerkschrank, empfiehlt es sich auf abgesetzte Antennen zurückzugreifen. Montieren Sie die Montagewinkel mit den im Set beiliegenden Schrauben am Gehäuse. Die Montagewinkel und die Schrauben sind als Zubehör erhältlich (Artikelnummer MN40285514).



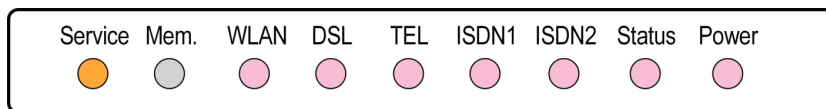
Hinweis

Bei Betrieb im Netzwerkschrank darf die Umgebungstemperatur 40 °C nicht übersteigen!

1.1.5 LEDs

Anhand der LEDs können Sie den Status Ihres Geräts ablesen.

Die LEDs der **be.IP** sind folgendermaßen angeordnet:



Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Service	an	Automatische Wartung aktiv (wird derzeit nicht unterstützt)
	aus	Automatische Wartung inaktiv
Mem.		ohne Funktion
WLAN	aus	WLAN oder alle zugeordneten Drahtlosnetzwerk deaktiviert
	langsam blinkend	Drahtlosnetzwerk ist aktiv, kein Client ist angemeldet
	schnell blinkend	Drahtlosnetzwerk ist aktiv, mindestens ein Client ist angemeldet
DSL	flackernd	Drahtlosnetzwerk ist aktiv, mindestens ein Client ist angemeldet, es besteht Datenverkehr
	an	Verbindung hergestellt
	langsam blinkend	Synchronisation läuft
	aus	Keine Synchronisation
TEL	flackernd	Datentransfer
	an	Telefonie am IP-Anschluss (Voice over IP) bereit
ISDN1 / ISDN 2	aus	Telefonie nicht eingerichtet
	an	ISDN-Endgeräte angeschlossen
Status	aus	Ruhezustand oder außer Betrieb
	an	Nach dem Einschalten: Gerät wird gestartet während des Betriebs: Fehler
Power	langsam blinkend	Gerät ist aktiv
	an	Stromversorgung ist angeschlossen
	aus	Keine Stromversorgung

Die LEDs der Ethernet-Buchsen LAN 1-4 (LAN) und LAN 5 (WAN) zeigen folgende Statusinformationen an:

Ethernet-LEDs

LED	Farbe	Status	Information
LAN 1 bis 4 (Link/Act)	Grün	an	Ethernet -Verbindung hergestellt
LAN 1 bis 4 (Link/Act)	Grün	blinkend	Datenübertragung über Ethernet
LAN 1 bis 4 (Link/Act)		aus	Keine Ethernet-Verbindung
LAN 1 bis 4 (Speed)	Grün	an	1000 Mbit/s Übertragungsrate
LAN 1 bis 4 (Speed)	Orange	an	100 Mbit/s Übertragungsrate
LAN 1 bis 4 (Speed)		aus	10 Mbit/s Übertragungsrate
LAN 5 (Link/Act)	Grün	an	WAN- Ethernet -Verbindung hergestellt
LAN 5 (Link/Act)	Grün	blinkend	Daten über ETH 5 senden/ empfangen
LAN 5 (Link/Act)		aus	Keine Ethernet-Verbindung
LAN 5 (Speed)	Grün	an	1000 Mbit/s Übertragungsrate
LAN 5 (Speed)	Orange	an	100 Mbit/s Übertragungsrate
LAN 5 (Speed)		aus	10 Mbit/s Übertragungsrate

Leuchtdioden Ansicht Anschlussseite

Die LEDs sind mit den LEDs auf der Vorderseite gekoppelt und zeigen das gleiche Leuchtverhalten.



- 1 Status Grün
- 2 Service Gelb (wird derzeit nicht unterstützt)

1.1.6 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Produktname	Kabelsätze/Sonstiges	Dokumentation
be.IP	ein Ethernet LAN-Kabel (gelb)	Installationsposter
	ein Ethernet WAN-Kabel (blau)	Sicherheitshinweise
	ein DSL-Kabel (grau)	
	ein Netzteil	
	zwei WiFi-Antennen	
	19" Kit und Schrauben	

1.1.7 Allgemeine Produktmerkmale

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

Allgemeine Produktmerkmale be.IP

Eigenschaft	
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	328 x 193 x 44 mm
Gewicht	ca. 900 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1800 g
Speicher	128 MB SDRAM
LEDs	19 (8 x Funktion, 1 x Service, 5x2 Ethernet)

Eigenschaft	
Leistungsaufnahme Gerät	max. 24 W 12 V DC
Spannungsversorgung	12 V DC 2 A
Umweltanforderungen:	
Lagertemperatur	-20 °C bis +70 °C
Betriebstemperatur	+5 °C bis +40 °C
Relative Luftfeuchtigkeit	max. 85 %
Raumklassifizierung	Nur in trockenen Räumen betreiben
Verfügbare Schnittstellen:	
DSL-Schnittstelle	Internes DSL-Modem
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, auto-sensing, MDIX
ISDN-Schnittstellen	2 interne ISDN-Schnittstellen, ISDN-Terminierung
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud
Vorhandene Buchsen:	
WLAN Antennen	R-SMA-Buchsen
Ethernet-Schnittstellen 1 - 4 (LAN)	RJ45-Buchse
Ethernet-Schnittstelle 5 (WAN)	RJ45-Buchse
ISDN-Schnittstelle (ISDN1, ISDN2)	RJ45-Buchse
DSL-Schnittstelle	RJ45-Buchse
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse
USB	USB-Anschluss Typ A
Hohlsteckerbuchse für Stromversorgung	

1.2 Reset

Der Reset wird über den Reset-Knopf an der Anschlussseite des Systems durchgeführt.

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

Drücken Sie die Reset-Taste für ca. 30 bis 40 Sekunden, wird das Gerät in den Auslieferungszustand zurückversetzt. Die Verbindungsdaten ein und ausgehender Anrufe werden dabei nicht gelöscht. Die Konfiguration wird gelöscht und alle Passwörter werden zurückgesetzt. Der Reset ist beendet, wenn nach 30 bis 40 Sekunden die Status-LED gleichmäßig blinkt.

1.3 Voreinstellungen

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



Hinweis

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

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

Konfigurationsoberfläche

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

- **IP-Adresse:** *192.168.0.251*
- **Netzmaske:** *255.255.255.0*

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

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




Hinweis

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

Anbieterswahl

Bei der Erstanmeldung an der Web-Oberfläche haben Sie die Möglichkeit den Internet-Anbieter zu wählen.

Wenn Sie einen Anschluss der Deutschen Telekom in Betrieb nehmen wollen, folgen Sie den Schritten **Ersteinrichtung Telekom**. Mit der Schaltfläche **Weiter** können Sie die einzelnen Fenster durchlaufen (siehe auch Poster **Inbetriebnahme be.IP mit dem Schnellstartmenü**).

Wenn Sie einen Anschluss eines anderen Anbieters in Betrieb nehmen wollen, gelangen Sie auf die Statusseite des Geräts in der Ansicht **Benutzer**. Wenn Sie auf der Statusseite **Benutzer** auf die Schaltflächen  klicken, werden Sie direkt zu den **Assistenten** in das jeweilige Menü geführt.

1.4 Support-Information

Falls Sie zu Ihrem neuen Produkt Fragen haben, wenden Sie sich für prompte technische Unterstützung bitte an einen zertifizierten Fachhändler in Ihrer Nähe. Fachhändler sind von uns geschult und erhalten bevorzugt Support.

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

Kapitel 2 Montage



Warnung

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



Achtung

Um einen störungsfreien Betrieb zu gewährleisten, sollte die **be.IP** aufrecht an einer Wand oder gut belüftet in einem Netzwerkschrank montiert sein. Das Gerät darf keiner direkten Sonneneinstrahlung oder anderen Wärmequellen ausgesetzt sein. Beachten Sie auch die einzuhaltenden Abstände (siehe [Wandmontage](#) auf Seite 11).

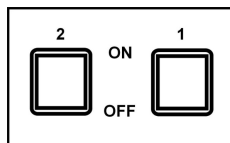
2.1 Anschluss von Endgeräten

2.1.1 Interner ISDN-Anschluss

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

2.1.2 Terminierung der ISDN-Schnittstellen

Die Schalter für die Terminierung der ISDN-Schnittstellen befinden sich im Boden/Unterschale des Geräts. Im Auslieferungszustand sind beide Schalter auf ON gestellt. Damit ist die Terminierung aktiv und das Gerät für alle gängigen Anwendungen vorkonfiguriert.



2.2 Reset Taster

An der Anschlussseite des Geräts befindet sich der Reset-Taster, mit dem Sie einen Neustart des Geräts erzwingen oder den Auslieferungszustand wieder herstellen können (siehe [Reset](#) auf Seite 8).

2.3 Wandmontage

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

- (1) Suchen Sie einen Montageort aus, der max. 1,5 Meter von einer 230 V ~ Netzsteckdose und 2,5 Meter vom Übergabepunkt des Netzbetreibers entfernt ist.
- (2) Um eine gegenseitige Beeinträchtigung auszuschließen, montieren Sie das Gerät nicht in unmittelbarer Nähe von elektronischen Geräten wie z. B. HiFi-Geräten, Bürogeräten oder Mikrowellengeräten. Vermeiden Sie auch einen Aufstellort in der Nähe von Wärmequellen, z. B. Heizkörpern oder in feuchten Räumen.
- (3) Halten Sie die Abstände ein, die auf der Rückseite des Geräts eingepreßt sind.
- (4) Markieren Sie die Bohrlöcher an der Wand.
- (5) Überprüfen Sie die feste Auflage aller Befestigungspunkte der **be.IP** an der Wand. Vergewissern Sie sich, dass im Bereich der markierten Bohrlöcher keine Versorgungsleitungen, Kabel o. ä. verlegt sind.
- (6) Bohren Sie die Befestigungslöcher an den markierten Stellen (bei Montage mit den Dübeln verwenden Sie einen 5 mm Steinbohrer). Setzen Sie die Dübel ein.
- (7) Schrauben Sie die beiden Schrauben so ein, dass zwischen Schraubenkopf und Wand noch ein Abstand von ca. 5 mm verbleibt.
- (8) Hängen Sie die **be.IP** mit den rückseitigen Halterungen von oben hinter den Schraubenköpfen ein.
- (9) Installieren Sie, wenn erforderlich, die Anschlussdosen für die Endgeräte. Verbinden Sie die Installation der Anschlussdosen mit der des Geräts. Die Anschlussdosen dienen der festen Installation, beispielsweise im Flur. Wenn diese installiert sind, werden die Anschlusskabel mit den Anschlüssen des Geräts verbunden.
- (10) Stecken Sie die Anschlüsse der Endgeräte in die Anschlussdosen.
- (11) Verbinden Sie die **be.IP** mit dem externen xDSL-Anschluss. Sie können dazu so vorgehen, wie auf dem beigelegten Installationsposter beschrieben.
- (12) Stecken Sie das Steckernetzgerät in die 230 V~ Steckdose.
- (13) Stecken Sie den Hohlstecker des Steckernetzgeräts in die entsprechende Buchse an Ihrem Gerät.

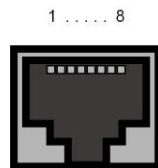
(14) Sie können das Gerät in Betrieb nehmen.

2.4 Pin-Belegungen

2.4.1 Ethernet-Schnittstellen

Die Geräte verfügen über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (LAN1 - LAN4) sowie über eine weitere Ethernet-Schnittstelle für den Anschluss einer WAN-Verbindung oder eines Servers.

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



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

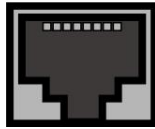
RJ45-Buchse für Ethernet-Anschluss

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

2.4.2 ISDN-Schnittstelle

Der Anschluss erfolgt über eine RJ45-Buchse:

1 8



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

RJ45-Buchse für ISDN-Anschluss

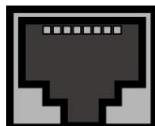
Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Senden (+)
4	Empfangen (+)
5	Empfangen (-)
6	Senden (-)
7	Nicht genutzt
8	Nicht genutzt

2.4.3 xDSL-Schnittstelle

Die **be.IP** verfügt über eine xDSL-Schnittstelle. Die xDSL-Schnittstelle wird mittels eines RJ45-Steckers vergebunden.

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

1 8



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

RJ45-Buchse für xDSL-Anschluss

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt

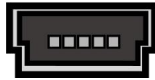
Pin	Funktion
3	Nicht genutzt
4	Leitung 1a
5	Leitung 1b
6	Nicht genutzt
7	Nicht genutzt
8	Nicht genutzt

2.4.4 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



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

2.4.5 USB-Schnittstelle

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

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



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

Kapitel 3 Grundkonfiguration

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

3.1 Vorbereitungen

Ihr Gerät ist werksseitig als DHCP-Server eingerichtet, es übermittelt also PCs in Ihrem LAN, die über keine IP-Konfiguration verfügen, alle für eine Verbindung notwendigen Einstellungen. Wie Sie den PC, mit dem Sie die Grundkonfiguration durchführen wollen, für den automatischen Bezug einer IP-Konfiguration einrichten, ist in [PC einrichten](#) auf Seite 18 beschrieben.



Hinweis

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

3.1.1 Systemsoftware

Das Gerät wird mit der zum Zeitpunkt der Produktion aktuellen Systemsoftwareversion betrieben. Die Systemsoftware wird fortwährend weiterentwickelt, um die Sicherheit und Funktionsvielfalt des Geräts zu erhöhen.

Eine Aktualisierung können Sie bequem mit der Konfigurationsoberfläche im Menü **Wartung->Software & Konfiguration** vornehmen. Eine Beschreibung der Vorgehensweise finden Sie in [Softwareaktualisierung be.IP](#) auf Seite 21.

3.1.2 System-Voraussetzungen

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

- geeignetes Betriebssystem (Windows, Linux, MAC OS)
- ein Web-Browser (internet Explorer, Firefox, Chrome) in der jeweils aktuellen Version
- installierte Netzwerkkarte (Ethernet)

- installiertes TCP/IP-Protokoll
- hohe Farbanzeige für die korrekte Darstellung der Grafiken

3.1.3 Daten sammeln

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

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

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

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

Grundkonfiguration

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

Netzwerkeinstellungen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	192.168.0.251	
Netzmaske Ihres Gateways	255.255.255.0	

SIP-Provider

Zugangsdaten	Beispielwert	Ihre Werte
Beschreibung	Geben Sie den Namen Ihres SIP-Providers an, z.B. <i>Sipgate</i> .	
Authentifizierungsname/Benutzername	Geben Sie Ihre ID ein, z.B. Ihre Email-Adresse	
Passwort	Geben Sie Ihr Passwort ein, das Sie vom SIP-Provider erhalten haben.	

Zugangsdaten	Beispielwert	Ihre Werte
Registrar	Geben Sie den entsprechenden Registrar ein, z. B. <i>sipgate.de</i> .	
Rufnummer	z. B. <i>123456</i>	

Daten für den Internetzugang über xDSL

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

3.1.4 PC einrichten

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

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

TCP/IP-Protokoll prüfen

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

- (1) Klicken Sie z. B. bei Windows 7 im Startmenü auf **Systemsteuerung** -> **Netzwerk- und Freigabecenter** -> **Adaptoreinstellungen ändern**.
- (2) Klicken Sie auf **LAN-Verbindung**.
- (3) Klicken Sie im Statusfenster auf **Eigenschaften**.
- (4) Suchen Sie in der Liste der Netzwerkkomponenten den Eintrag **Internetprotokoll (TCP/IP)**.

TCP/IP-Protokoll installieren

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

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

Windows PC als DHCP-Client konfigurieren

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

- (1) Gehen Sie zunächst vor, wie oben beschrieben, um die Netzwerkeigenschaften anzuzeigen.
- (2) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
- (3) Wählen Sie **IP-Adresse automatisch beziehen**.
- (4) Wählen Sie ebenfalls **DNS-Serveradresse automatisch beziehen**.
- (5) Schließen Sie alle Fenster mit **OK**.

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



Hinweis

Zur Konfiguration können Sie nun die Konfigurationsoberfläche aufrufen, indem Sie in einem unterstützten Browser die vorkonfigurierte IP-Adresse Ihres Gerätes eingeben (192.168.0.251) und sich mit den voreingestellten Anmeldedaten (**User:** *admin*, **Password:** *admin*) anmelden.

3.2 Konfiguration des Systems

3.2.1 Netzwerkeinstellung (LAN)

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

3.2.2 SIP-Provider eintragen

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

3.3 Internetverbindung einrichten

Sie können mit Ihrem Gerät eine Internetverbindung aufbauen.

3.3.1 Internetverbindung über das interne VDSL-Modem

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

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

3.3.2 Andere Internetverbindungen

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

3.3.3 Konfiguration prüfen

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

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

- (1) Testen Sie die Verbindung von einem beliebigen Gerät im lokalen Netzwerk zum Gerät. Klicken Sie im Windows-Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihres Geräts ein (z. B. `192.168.0.251`). Es erscheint ein Fenster mit dem Hinweis "Antwort von...".
- (2) Testen Sie den Internetzugang, indem Sie im Internet Browser <http://www.bintec-elmeg.com> eingeben.



Hinweis

Durch eine Fehlkonfiguration von Endgeräten kann es zu ungewollten Verbindungen und erhöhten Gebühren kommen! Kontrollieren Sie, ob das Gerät Verbindungen nur zu gewollten Zeiten aufbaut! Beobachten Sie die Leuchtanzeigen Ihres Geräts.

3.4 Softwareaktualisierung be.IP

Die Funktionsvielfalt der **be.IP** wird permanent erweitert. Eine Softwareaktualisierung kann 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 ->Optionen**.
- (2) Wählen Sie unter **Aktion** *Systemsoftware aktualisieren* und unter **Quelle** *Aktuelle Software vom Update-Server*.
- (3) Bestätigen Sie mit **Los**.

Alternativ können Sie eine Software-Aktualisierung in der Ansicht **Benutzer** durchführen. Klicken Sie auf der **Status**-Seite bei **Systemsoftware-Aktualisierung** auf die Schaltfläche **Aktualisierung**, um den Vorgang zu starten. Unterbrechen Sie weder die Internetverbindung noch die Stromversorgung.

Nach der Installation einer neuen Systemsoftware müssen Sie das System neu starten.

Optionen zu Software und Konfiguration	
Aktion	Systemsoftware aktualisieren ▼
Quelle	Aktuelle Software vom Update-Server ▼

START

Das Gerät verbindet sich nun mit dem Download-Server 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 **Start** 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 4 Zugang und Konfiguration

4.1 Zugang über LAN

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

4.1.1 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://192.168.0.251`

oder

`https://192.168.0.251`

4.2 Konfiguration

Die Konfiguration wird mit der HTML-Konfigurationsoberfläche durchgeführt.

4.2.1 Konfigurationsoberfläche

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

Die Einstellungsänderungen, die Sie vornehmen, werden mit der **OK-** bzw. **Übernehmen-**Schaltfläche des jeweiligen Menüs übernommen, ohne dass das Gerät neu gestartet werden muss. Wenn Sie die Konfiguration abschließen und so speichern möchten, dass sie beim nächsten Neustart des Geräts als Start-Konfiguration geladen wird, speichern Sie diese, indem Sie auf die Schaltfläche **Konfiguration speichern** klicken.

Mit der Konfigurationsoberfläche können Sie ebenfalls die wichtigsten Funktionsparameter Ihres Geräts überwachen.

4.2.1.1 Die Konfigurationsoberfläche aufrufen

- (1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind.
- (2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten.
- (3) Öffnen Sie einen Webbrowser.
- (4) Geben Sie `http://192.168.0.251` in das Adressfeld des Webbrowsers ein.
- (5) Sie werden zur Änderung des Administrator-Passworts aufgefordert. Ändern Sie das Login-Passwort.

Sie befinden sich nun im Statusmenü der Konfigurationsoberfläche Ihres Geräts.

4.2.1.2 Bedienelemente


Fenster der Konfigurationsoberfläche

Das Fenster der Konfigurationsoberfläche ist in drei Bereiche geteilt:

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

Kopfleiste

Konfigurationsoberfläche Kopfleiste

Menü	Funktion
	Öffnet die Navigationsleiste, über die Sie Zugriff auf die Menüs zur Konfiguration haben.
HOME	Führt aus jedem Menü auf die Startseite zurück.
Ausloggen	<p>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:</p> <ul style="list-style-type: none"> • Konfiguration speichern, vorherige Konfiguration sichern, dann verlassen: Ihre Änderungen werden gespeichert, aber die zuvor aktive Konfiguration wird so gesichert, so dass Sie ggf. später wieder darauf zurückgreifen können. Erst dann er-

Menü	Funktion
	<p>folgt die Abmeldung vom Gerät.</p> <ul style="list-style-type: none"> • Konfiguration speichern, dann verlassen: Ihre Änderungen werden gespeichert. Dabei wird die zuvor aktive Konfiguration ersetzt. Erst dann erfolgt die Abmeldung vom Gerät. • Ohne zu speichern verlassen: Ihre Änderungen sind zwar aktiv, werden aber nicht gespeichert. Nach einem Neustart sind wieder die zuvor gültigen Einstellungen aktiv.
	<p>Online-Hilfe: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Eine Beschreibung des Untermenüs mit den wichtigsten Informationen zu den verfügbaren Optionen wird angezeigt.</p>
<div style="background-color: #800040; color: white; padding: 5px; text-align: center;">SPRACHE</div> <div style="padding: 5px;">English</div> <div style="padding: 5px; background-color: #f0f0f0;">Deutsch</div>	<p>Sprache: Wählen Sie in dem Aufklappmenü die gewünschte Sprache aus, in der die Konfigurationsoberfläche angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen <i>Deutsch</i> und <i>English</i>. Der Standardwert ist <i>Deutsch</i>.</p>
<div style="background-color: #800040; color: white; padding: 5px; text-align: center;">ANSICHT</div> <div style="padding: 5px;">Schnellstart</div> <div style="padding: 5px;">Benutzer</div> <div style="padding: 5px;">Experte</div> <div style="padding: 5px; background-color: #f0f0f0;">Vollzugriff</div>	<p>Ansicht: Wählen Sie in dem Aufklappmenü die gewünschte Ansicht aus. Zur Auswahl stehen <i>Benutzer</i>, <i>Experte</i> und <i>Vollzugriff</i>. Auch den Schnellstart können Sie von hier aus erneut aufrufen.</p> <p>In der Benutzer-Ansicht sind nur die wichtigsten Assistenten und Menüs aufrufbar. Diese reichen, um das Gerät in Betrieb zu nehmen und die am häufigsten benötigten Funktionen zu konfigurieren. Die Zugriffsstufen Experte und Vollzugriff fügen jeweils zusätzliche Menüs hinzu, die jedoch weitergehende Kenntnisse voraussetzen.</p>
<div style="background-color: #800040; color: white; padding: 5px; text-align: center;">KONFIGURATION SPEICHERN</div>	<p>Die Schaltfläche Konfiguration speichern.</p> <p>Wenn Sie Änderungen an der Konfiguration vorgenommen haben, können Sie diese auf zwei Arten speichern:</p> <ul style="list-style-type: none"> • Konfiguration speichern - Ihre Änderungen werden in die ak-

Menü	Funktion
	<p>tuelle Startkonfiguration (die Konfiguration, mit der Ihr Gerät nach jedem Start aktiv wird) übernommen und gespeichert. Die zuvor aktive Konfiguration wird dabei ersetzt.</p> <ul style="list-style-type: none"> • Konfiguration speichern und vorhergehende Boot-Konfiguration sichern: Ihre Änderungen werden wie oben gespeichert, aber die zuvor aktive Konfiguration wird so gesichert, so dass Sie ggf. später wieder darauf zurückgreifen können. Es kann immer nur eine Sicherungsdatei erzeugt werden.

Navigationsleiste

Die Navigationsleiste enthält die Hauptkonfigurationsmenüs und deren Untermenüs. Klicken Sie auf das gewünschte Hauptmenü. Es öffnet sich das jeweilige Untermenü. Wenn Sie auf das gewünschte Untermenü gehen, wird der gewählte Eintrag farbig unterlegt angezeigt. Nach der Wahl des Untermenüs wird die Navigationsleiste geschlossen.

Hauptkonfigurationsfenster



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

Konfigurationselemente







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





Schaltflächen

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

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

Symbole

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

Symbol	Funktion
	ner Verbindung.
	Kennzeichnet, dass der Datenverkehr verschlüsselt wird.
	Löst einen WLAN-Bandscan aus.
	Zeigt die nächste Seite einer Liste an.
	Zeigt die vorherige Seite einer Liste an.

Listenoptionen

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

Auf der **Statusseite** können Sie über den Button  die Option **Automatisches Aktualisierungsintervall** öffnen.




Klicken Sie auf **Automatisches Aktualisierungsintervall**.

Geben Sie die Zeit in Sekunden ein und klicken Sie auf **ÜBERNEHMEN**.

Struktur der Konfigurationsmenüs




Die Menüs enthalten folgende Grundstrukturen:



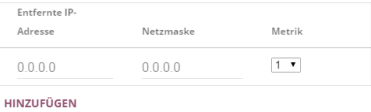

Menüstruktur

Menü	Funktion
Basis-Konfigurationsmenü / Liste	Bei Auswahl eines Menüs der Navigationsleiste wird zunächst das Menü mit den Basisparametern angezeigt. Bei einem Untermenü mit mehreren Seiten wird jeweils das Menü mit den Basisparametern der ersten Seite angezeigt. 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 Einträge angezeigt wird. Klicken Sie diese Schaltfläche, um das Konfigurationsmenü für das Anlegen eines neuen Listeneintrags aufzurufen.
Untermenü 	Klicken Sie auf diese Schaltfläche, um den bestehenden Listeneintrag zu bearbeiten. Sie gelangen in das Konfigurationsmenü.
Menü 	Klicken Sie auf diesen Reiter, um erweiterte Konfigurationsoptionen anzuzeigen.

Für die Konfiguration stehen folgende Optionen zur Verfügung:

Konfigurationselemente

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

Menü	Funktion
	Wählen Sie die entsprechende Option aus.
Checkbox	z. B. Aktivieren durch Auswahl der Checkbox 
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 statt dessen grau dargestellt und sind nicht auswählbar.



Wichtig

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

4.2.1.3 Menüs

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

**Hinweis**

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

Kapitel 5 Assistenten

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

- **Ersteinrichtung Telekom**
- **Erste Schritte**
- **Internet**
- **WLAN**
- **VoIP PBX im LAN**
- **Telefonie**
- **VPN**
- **SWYX**

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

Kapitel 6 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.

6.1 Status

Wenn Sie sich in die Konfigurationsoberfläche einloggen, gelangen Sie auf die Status-Seite in der Ansicht **Benutzer**.

Auf der Status-Seite finden Sie Links zu den Konfigurations-Assistenten, die Ihnen eine einfache Konfiguration der wichtigsten Einstellungen ermöglichen.

Außerdem können Sie hier eine **Systemsoftware-Aktualisierung** durchführen. Klicken Sie auf die Schaltfläche **Aktualisierung**, um den Vorgang zu starten.



Hinweis

Unterbrechen Sie weder die Internetverbindung noch die Stromversorgung.

Nach der Installation einer neuen Systemsoftware müssen Sie das System neu starten.

Auf der Status-Seite in der Ansicht **Vollzugriff** und **Experte** Ihres Geräts, werden die wichtigsten System-Informationen angezeigt.

Sie erhalten einen Überblick über folgende Daten:

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

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

Felder im Menü Systeminformationen

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

Felder im Menü Ressourceninformationen

Feld	Wert
CPU-Nutzung	Zeigt die CPU-Auslastung in Prozent an.
Arbeitsspeichernutzung	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtarbeitsspeicher in MByte an. Die Auslastung wird außerdem in Klammern in Prozent angezeigt.
Interner Speicher	Zeigt den Status eines internen Speichers und die Speichergröße in GByte oder MByte an.
ISDN Verwendung Intern	Zeigt die Anzahl der aktiven B-Kanäle und die maximale Anzahl an zur Verfügung stehenden B-Kanäle für interne Verbindungen.
Aktive Sitzungen (SIF, RTP, etc...)	Zeigt die Summe aller SIF, TDRS und IP-Lastverteilung Sessions an.

Feld	Wert
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Felder im Menü Module

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

Felder im Menü SIP-Provider

Feld	Wert
Nr.	Zeigt die laufende Nummer des SIP-Providers (Ihres IP-Telefonie-Anbieters) an.
Beschreibung	Zeigt die Beschreibung des SIP-Providers an, die bei dessen Einrichtung eingegeben wurde.
Registrar	Zeigt an, an welchem Server sich Ihr Gerät anmeldet, um IP-Telefongespäche zu ermöglichen.
Anschlussart	Zeigt an, ob es sich um einen Mehrgeräte- oder einen Anlagenanschluss handelt.
Status	Zeigt den aktuellen Status der Verbindung zu diesem SIP-Provider an.

Felder im Menü Physikalische Schnittstellen

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

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.

6.2 Globale Einstellungen

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

6.2.1 System

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

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.
Maximale Anzahl der Syslog-Protokolleinträge	Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen. Mögliche Werte sind 0 bis 1000. Der Standardwert ist 50. Sie können die gespeicherten Meldungen in Monitoring -> Internes Protokoll anzeigen lassen.
Maximales Nachrichtenlevel von Systemprotokolleinträgen	Wählen Sie die Priorität der Systemmeldungen aus, ab der protokolliert werden soll. Nur Systemmeldungen mit gleicher oder höherer Priorität als

Feld	Wert
	<p>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>Information</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>Der Standardwert ist <i>20</i>.</p>
<p>Kommunikation mit dem Cloud NetManager</p>	<p>Nur für Geräte, die eine Verwaltung durch den Cloud NetManager unterstützen.</p> <p>Aktivieren oder deaktivieren Sie die Option Kommunikation mit dem Cloud NetManager.</p> <p>Im Auslieferungszustand ist die Option <i>Aktiviert</i>.</p>
<p>IP-Adresse des Cloud NetManagers</p>	<p>Nur für Geräte, die eine Verwaltung durch den Cloud NetManager unterstützen.</p>

Feld	Wert
	Hier ist die Adresse des bintec elmeg Cloud NetManagers bereits vorkonfiguriert. Sollten Sie einen eigenen Manager betreiben wollen, müssen Sie hier die Adresse Ihres Servers eintragen.
LED-Modus	Nur für WLAN-Geräte Wählen Sie das Leuchtverhalten der LEDs. Mögliche Werte: <ul style="list-style-type: none"> • <i>Status</i> (Standardwert): Die LEDs zeigen ihr Standardverhalten. • <i>Blinkend</i>: Nur die Status-LED blinkt einmal in der Sekunde. • <i>Aus</i>: Alle LEDs sind deaktiviert.
Manuelle IP-Adresse des WLAN-Controller	Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar. Geben Sie die IP-Adresse des WLAN-Controllers an. Der Wert kann nur verändert werden, wenn die WLAN-Controller-Funktion aktiviert ist.
Herstellernamen anzeigen	Hier können Sie die Anzeige des Herstellers in der MAC-Adresse ein- oder ausschalten. Für den Herstellernamen (meist eine Abkürzung desselben) werden bis zu acht Zeichen am Anfang der MAC-Adresse verwendet. Statt <code>00:a0:f9:37:12:c9</code> wird mit Herstelleranzeige zum Beispiel <code>BintecCo_37:12:c9</code> angezeigt.

Felder im Menü Energieeinstellungen (nur für Geräte mit GPS)

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

6.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.



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.
SNMP Write Community	Geben Sie das Passwort für den Benutzernamen <code>write</code> ein.

Feld im Menü Globale Passwortoptionen

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

Feld	Wert
	<p>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>

6.2.3 Datum und Uhrzeit

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

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

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	Nur für Geräte mit ISDN-Schnittstelle.

Feld	Beschreibung
	<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 Domänennamen 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.
Zweiter Zeitserver	<p>Geben Sie den zweiten Zeitserver an, entweder mit Domänennamen 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

Feld	Beschreibung
	<p>über TCP-Port 37.</p> <ul style="list-style-type: none"> • <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 Minuten versucht, den Zeitserver zu erreichen. • <i>Aggressiv</i>: Zehn Minuten lang wird versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • <i>Endlos</i>: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver zuerst nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. <p>Bei der Verwendung von Zertifikaten für die Verschlüsselung des Datenverkehrs in einem VPN ist es von zentraler Bedeu-</p>

Feld	Beschreibung
	tung, dass auf dem Gerät die korrekte Zeit eingestellt ist. Um dies sicherzustellen, wählen Sie für Zeitaktualisierungsrichtlinie den Wert <i>Endlos</i> .
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>

6.2.4 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 **Std. Lizenzen** (Standardlizenzen).

6.2.4.1 Bearbeiten oder Neu

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

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.

6.3 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 Bridge-Links setzt sich aus den folgenden Bestandteilen zusammen:

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

Beispiel: *wds1-0* (erster 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)

6.3.1 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 be-

trieben.

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

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschreibung	Zeigt den Namen der Schnittstelle an.
Modus / Bridge-Gruppe	Wählen Sie aus, ob Sie die Schnittstelle im <i>Routing-Modus</i> betreiben möchten oder ordnen Sie die Schnittstelle einer bestehenden (<i>br0, br1</i> usw.) oder neuen Bridge-Gruppe (<i>Neue Bridge-Gruppe</i>) zu. Bei Auswahl von <i>Neue Bridge-Gruppe</i> wird nach Anklicken des OK -Buttons automatisch eine neue Bridge-Gruppe erzeugt.
Konfigurationsschnittstelle	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.

6.3.1.1 Hinzufügen


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

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

Felder im Menü Schnittstellen

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


Bearbeiten für Geräte der Wxxxxn und RS-Serie

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

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-

Feld	Wert
	<p>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.</p> <ul style="list-style-type: none"> • <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.
<p>Wildcard-MAC-Adresse</p>	<p>Nur für Wildcard-Modus = <i>statisch</i></p> <p>Geben Sie die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist.</p>
<p>Transparente MAC-Adresse</p>	<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 zum Access Point herzustellen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

6.4 Administrativer Zugriff

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

**Hinweis**

Beachten Sie, dass manche Optionen wie SSH, Telnet, SNMP und ISDN-Login für die be.IP nicht zur Verfügung stehen.

6.4.1 Zugriff

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

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

**Hinweis**


Nicht alle Optionen sind für alle bintec elmeg-Geräte verfügbar. Informieren Sie sich im Datenblatt Ihres Geräts, welche Verbindungstypen unterstützt werden!

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

Service Login (ISDN Web-Access) ist standardmäßig nicht aktiv.

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

Felder im Menü Erweiterte Einstellungen

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

6.4.1.1 Hinzufügen

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

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.

6.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

6.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete


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

Pakettypen

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

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

6.5.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Wert
Authentifizierungstyp	<p>Wählen Sie aus, wofür der RADIUS-Server verwendet werden soll.</p> <p>Mögliche Werte:</p> <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 kontrollieren. • <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.

Feld	Wert
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>Der Standardwert ist 0.</p> <p>Siehe auch Richtlinie in den erweiterten Einstellungen.</p>
Eintrag aktiv	<p>Wählen Sie aus, ob der in diesem Eintrag konfigurierte RADIUS-Server verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Gruppenbeschreibung	<p>Definieren Sie eine neue RADIUS-Gruppenbeschreibung bzw. weisen Sie den neuen RADIUS-Eintrag einer schon definierten Gruppe zu. Die konfigurierten RADIUS-Server einer Gruppe werden gemäß der Priorität und der Richtlinie abgefragt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neu</i> (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein. • <i>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	Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negati-

Feld	Wert
	<p>ve 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 Gebührenerfassung (1646 in älteren RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist.</p> <p>Der 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>Der 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>

Feld	Wert
	<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 0 und 10.</p> <p>Der Standardwert ist 1. Um zu verhindern, dass Status auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf 0.</p>
RADIUS-Dialout	<p>Nur für Authentifizierungstyp = <i>PPP-Authentifizierung</i> und <i>IPSec-Authentifizierung</i>.</p> <p>Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiv ist, können Sie folgende 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 0 eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>

6.5.2 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.

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, <i>Outband (CLID)</i> deaktiviert.</p>



6.6 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.

6.6.1 Zugriffsprofile

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

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

6.6.1.1 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.

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 Zugriffsprofil. Diese kann nicht editiert werden.


Felder im Menü Schaltflächen

Feld	Beschreibung
Konfiguration speichern	Wenn Sie die Schaltfläche Konfiguration speichern aktivieren, darf der Benutzer Konfigurationen speichern.










Hinweis

Beachten Sie, dass die Passwörter in der gespeicherten Datei im Klartext eingesehen werden können.


Feld	Beschreibung
	<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; background-color: #f0f0f0; padding: 10px;"> <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> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

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>







Feld	Beschreibung
	<p>Jedes Element in der Navigationsleiste kann drei Werte annehmen. Klicken Sie in der gewünschten Zeile auf das Symbol , um diese drei Werte anzuzeigen 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>

6.6.2 Benutzer


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

Es sind keine Benutzer vorkonfiguriert.

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

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.

6.6.2.1 Bearbeiten oder Neu

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

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 beliebige 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>

6.7 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 Sprachverbindungen über Voice over IP ausgestattet.

6.7.1 Zertifikatsliste

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

6.7.1.1 Bearbeiten

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

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 = wahr</p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Einstellungen:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i>: keine Überprüfung von CRLs. • <i>Immer</i>: CRLs werden grundsätzlich überprüft. • <i>Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist (Standardwert)</i>: Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden. • <i>Einstellungen des übergeordneten Zertifikates benutzen</i>: Es werden die Einstellungen des übergeordneten

Feld	Beschreibung
	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	<p>Legen Sie fest, dass dieses Zertifikat ohne weitere Überprüfung bei der Authentifizierung als Benutzerzertifikat akzeptiert werden soll.</p> <p>Mit <i>wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>



Achtung

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

6.7.1.2 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.

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 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. • <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.</p>

Feld	Beschreibung
	<p>http://scep.beispiel.com:8080/scep/scep.dll</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. 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"> • <i><Name eines vorhandenen Zertifikats></i>: 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>Der 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 Kommunika-</p>

Feld	Beschreibung
	<p>tion mit der RA verwenden, haben Sie hier die Möglichkeit, ein weiteres zur Verschlüsselung der Kommunikation auszuwählen.</p> <p>Der Standardwert ist <code>-- RA-Signierungszertifikat verwenden --</code>, 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 Subjektnamen

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>

Feld	Beschreibung
	Geben Sie die E-Mail-Adresse laut CA ein.
Organisationseinheit	Nur für Benutzerdefiniert = deaktiviert. Geben Sie die Organisationseinheit laut CA ein.
Organisation	Nur für Benutzerdefiniert = deaktiviert. Geben Sie die Organisation laut CA ein.
Ort	Nur für Benutzerdefiniert = deaktiviert. Geben Sie den Standort laut CA ein.
Staat/Provinz	Nur für Benutzerdefiniert = deaktiviert. Geben Sie den Staat/das Bundesland laut CA ein.
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	<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>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

6.7.1.3 Importieren

Wählen Sie die Schaltfläche **Importieren**, um Zertifikate zu 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	<p>Wählen Sie die Art der Kodierung, so dass Ihr Gerät das Zertifikat dekodieren kann.</p> <p>Mögliche Werte:</p> <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

Feld	Beschreibung
	möglicherweise ein Passwort. Tragen Sie das Passwort hier ein.

6.7.2 CRLs

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

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

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

6.7.2.1 Importieren

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

Feld	Beschreibung
	versuchen Sie es mit einer bestimmten Kodierung. <ul style="list-style-type: none"> • <i>Base64</i> • <i>Binär</i>
Passwort	Geben Sie das zum Importieren zu verwendende Passwort ein.

6.7.3 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.

6.7.3.1 Neu

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

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 7 Physikalische Schnittstellen

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

7.1 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** *192.168.0.251* und **Netzmaske** *255.255.255.0* vorkonfiguriert.

Der Port **ETH5** 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

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

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.

7.1.1 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.

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

Felder im Menü Switch-Konfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Ethernet-Schnittstellenauswahl	Ordnen Sie dem jeweiligen Switch-Port eine logische Ethernet-Schnittstelle zu. Zur Auswahl stehen 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>

Feld	Beschreibung
	, Switch Port 5 die Schnittstelle <i>en1-4</i> zugeordnet.
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 (Standardwert)</i> • <i>Auto 1000 Mbit/s only</i> • <i>Auto 100 Mbit/s only</i> • <i>Auto 10 Mbit/s only</i> • <i>Auto 100 Mbit/s / Full Duplex</i> • <i>Auto 100 Mbit/s / Half Duplex</i> • <i>Auto 10 Mbit/s / Full Duplex</i> • <i>Auto 10 Mbit/s / Half Duplex</i> • <i>Fest 1000 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Half Duplex</i> • <i>Fest 10 Mbit/s / Full Duplex</i> • <i>Fest 10 Mbit/s / Half Duplex</i> • <i>Keiner</i>: Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	<p>Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>1000 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Half Duplex</i> • <i>10 Mbit/s / Full Duplex</i> • <i>10 Mbit/s / Half Duplex</i> • <i>Inaktiv</i>
Flusskontrolle	<p>Wählen Sie aus, ob auf der entsprechenden Schnittstelle eine Flusskontrolle vorgenommen werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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.

7.2 ISDN-Ports

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

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

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

7.2.1 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.

7.2.1.1 Bearbeiten

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

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

Felder im Menü **Basisparameter**

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Automatische Konfiguration beim Start	Wählen Sie aus, ob der ISDN Switch Typ (D-Kanalerkennung für Wählverbindungen) automatisch erkannt werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Port-Verwendung	Nur wenn Automatische Konfiguration beim Start deaktiviert ist. Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Nicht verwendet</i>: Der ISDN-Anschluss wird nicht genutzt. • <i>Dialup (Euro-ISDN)</i> • <i>Standleitung</i> • <i>Q-SIG</i>
ISDN-Konfigurationstyp	Nur wenn Automatische Konfiguration beim Start deaktiviert ist und für Port-Verwendung = <i>Dialup (Euro-ISDN)</i> oder <i>Q-SIG</i> Wählen Sie die ISDN-Anschlussart aus. Mögliche Werte: <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)	Wählen Sie aus, ob Sie X.31 (X.25 im D-Kanal) z. B. für CAPI-Applikationen nutzen wollen. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
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>

7.2.2 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 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 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.

7.2.2.1 Neu

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

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	<p>Wählen Sie den Dienst aus, dem ein Ruf auf die untenstehende MSN zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>ISDN-Login</i> (Standardwert): Ermöglicht Einloggen mit <i>ISDN-Login</i>. • <i>PPP (Routing)</i>: Standardeinstellung für PPP-Routing. Enthält die automatische Erkennung der unten genannten PPP-Verbindungen außer <i>PPP DOVB</i>. • <i>IPSec</i>: Ermöglicht die Festlegung einer Rufnummer für IP-Sec-Callback. • <i>Andere (PPP)</i>: Weitere Dienste können ausgewählt werden: <i>PPP 64k</i> (Ermöglicht 64 kBit/s PPP-Datenverbindungen), <i>PPP 56k</i> (Ermöglicht 56 kBit/s PPP-Datenverbindungen), <i>PPP V.110 (9600) PPP V.110 (14400)</i>, <i>PPP V.110 (19200)</i>, <i>PPP V.110 (38400)</i> (Ermöglicht PPP-Verbindungen mit V.110 und mit Bit-Raten von 9600 Bit/s, 14400 Bit/s, 19200 Bit/s, 38400 Bit/s), <i>PPP V.120</i> (Ermöglicht eingehende PPP-Verbindungen mit V.120).
MSN	Geben Sie die Rufnummer ein, die zur Überprüfung der Called Party Number verwendet wird, wobei zur Rufannahme eine Übereinstimmung einzelner Ziffern im Eintrag unter Berücksichtigung der Konfiguration in MSN-Erkennung genügt.
MSN-Erkennung	<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)

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

7.3 DSL-Modem

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

7.3.1 DSL-Konfiguration

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

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 DSL-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>

Felder im Menü Aktuelle Leitungsgeschwindigkeit

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

Felder im Menü DSL Parameter

Feld	Beschreibung
DSL-Modus	<p>Wählen Sie den DSL-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>: Die ADSL-Schnittstelle ist nicht aktiv. • <i>ADSL1</i>: ADSL1 / G.DMT wird angewendet. • <i>Automatischer Modus (ADSL)</i> (Standardwert): Der ADSL-Modus wird dem der Gegenstelle automatisch angepasst. • <i>ADSL2</i>: ADSL2 / G.992.3 wird angewendet. • <i>ADSL2 Plus</i>: ADSL2 Plus / G.992.5 wird angewendet.
Transmit Shaping	<p>Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DS-</p>

Feld	Beschreibung
	<p>LAMs notwendig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (<i>Leitungsgeschwindigkeit</i>) (Standardwert): Die Datenrate in Senderichtung wird nicht reduziert. • <i>128.000 bit/s bis 2.048.000 bit/s</i>: Die Datenrate in Senderichtung wird in festgesetzten Schritten reduziert auf maximal 128.000 bit/s bis 2.048.000 bit/s. • <i>Benutzerdefiniert</i>: Die Datenrate wird reduziert auf den in Maximale Upstream-Bandbreite eingegebenen Wert.
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>Nur für Geräte mit VDSL-Modem</p> <p>Wählen Sie das Leitungsprofil Ihres Internet-Service-Providers. Ist Ihr Provider nicht in der Auswahlliste aufgeführt, verwenden Sie das Profil <i>Standard</i>.</p>

7.4 UMTS/LTE

7.4.1 UMTS/LTE

Im Menü **UMTS/LTE** konfigurieren Sie die Anbindung des integrierten UMTS/HSD-PA/LTE-Modems (je nach Ausstattung Ihres Geräts) oder eines optional steckbaren UMTS/LTE-USB-Sticks.

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.

7.4.1.1 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.

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. Mit <i>Aktiviert</i> wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
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> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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 ausreichender Signalstärke und Signalqualität von LTE wird GPRS verwendet..

Feld	Beschreibung
	<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="539 635 1319 1120" style="border: 1px solid #ccc; background-color: #f0f0f0; 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 zugewiesen. • <i>IPSec</i>: Der Ruf erfolgt über IPSec.

Feld	Beschreibung
	<p>Beachten Sie für die Einstellung Eingehender Dienstyp <i>IP-sec</i> Folgendes:</p> <p>IPSec-Callback wird dazu verwendet, einen IPSec-Peer zu veranlassen, eine Internetverbindung aufzubauen, um so einen IPSec-Tunnel über das Internet zu ermöglichen. Mit Hilfe eines direkten Anrufs über das UMTS/LTE-Mobilfunknetz kann dem Peer signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den Anruf über Mobilfunk veranlasst, eine Verbindung aufzubauen.</p> <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 1274 1320 1431" style="border: 1px solid gray; padding: 5px;"> <p> Hinweis</p> <p>Die Eingabe einer falschen PIN unterbindet die Kommunikation bis der Eintrag korrigiert wird.</p> </div>

Feld	Beschreibung
	<div data-bbox="539 211 1315 433" style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px;">  <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>
Fallback-Nummer	<p>Nur für UMTS/LTE-Status = <i>Aktiviert</i></p> <p>Tragen Sie die Rufnummer für die Funktion GSM Fallback ein.</p> <p>Wenn ein Sprachruf auf diese Nummer eingeht, wird eine ggf. aktive Verbindung sofort getrennt und der Betriebsmodus des Modems auf GSM zurückgesetzt, in welchem das Modem so lange bleibt, bis wieder ein Datenruf (PPP, ISDN-Login, IPSec-Callback) erfolgt. Ist für die WAN-Verbindung der Flatrate-Modus aktiviert (Option Immer aktiv aktiviert in WAN->Internet + Einwählen->UMTS/LTE-> ), führt dies zu sofortigem Verbindungswiederaufbau.</p> <div data-bbox="539 924 1315 1111" style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px;">  <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>
APN (Access Point Name)	<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 26201.

Felder im Menü Geschlossene Benutzergruppe

Feld	Beschreibung
Authentifizierungs-APN	Tragen Sie hier den Authentifizierungs Access Point Namen für die Geschlossene Benutzergruppe ein, den Sie von Ihrem Provider erhalten haben.
Authentifizierungsmethode	Wählen Sie das Authentifizierungsprotokoll für die Geschlossene Benutzergruppe aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: <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.

Werte in der Liste Status des Mobilgerätes

Feld	Beschreibung
Gerät	Zeigt die Bezeichnung des internen Modemanschlusses an.
Modemmodell	Zeigt die Bezeichnung des Modems an.

Feld	Beschreibung
IMEI	Die IMEI (International Mobile Station Equipment Identity) zeigt die 15-stellige Sereinnummer 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 PLNM angezeigt.
Aktuelles Netzwerk	Zeigt an, welches Netz aktuell verwendet wird (z. B. UMTS oder GSM).
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 8 LAN


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

8.1 IP-Konfiguration

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



8.1.1 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.

Durch Klicken auf die -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert.

Über die -Schaltfläche können Sie die Details einer vorhandenen Schnittstelle anzeigen lassen.



Hinweis

Beachten Sie bei IPv4:

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

IPv6-Adressen konfigurieren

Zusätzlich zu IPv4-Adressen können Sie IPv6-Adressen verwenden.

Im Folgenden sehen Sie ein Beispiel für eine IPv6-Adresse:

Ihr Gerät kann auf einer Schnittstelle entweder als Router oder als Host agieren. In der Regel agiert es auf den LAN-Schnittstellen als Router und auf den WAN- sowie den PPP-Verbindungen als Host.

Wenn Ihr Gerät als Router agiert, so können seine eigenen IPv6-Adressen folgendermaßen gebildet werden: ein Link-Präfix kann von einem Allgemeinen Präfix abgeleitet werden oder Sie können einen statischen Wert eingeben. Eine Host-Adresse kann über *Auto eui-64* erzeugt werden, für weitere Host-Adressen können Sie statische Werte eingeben.


Wenn Ihr Gerät als Router agiert, so verteilt es den konfigurierten Link-Präfix in der Regel per Router Advertisements an die Hosts. Über einen DHCP-Server werden Zusatzinformationen, wie z. B. die Adresse eines Zeitservers, an die Hosts übermittelt. Der Client kann sich seine Host-Adresse entweder über Stateless Address Autoconfiguration (SLAAC) erzeugen oder diese Adresse von einem DHCP-Server zugeteilt bekommen.

Verwenden Sie für den oben beschriebenen Router-Modus im Menü **LAN->IP-Konfiguration->Schnittstellen->Neu** die Einstellungen **IPv6-Modus = Router**, **Router Advertisement übertragen *Aktiviert*** **DHCP-Server *Aktiviert*** und **IPv6-Adressen Hinzufügen**.

Wenn Ihr Gerät als Host agiert, wird ihm ein Link-Präfix von einem anderen Router per

Router Advertisement zugeteilt. Die Host- Adresse wird dann per SLAAC automatisch erzeugt. Zusatzinformationen, wie z. B. der Allgemeine Präfix vom Provider oder die Adresse eines Zeitservers können per DHCP bezogen werden. Verwenden Sie dazu im Menü **LAN->IP-Konfiguration->Schnittstellen->Neu** die Einstellungen **IPv6-Modus** = *Client*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** = *Aktiviert*.

8.1.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	<p>Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird.</p> <p>Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.</p>
Schnittstellenmodus	<p>Nur bei physikalischen Schnittstellen im Routing-Modus 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>
VLAN-ID	<p>Nur für Schnittstellenmodus = <i>Tagged (VLAN)</i></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>

Feld	Beschreibung
	Mögliche Werte sind 1 (Standardwert) bis 4094.
MAC-Adresse	<p>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).</p> <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>

Felder im Menü Grundlegende IPv4-Parameter

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 283 konfigurieren.</p>
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-

Feld	Beschreibung
	Adresse.
IP-Adresse / Netzmaske	Nur für Adressmodus = <i>Statisch</i> Fügen Sie mit Hinzufügen einen neuen Adresseintrag hinzu und geben Sie die IP-Adresse und die entsprechende Netzmaske der virtuellen Schnittstelle ein.

Felder im Menü Grundlegende IPv6-Parameter

Feld	Beschreibung
IPv6	Wählen Sie aus, ob die gewählte Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	Hier nur für IPv6 = <i>Aktiviert</i> Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen. • <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen. Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 283 konfigurieren.
IPv6-Modus	Nur für IPv6 = <i>Aktiviert</i> Wählen Sie, ob die Schnittstelle im Host- oder im Router-Modus

Feld	Beschreibung
	<p>betrieben werden soll. Abhängig von der getroffenen Auswahl werden unterschiedliche Parameter angezeigt, die Sie konfigurieren müssen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Router (Router-Advertisement übermitteln)</i> (Standardwert): Die Schnittstelle wird im Router-Modus betrieben. • <i>Host</i>: Die Schnittstelle wird im Host-Modus betrieben.
<p>Router Advertisement übertragen</p>	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Router (Router-Advertisement übermitteln)</p> <p>Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle gesendet werden sollen.</p> <p>Mithilfe der Router Advertisements wird z.B. die Präfix Liste übertragen und der Router propagiert sich als Standard-Gateway.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>DHCP-Server</p>	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Router (Router-Advertisement übermitteln)</p> <p>Legen Sie fest, ob Ihr Gerät als DHCP-Server agieren soll, d.h. ob es DHCP-Options versenden soll, um z. B. Informationen zu den DNS-Servern an die Clients weiterzuleiten.</p> <p>Aktivieren Sie diese Option, wenn Hosts IPv6-Adressen per SLAAC erzeugen sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>IPv6-Adressen</p>	<p>Nur für IPv6 = Aktiviert</p> <p>Sie können der gewählten Schnittstelle IPv6-Adressen zuordnen.</p> <p>Mit Hinzufügen können Sie einen oder mehrere Adresseinträge</p>

Feld	Beschreibung
	<p>anlegen.</p> <p>Ein zusätzliches Fenster öffnet sich, in dem Sie eine IPv6-Adresse bestehend aus einem Link-Präfix und einem Host-Anteil festlegen können.</p> <p>Wenn Ihr Gerät im Host-Modus arbeitet (IPv6-Modus = Host, Router Advertisement annehmen <i>Aktiviert</i> und DHCP-Client <i>Aktiviert</i>), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen.</p> <p>Wenn Ihr Gerät im Router-Modus arbeitet (IPv6-Modus = Router (<i>Router-Advertisement übermitteln</i>), Router Advertisement übertragen <i>Aktiviert</i> und DHCP-Server <i>Aktiviert</i>), so müssen Sie hier seine IPv6-Adressen konfigurieren.</p>
Router Advertisement annehmen	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Host</p> <p>Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle empfangen werden sollen. Mithilfe der Router Advertisements wird z. B. die Präfix-Liste erstellt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
DHCP-Client	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Host</p> <p>Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll, d.h. ob es DHCP-Options empfangen soll, um z. B. Informationen zu den DNS-Servern zu erhalten.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü Basisparameter

Feld	Beschreibung
Ankündigen	Nur für IPv6-Modus = Router (<i>Router-Advertisement</i>

Feld	Beschreibung
	<p><i>übermitteln</i>)</p> <p>Hier können Sie - bezogen auf den Link-Präfix, der im aktuellen Fenster definiert wird - festlegen, ob dieser Präfix per Router Advertisement über die gewählte Schnittstelle versendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Link-Präfix

Feld	Beschreibung
Art der Einrichtung	<p>Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Von Allgemeinem Präfix</i> (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet. • <i>Statisch</i>: Sie können den Link-Präfix eingeben.
Allgemeiner Präfix	<p>Nur für Art der Einrichtung = <i>Von Allgemeinem Präfix</i></p> <p>Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes->Neu angelegt sind.</p>
Automatische Subnetzerstellung	<p>Nur wenn Art der Einrichtung = <i>Von Allgemeinem Präfix</i> und wenn ein Allgemeiner Präfix gewählt ist.</p> <p>Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID 0 verwendet, für das zweite Subnetz die Subnetz-ID 1, usw.</p> <p>Mögliche Werte für die Subnetz-ID sind 0 bis 65535.</p> <p>Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix. Bei der Subnetzerstellung wird der dezimale ID-Wert in einen hexadezimalen Wert umgerechnet.</p>

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Wenn die Funktion nicht aktiv ist, so können Sie durch Eingabe der Subnetz-ID ein Subnetz definieren.</p>
Subnetz-ID	<p>Nur wenn Automatische Subnetzerstellung nicht aktiv ist.</p> <p>Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix.</p> <p>Mögliche Werte sind 0 bis 65535.</p> <p>Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.</p>
Link-Präfix	<p>Nur für Art der Einrichtung = <i>Statisch</i></p> <p>Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit <code>::</code> enden. Seine Länge ist mit 64 vorgegeben.</p>

Felder im Menü Host-Adresse


Feld	Beschreibung
Erzeugungsmethode	<p>Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>EUI-64 setzt folgenden Prozess in Gang:</p> <ul style="list-style-type: none"> • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird <i>FFFF</i> eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf 1 gesetzt.

Feld	Beschreibung
Statische Adressen	Sie können, unabhängig von der automatischen Erzeugung, die unter Erzeugungsmethode festgelegt ist, mit Hinzufügen den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit <i>64</i> vorgegeben. Beginnen Sie die Eingabe mit <i>: :</i>

Die Felder im Menü **Erweitert** sind Bestandteil der Präfix-Informationen, die im Router Advertisement gesendet werden, wenn **Ankündigen** aktiv ist. Das Menü **Erweitert** besteht aus folgenden Feldern:

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
On Link Flag	Wählen Sie, ob das On-Link Flag (L-Flag) gesetzt werden soll. Dadurch fügt der Host das Präfix der Präfixliste hinzu. Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Autonomous Flag	Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll. Dadurch nutzt ein Host das Präfix und eine Schnittstellen-ID, um daraus seine Adresse abzuleiten. Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Bevorzugte Gültigkeitsdauer	Geben Sie eine Zeitspanne in Sekunden ein. Während dieser Zeit werden die Adressen, die mit Hilfe des Präfix per SLAAC erzeugt wurden, bevorzugt verwendet. Der Standardwert ist <i>604800</i> Sekunden.
Gültigkeitsdauer	Geben Sie eine Zeitspanne in Sekunden an, für die das Präfix gültig ist. Der Standardwert ist <i>2592000</i> Sekunden.

Feld	Beschreibung
	 <p>Hinweis</p> <p>Der Wert für die Gültigkeitsdauer sollte niedriger sein als derjenige, der unter Erweiterte IPv6-Einstellungen für die Option Router-Gültigkeitsdauer konfiguriert ist.</p>


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

Felder im Menü **Erweiterte IPv4-Einstellungen**

Feld	Beschreibung
DHCP-MAC-Adresse	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Ist Voreingestellte verwenden aktiviert (Standardeinstellung) wird die Hardware-MAC-Adresse der Ethernet-Schnittstelle verwendet. Bei physikalischen Schnittstellen ist die aktuelle MAC-Adresse standardmäßig eingetragen.</p> <p>Wenn Sie Voreingestellte verwenden deaktivieren, geben Sie eine MAC-Adresse für die virtuelle Schnittstelle ein, z. B. <i>00:e1:f9:06:bf:03.</i></p> <p>Manche Provider verwenden hardware-unabhängige MAC-Adressen, um ihren Clients IP-Adressen dynamisch zuzuweisen. Sollte Ihnen Ihr Provider eine MAC-Adresse zugewiesen haben, so tragen Sie diese hier ein.</p>
DHCP-Hostname	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Geben Sie den Hostnamen ein, der vom Provider gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.</p>
DHCP Broadcast Flag	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für definierte Gegenstellen beantworten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-MSS-Clamping	<p>Wählen Sie aus, ob Ihr Gerät das Verfahren MSS Clamping anwenden soll. Um die Fragmentierung von IP-Paketen zu verhindern, wird hierbei vom Gerät automatisch die MSS (Maximum Segment Size) auf den hier einstellbaren Wert verringert.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Bei Aktivierung ist im Eingabefeld der Standardwert <i>1350</i> eingetragen.</p>

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
Router-Gültigkeitsdauer	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router (<i>Router-Advertisement übermitteln</i>) und Router Advertisement übertragen = Aktiviert</p> <p>Geben Sie eine Zeitspanne in Sekunden an. Für dieses Intervall verbleibt der Router in der Default Router List.</p> <p>Der Standardwert ist <i>600</i> Sekunden. Der Maximalwert ist <i>65520</i> Sekunden. Ein Wert von <i>0</i> besagt, dass der Router kein Standardrouter ist und nicht in die Default Router List eingetragen werden soll.</p>
	<p> Hinweis</p> <p>Der Wert für die Router-Gültigkeitsdauer sollte höher sein als die kürzeste Link-Präfix-Gültigkeitsdauer, die im unter Grundlegende IPv6-Parameter für die Schnittstelle konfiguriert ist.</p>
Router-Präferenz	Nur für IPv6 = Aktiviert , IPv6-Modus = Router

Feld	Beschreibung
	<p>(<i>Router-Advertisement übermitteln</i>) und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die Präferenz Ihres Routers für die Wahl des Standardrouters. Dies ist in Fällen nützlich, in denen ein Knoten Advertisements von mehreren Routern erhält oder in Back-Up-Szenarien.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hoch</i> • <i>Mittel</i> (Standardwert) • <i>Niedrig</i>
DHCP-Modus	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router (<i>Router-Advertisement übermitteln</i>) und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus.</p>
	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;">  <p>Hinweis</p> <p>Der Router muss nicht als DHCP-Server eingerichtet sein.</p> </div> <p>Mit Auswahl von <i>Andere - DNS-Server, SIP-Server</i> (Standardwert) werden nicht-adressbezogene Informationen, wie z. B. DNS, VoIP, usw. durchgeleitet.</p> <p>Aktivieren Sie diese Option, wenn die Hosts im Netzwerk ihre IP-Adresse über SLAAC automatisch bilden sollen. Der Router sendet in diesem Fall ausschließlich nicht-adressbezogene Daten über DHCP.</p> <p>Mit Auswahl von <i>Verwaltet - IPv6-Adressverwaltung</i> werden sowohl die IPv6-Adressen als auch alle nicht adressbezogenen Daten vom Host per DHCP bezogen.</p>
DNS-Propagation	<p>Nur für IPv6-Modus = Router (<i>Router-Advertisement übermitteln</i>) und Router Advertisement übertragen Aktiviert</p>

Feld	Beschreibung
	<p>Wählen Sie aus, ob DNS-Server-Adressen über Router Advertisements propagiert werden sollen und wenn ja, auf welche Weise. Es werden maximal zwei DNS-Server-Adressen propagiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</i>: Es wird keine DNS-Server-Adresse propagiert. • <i>Selbst</i>: Die eigene IP-Adresse wird als DNS-Server-Adresse propagiert. Bei mehreren Adressen, werden die Adressen in folgender Reihenfolge propagiert: <ul style="list-style-type: none"> • Globale Adressen • ULA (Unique Local Addresses) • Link-Lokale-Adressen • <i>Sonstige</i>: Die statisch konfigurierten und die dynamisch gelernten DNS-Server-Einträge werden gemäß ihrer Priorität propagiert. Sind keine Einträge vorhanden, werden keine Adressen propagiert.

8.2 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.

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**.

8.2.1 VLANs


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

8.2.1.1 Bearbeiten oder Neu

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

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

Felder im Menü VLAN konfigurieren

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

8.2.2 Portkonfiguration

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

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.

8.2.3 Verwaltung

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

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

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

Feld	Beschreibung
VLAN aktivieren	Aktivieren oder deaktivieren Sie die spezifizierte Bridge-Gruppe für VLAN. Mit <i>Aktiviert</i> wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion deaktiviert.
Verwaltungs-VID	Wählen Sie die VLAN-ID des VLANs aus, in dem Ihr Gerät arbeiten soll.

Kapitel 9 Wireless LAN Controller

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

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

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

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

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

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

9.1 Wizard

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

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



Hinweis

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

9.1.1 Grundeinstellungen

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

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

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

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

Schnittstelle

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

DHCP-Server

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

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

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

Wenn Sie z. B. ein bintec elmeg Gateway als DHCP-Server verwenden wollen, klicken Sie im **GUI** Menü dieses Geräts unter **Lokale Dienste->DHCP-Server->DHCP Pool->Neu->Erweiterte Einstellungen** im Feld **DHCP-Optionen** auf die Schaltfläche **Hinzufügen**. Wählen Sie als **Option** *CAPWAP Controller* und tragen Sie im Feld **Wert** die IP-Adresse des WLAN Controllers ein.

IP-Adressbereich

Wenn die IP-Adressen intern vergeben werden sollen, müssen Sie die Anfangs- und End-IP-Adresse des gewünschten Bereiches eingeben.

Hinweis: Wenn Sie auf **Weiter** klicken, erscheint eine Warnung, dass beim Fortfahren die Wireless-LAN-Controller-Konfiguration überschrieben wird. Mit Klicken auf **OK** sind Sie einverstanden und fahren mit der Konfiguration fort.

9.1.2 Funkmodulprofil

Wählen Sie aus, welches Frequenzband Ihr WLAN Controller verwenden soll.

Mit der Einstellung *2.4 GHz Radio Profile* wird das 2.4-GHz-Frequenzband verwendet.

Mit der Einstellung *5 GHz Radio Profile* wird das 5-GHz-Frequenzband verwendet.


Wenn das entsprechende Gerät zwei Funkmodule enthält, können Sie **Zwei unabhängige Funkmodulprofile verwenden**. Modul 1 wird dadurch das *2.4 GHz Radio Profile* zugeordnet, Modul 2 das *5 GHz Radio Profile*.

Mit Auswahl von *Aktiviert* wird die Funktion aktiv.

Standardmäßig ist die Funktion nicht aktiv.

9.1.3 Drahtlosnetzwerk

In der Liste werden alle konfigurierten Drahtlosnetzwerke (VSS) angezeigt. Es ist mindestens ein Drahtlosnetzwerk (VSS) angelegt. Dieser Eintrag kann nicht gelöscht werden.

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

Mithilfe von -Symbol können Sie Einträge löschen.


Mit **Hinzufügen** können Sie neue Einträge anlegen. Für ein Funkmodul können Sie bis zu acht Drahtlosnetzwerke (VSS) anlegen.



Hinweis

Wenn Sie das standardmäßig angelegte Drahtlosnetzwerk verwenden wollen, müssen Sie mindestens den Parameter **Preshared Key** ändern. Andernfalls erscheint eine Aufforderung.

9.1.3.1 Drahtlosnetzwerke ändern oder hinzufügen

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

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

Folgende Parameter stehen zur Verfügung

Netzwerkname (SSID)

Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.

Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.

Wählen Sie außerdem aus, ob der **Netzwerkname (SSID)** *Sichtbar* übertragen werden soll.

Sicherheitsmodus

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

Hinweis: *WPA-Enterprise* bedeutet 802.11x.

WPA-Modus

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

Preshared Key

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

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



Wichtig

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

RADIUS-Server

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

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

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

EAP-Vorabauthentifizierung

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

VLAN

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

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




Hinweis

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

9.1.4 Automatische Installation starten

Sie sehen eine Liste der gefundenen Access Points.

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

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

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

Standort

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

Zugewiesene Drahtlosnetzwerke (VSS)

Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

Folgende Parameter stehen im Menü Funkmodul 1 zur Verfügung:

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

Betriebsmodus

Wählen Sie den Betriebsmodus des Funkmoduls.

Mögliche Werte:

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

- *Aus*: Das Funkmodul ist nicht aktiv.

Aktives Funkmodulprofil

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

Kanal

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

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



Hinweis

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

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

Sendeleistung

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

Mit **OK** übernehmen Sie die Einstellungen.

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

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



Hinweis

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

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

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

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

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

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

9.2 Controller-Konfiguration

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

9.2.1 Allgemein

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Region	Wählen Sie das Land, in welchem der Wireless LAN Controller

Feld	Beschreibung
	<p>betrieben werden soll.</p> <p>Mögliche Werte sind alle auf dem Wirelessmodul des Geräts vorkonfigurierten Länder.</p> <p>Der Bereich der verwendbaren Kanäle variiert je nach Länder-einstellung.</p> <p>Der Standardwert ist <i>Germany</i>.</p>
Schnittstelle	<p>Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.</p>
DHCP-Server	<p>Wählen Sie aus, ob ein externer DHCP-Server die IP-Adressen an die APs vergeben soll bzw. ob Sie selbst feste IP-Adressen vergeben wollen. Alternativ können Sie Ihr Gerät als DHCP-Server verwenden. Bei diesem internen DHCP-Server ist die CAPWAP Option 138 aktiv, um die Kommunikation zwischen Master und Slaves zu ermöglichen.</p> <p>Hinweis: Stellen Sie bei Nutzung eines externen DHCP-Servers sicher, dass CAPWAP Option 138 aktiv ist.</p> <p>Wenn Sie z. B. ein bintec elmeg Gateway als DHCP-Server verwenden wollen, klicken Sie im GUI Menü dieses Geräts unter Lokale Dienste->DHCP-Server->DHCP Pool->Neu->Erweiterte Einstellungen im Feld DHCP-Optionen auf die Schaltfläche Hinzufügen. Wählen Sie als Option <i>CAPWAP Controller</i> und tragen Sie im Feld Wert die IP-Adresse des WLAN Controllers ein.</p> <p>Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü Systemverwaltung->Globale Einstellungen->System im Feld Manuelle IP-Adresse des WLAN-Controller eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Extern oder statisch</i> (Standardwert): Ein externer DHCP-Server mit aktiver CAPWAP Option 138 vergibt die IP-Adressen an die APs oder Sie vergeben statische IP-Adressen an die APs.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Intern</i>: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.
IP-Adressbereich	<p>Nur für DHCP-Server = <i>Intern</i></p> <p>Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein. Diese IP-Adressen und Ihr Gerät müssen aus demselben Netz stammen.</p>
Slave-AP-Standort	<p>Wählen Sie aus, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal (LAN)</i> (Standardwert) • <i>Entfernt (WAN)</i> <p>Die Einstellung <i>Entfernt (WAN)</i> ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die APs über VPN angebunden sind, kann es vorkommen, dass eine Verbindung unterbrochen wird. In diesem Fall behält der entsprechende AP mit der Einstellung <i>Entfernt (WAN)</i> seine Konfiguration bis die Verbindung wieder hergestellt ist. Danach bootet er und anschließend synchronisieren sich Controller und AP erneut.</p>
Slave-AP-LED-Modus	<p>Wählen Sie das Leuchtverhalten der Slave-AP-LEDs.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Status</i> (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde. • <i>Blinkend</i>: Die LEDs zeigen ihr Standardverhalten. • <i>Aus</i>: Alle LEDs sind deaktiviert.

9.2.2 Slave-AP-Autoprofil

Der Wireless LAN Controller bietet die Möglichkeit, Access Points, die in das ihm zugängliche Netz integriert werden, automatisch in die Verwaltung zu übernehmen und zu konfigurieren. Um einem neuen Access Point automatisch eine Konfiguration zuweisen zu können, erstellen Sie in diesem Menü ein Profil, das für alle neu zu verwaltenden Access Points Gültigkeit hat, auf die bestimmte Kriterien zutreffen.

9.2.2.1 Bearbeiten oder Neu

Das Menü **Wireless LAN**

Controller->Controller-Konfiguration->Slave-AP-Autoprofil->Neu besteht aus folgenden Feldern:

Felder im Menü Access-Point-Filter

Feld	Beschreibung
MAC-Adresse	Geben Sie die MAC-Adresse eines Access Points ein, der bei seiner Integration in das Netzwerk automatisch konfiguriert werden soll. Standardmäßig ist Alle aktiviert, so dass der Eintrag auf jeden neu hinzukommenden Access Point zutrifft.
IP-Adresse/Netzmaske	Geben Sie eine IP-Adresse und eine Netzmaske ein. Sie können hier Host- ebenso wie auch Netzwerkadressen angeben und so einzelne Access Points ebenso herausfiltern wie auch Gruppen von Access Points in einem Subnetz.

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Standort	Geben Sie den Standort des APs an.
Beschreibung	Geben Sie eine eindeutige Beschreibung für den AP ein.

Felder im Menü Funkmodul 1 oder im Funkmodul 2

Feld	Beschreibung
Betriebsmodus	Wählen Sie aus, ob der Betriebsmodus vom verwendeten Funkmodulprofil bestimmt werden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Aktives Funkmodulprofil	Nur für Betriebsmodus = <i>Aktiviert</i> Wählen Sie ein Funkmodulprofil aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>2.4 GHz Radio Profile</i> • <i>5 GHz Radio Profile</i>

Feld	Beschreibung
Zugewiesene Drahtlosnetzwerke (VSS)	Nur für Betriebsmodus = <i>Aktiviert</i> Fügen Sie mit Hinzufügen ein Drahtlosnetzwerk hinzu.

9.3 Slave-AP-Konfiguration

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

9.3.1 Slave Access Points

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

Für jeden Access Point sehen Sie einen Eintrag mit einem Parametersatz (**Standort, Name, IP-Adresse, LAN-MAC-Adresse, Kanal, Kanalsuche, Status, Aktion**). Durch Klicken auf die \wedge -Schaltfläche oder der \vee -Schaltfläche in der Spalte **Aktion** wählen Sie aus, ob der gewählte Access Point vom WLAN Controller verwaltet werden soll.

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


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


Mögliche Werte für Status


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

Status	Bedeutung
Aus	Der AP ist entweder administrativ deaktiviert oder ausgeschaltet bzw. ohne Stromversorgung o.ä.

9.3.1.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Mithilfe von -Symbol können Sie Einträge löschen. Wenn Sie APs gelöscht haben, werden diese erneut gefunden, jedoch ohne Konfiguration.

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Gerät	Zeigt den Gerätetyp des APs.
Standort	Zeigt den Standort des APs. Wenn kein Standort angegeben ist, werden die Standorte nummeriert. Sie können einen anderen Standort eingeben.
Name	Zeigt den Namen des APs. Sie können den Namen ändern.
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den AP ein.
CAPWAP-Verschlüsselung	Wählen Sie aus, ob die Kommunikation zwischen Master und Slaves verschlüsselt werden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv. Sie können die Verschlüsselung aufheben, um die Kommunikation zu Debug-Zwecken einzusehen.

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
Betriebsmodus	<p>Zeigt, in welchem Modus das Funkmodul betrieben werden soll. Sie können den Modus ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ein</i> (Standardwert): Das Funkmodul dient als Access Point in Ihrem Netzwerk. • <i>Aus</i>: Das Funkmodul ist nicht aktiv.
Aktives Funkmodulprofil	<p>Zeigt das aktuell gewählte Funkmodulprofil. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere Funkmodulprofile angelegt sind.</p>
Kanal	<p>Zeigt den zugewiesenen Kanal. Sie können einen anderen Kanal wählen.</p> <p>Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.</p> <p>Access Point Modus</p> <p>Durch das Einstellen des Netzwerknamens (SSID) im Access Point Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens vier Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt.</p> <p>Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden APs diese Kanäle auch unterstützen.</p> <p>Mögliche Werte (entsprechend dem gewählten Funkmodulprofil):</p> <ul style="list-style-type: none"> • Für Aktives Funkmodulprofil = 2,4 GHz Radio Profile Mögliche Werte sind <i>1</i> bis <i>13</i> und <i>Auto</i> (Standardwert). • Für Aktives Funkmodulprofil = 5 GHz Radio Profile Mögliche Werte sind <i>36</i>, <i>40</i>, <i>44</i>, <i>48</i> und <i>Auto</i>


Feld	Beschreibung
	(Standardwert)
Verwendeter Kanal	Nur für Managed APs. Zeigt den aktuell benutzten Kanal.
Sendeleistung	Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet. • 5 dBm • 8 dBm • 11 dBm • 14 dBm • 16 dBm • 17 dBm
Zugewiesene Drahtlosnetzwerke (VSS)	Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

9.3.2 Funkmodulprofile

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

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

9.3.2.1 Bearbeiten oder Neu

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

Das Menü **Wireless LAN**

Neu besteht aus folgenden Feldern:

Felder im Menü Funkmodulprofil-Konfiguration

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung des Funkmodulprofils ein.
Betriebsmodus	Legen Sie fest, in welchem Modus das Funkmodulprofil betrieben werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Das Funkmodulprofil ist nicht aktiv. • <i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk.
Frequenzband	Wählen Sie das Frequenzband des Funkmodulprofils aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>2,4 GHz In/Outdoor</i> (Standardwert): Ihr Gerät wird mit 2,4 GHz innerhalb oder außerhalb von Gebäuden betrieben. • <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz innerhalb von Gebäuden betrieben. • <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz außerhalb von Gebäuden betrieben. • <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz innerhalb oder außerhalb von Gebäuden betrieben. • <i>5,8 GHz Outdoor</i>: Nur für so genannte Broadband Fixed Wireless Access (BFWA) Anwendungen. Die Frequenzen im Frequenzbereich von 5 755 MHz bis 5 875 MHz dürfen nur in Verbindung mit gewerblichen Angeboten für öffentliche Netzzugänge genutzt werden und bedürfen einer Anmeldung bei der Bundesnetzagentur.

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	Wählen Sie die Wireless-Technologie aus, die der Access-Point anwenden soll. Für Frequenzband = <i>2,4 GHz In/Outdoor</i> Mögliche Werte:

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>802.11g</i>: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • <i>802.11b</i>: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • <i>802.11 mixed (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. • <i>802.11 mixed long (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Nur die Datenrate von 1 und 2 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). Dieser Modus wird auch für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind. • <i>802.11 mixed short (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • <i>802.11b/g/n</i>: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. • <i>802.11g/n</i>: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n. • <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. <p>Für Frequenzband = 5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor oder 5,8 GHz Outdoor</p> <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>802.11ac/a/n</i>: (sofern von Ihrem Gerät unterstützt) Ihr Gerät arbeitet nach 802.11 ac, 802.11a oder nach 802.11n. • <i>802.11ac/n</i>: (sofern von Ihrem Gerät unterstützt) Ihr Gerät arbeitet entweder nach 802.11ac oder 802.11n.
Bandbreite	Nicht für Frequenzband = 2,4 GHz In/Outdoor

Feld	Beschreibung
	<p>Wählen Sie aus, wieviele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>20 MHz</i> (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • <i>40 MHz</i>: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal. • <i>80 MHz</i>: Im Modus 802.11ac steht zusätzlich eine Bandbreite von 80 MHz zur Verfügung.
Anzahl der Spatial Streams	<p>Wählen Sie aus, wieviele 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.
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.
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>

Feld	Beschreibung
	Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.
Wiederkehrender Hintergrund-Scan	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Um in regelmäßigen Abständen automatisch nach benachbarten oder Rogue Access Points im Netzwerk zu suchen, können Sie die Funktion Wiederkehrender Hintergrund-Scan aktivieren. Diese Suche erfolgt ohne eine Beeinträchtigung der Funktion als Access Point.</p> <p>Aktivieren oder deaktivieren Sie die Funktion Wiederkehrender Hintergrund-Scan.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Kanalplan	<p>Wählen Sie den gewünschten Kanalplan aus.</p> <p>Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d.h. dass zwischen den verwendeten Kanälen ein Abstand von vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i>: Alle Kanäle können bei der Kanalwahl gewählt werden. • <i>Auto</i>: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • <i>Benutzerdefiniert</i>: Sie können die gewünschten Kanäle selbst auswählen.
Benutzerdefinierter Kanalplan	Nur für Kanalplan = <i>Benutzerdefiniert</i>

Feld	Beschreibung
	<p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <p>Mit Hinzufügen können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen.</p> <p>Mithilfe von -Symbol können Sie Einträge löschen.</p>
Beacon Period	<p>Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an.</p> <p>Dieser Wert wird in Beacon und Probe Response Frames übermittelt.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 100.</p>
DTIM Period	<p>Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an.</p> <p>Das DTIM Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 2.</p>
RTS Threshold	<p>Sie können hier den Schwellwert in Bytes (1..2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden.</p>
Short Guard Interval	<p>Aktivieren Sie diese Funktion, um den Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.</p>
Max. Übertragungsr	<p>Wählen Sie die Übertragungsgeschwindigkeit aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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.
Short Retry Limit	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Frames ein, dessen Länge kürzer oder gleich dem in RTS Threshold definierten Wert ist. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 7.</p>
Long Retry Limit	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, dessen Länge größer ist als der in RTS Threshold definierte Wert. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 4.</p>
Fragmentation Threshold	<p>Geben Sie die maximale Größe in Byte an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert.</p> <p>Möglich Werte sind 256 bis 2346.</p> <p>Der Standardwert ist 2346.</p>


9.3.3 Drahtlosnetzwerke (VSS)

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

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

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

9.3.3.1 Bearbeiten oder Neu

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

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

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	<p>Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.</p> <p>Wählen Sie außerdem aus, ob der Netzwerkname (SSID) übertragen werden soll.</p> <p>Mit Auswahl von <i>Sichtbar</i> wird der Netzwerkname sichtbar übertragen.</p> <p>Standardmäßig ist er sichtbar.</p>
Intra-cell Repeating	<p>Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
ARP Processing	<p>Wählen Sie aus, ob die Funktion ARP Processing aktiv sein soll. Dabei wird das ARP-Datenaufkommen im Netzwerk reduziert, indem in ARP-Unicasts umgewandelte ARP-Broadcasts an die intern bekannten IP-Adressen weitergeleitet werden. Unicasts sind zudem schneller, und Clients mit aktivierter Power-Save-Funktion werden nicht angesprochen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Beachten Sie, dass ARP Processing nicht zusammen mit der Funktion MAC-Bridge angewendet werden kann.</p>

Feld	Beschreibung
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>
IGMP Snooping	<p>IGMP Snooping reduziert den Datenverkehr und damit die Netzlast, weil Multicast Pakete aus dem LAN nicht weitergeleitet werden. Es werden ausschließlich Multicast-Pakete weitergeleitet, die von den entsprechenden Clients angefordert werden. Wenn Sie IGMP Snooping aktivieren, gibt IGMP Snooping daher den Rahmen vor, in dem Multicast angewendet wird.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	<p>Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch 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>: 802.11x
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Der Standardwert ist <i>Schlüssel 1</i>.</p>

Feld	Beschreibung
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>wep104</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> und <i>WPA 2</i> (Standardwert): WPA und WPA 2 können angewendet werden. • <i>WPA</i>: Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA</i> und <i>WPA</i> und <i>WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): TKIP wird angewendet. • <i>AES</i>: AES wird angewendet. • <i>AES</i> und <i>TKIP</i>: AES oder TKIP wird angewendet.
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA 2</i> und <i>WPA</i> und <i>WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA2 anwenden wollen.</p> <p>Mögliche Werte:</p>

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

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	<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 die-</p>

Feld	Beschreibung
	<p>sem 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>
Max. Anzahl Clients - Soft Limit	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Um eine vollständige Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehnt. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des Max. Anzahl Clients - Hard Limit werden Anfragen strikt abgelehnt.</p> <p>Der Wert der Max. Anzahl Clients - Soft Limit muss gleich oder kleiner sein als der Max. Anzahl Clients - Hard Limit.</p> <p>Der Standardwert ist 28.</p> <p>Sie können diese Funktion deaktivieren, indem Sie Max. Anzahl Clients - Soft Limit und Max. Anzahl Clients - Hard Limit auf den gleichen Wert einstellen.</p>
Auswahl des Client-Bands	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist.</p> <p>Die Option Auswahl des Client-Bands ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert, optimiert für Fast Roaming</i>(Standardwert): Die Funktion wird für dieses VSS

Feld	Beschreibung
	<p>nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN.</p> <ul style="list-style-type: none"> • <i>2,4-GHz-Band bevorzugt</i>: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • <i>5-GHz-Band bevorzugt</i>: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	<p>Wählen Sie aus, ob für dieses Drahtlosnetzwerk nur bestimmte Clients zugelassen werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erlaubte Adressen	<p>Legen Sie Einträge mit Hinzufügen an und geben Sie die MAC-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.</p>
Dynamische Black List	<p>Mithilfe der Funktion Dynamische Black List ist es möglich, Clients, die sich möglicherweise unbefugt Zugriff auf das Netzwerk verschaffen wollen, zu erkennen und für einen bestimmten Zeitraum zu sperren. Ein Client wird dann gesperrt, wenn die Anzahl erfolgloser Anmeldeversuche innerhalb einer definierten Zeit eine bestimmte Anzahl überschreitet. Diese Grenzwerte ebenso wie die Dauer der Sperrung können konfiguriert werden. Ein gesperrten Client wird auf allen vom Wireless LAN Controller verwalteten APs für das betroffene VSS gesperrt, kann sich also auch nicht in einer anderen Funkzelle an diesem VSS anmelden. Soll ein Client permanent gesperrt bleiben, so kann dies im Menü Wireless LAN Controller->Monitoring->Rogue Clients erfolgen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiviert.</p>
Fehlversuche per Zeitraum	<p>Geben Sie hier die Anzahl der Fehlversuche ein, die innerhalb einer bestimmten Zeit von einer MAC-Adresse ausgehen müssen, damit ein Eintrag in der dynamischen Black List angelegt</p>

Feld	Beschreibung
	wird. Standardwerte sind 10 Fehlversuche in 60 Sekunden.
Sperrzeit für Black List	Geben Sie die Zeit ein, für die ein Eintrag in der dynamischen Black List gelten soll. Der Standardwert ist 500 Sekunden.

Felder im Menü VLAN

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

Felder im Menü Bandbreitenbeschränkung für jeden WLAN-Client

Feld	Beschreibung
Rx Shaping	Wählen Sie die Begrenzung der Bandbreite in Empfangsrichtung. Mögliche Werte sind <ul style="list-style-type: none"> • <i>Keine Begrenzung</i> (Standardwert) • <i>0,25 Mbit/s, 0,5 Mbit/s, 1 Mbit/s bis 10 Mbit/s in Einerschritten, 15 Mbit/s, 20 Mbit/s, 30 Mbit/s, 40 Mbit/s und 50 Mbit/s.</i>
Tx Shaping	Wählen Sie die Begrenzung der Bandbreite in Senderichtung. Mögliche Werte sind <ul style="list-style-type: none"> • <i>Keine Begrenzung</i> (Standardwert) • <i>0,25 Mbit/s, 0,5 Mbit/s, 1 Mbit/s bis 10 Mbit/s in Einerschritten, 15 Mbit/s, 20 Mbit/s, 30 Mbit/s, 40 Mbit/s und 50 Mbit/s.</i>

9.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.



Hinweis

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

9.4.1 WLAN Controller

Im Menü **Wireless LAN Controller->Monitoring->WLAN Controller** wird eine Übersicht der wichtigsten Parameter des Wireless LAN Controllers angezeigt. Die Anzeige wird alle 30 Sekunden aktualisiert.

Werte in der Liste Übersicht

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

9.4.2 Slave Access Points

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

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

Points.

9.4.2.1 Übersicht

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

Werte in der Liste Übersicht

Status	Bedeutung
Durchsatz	Zeigt den empfangenen und den gesendeten Datenverkehr pro Funkmodul zeitabhängig an.
Verbundene Clients	Zeigt die Anzahl der angeschlossenen Clients pro Funkmodul zeitabhängig an.

9.4.2.2 Funkmodul 1

Im Menü **Funkmodul** wird der empfangene und der gesendete Datenverkehr pro Client zeitabhängig angezeigt. Jeder Graph in der Darstellung ist über eine Farbe und eine MAC-Adresse eindeutig einem Client zugeordnet.

Werte in der Liste Funkmodul

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

9.4.3 Aktive Clients


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

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

Mögliche Werte für Status

Status	Bedeutung
Keiner	Der Client befindet sich in keinem gültigen Zustand.
Anmeldung	Der Client meldet sich gerade beim WLAN an.
Zugeordnet	Der Client ist beim WLAN angemeldet.
Authentifizieren	Der Client wird gerade authentifiziert.

Status	Bedeutung
Authentifiziert	Der Client ist authentifiziert.

Über das -Symbol öffnen Sie eine Übersicht mit weiteren Details zu den **Aktive Clients**. Die Anzeige wird alle 30 Sekunden aktualisiert.

Werte in der Liste WLAN Client

Status	Bedeutung
Durchsatz	Zeigt den Datenverkehr getrennt nach empfangenen und gesendeten Daten für den gewählten WLAN Client zeitabhängig an.
Signal	Zeigt die Signalstärke für den gewählten WLAN Client zeitabhängig an.

9.4.4 Drahtlosnetzwerke (VSS)

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

9.4.5 Client-Verwaltung

Im Menü **Wireless LAN Controller->Monitoring->Client-Verwaltung** zeigt die Verwaltung der Clients durch die Access Points. Sie sehen u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

Mithilfe des -Symbols können Sie die Werte für den gewünschten Eintrag löschen.

9.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Acces Points und Clients.

9.5.1 Benachbarte APs

Im Menü **Wireless LAN Controller+Umgebungs-Monitoring->Benachbarte APs** werden die benachbarten APs angezeigt, die während des Scannens gefunden wurden. **Rogue**

APs, d.h. APs, die eine vom WLAN-Controller verwaltete SSID verwenden, aber nicht vom WLAN-Controller administriert werden, sind rot hinterlegt.



Hinweis

Überprüfen Sie die angezeigten APs sorgfältig, denn ein Angreifer könnte versuchen, über einen Rogue AP Daten in Ihrem Netz auszuspähen.

Jeder AP wird zwar mehrmals gefunden, aber nur einmal mit der größten Signalstärke angezeigt. Für jeden AP sehen Sie folgende Parameter **SSID**, **MAC-Adresse**, **Signal dBm**, **Kanal**, **Sicherheit**, **Zuletzt gesehen**, **Stärkstes Signal empfangen von**, **Summe der Erkennungen**.

Die Einträge werden alphabetisch nach **SSID** sortiert angezeigt. **Sicherheit** zeigt die Sicherheitseinstellungen des AP. Unter **Stärkstes Signal empfangen von** sehen Sie die Parameter **Standort** und **Name** desjenigen AP, über den der angezeigte AP gefunden wurde. **Summe der Erkennungen** zeigt an, wie oft der entsprechende AP während des Scannens gefunden wurde.

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

9.5.2 Rogue APs

Im Menü **Wireless LAN Controller+Umgebungs-Monitoring->Rogue APs** werden die APs angezeigt, die eine SSID des eigenen Netzes verwenden, aber nicht vom **Wireless LAN Controller** verwaltet werden. **Rogue APs**, die neu gefunden wurden, sind rot hinterlegt.

Für jeden Rogue AP sehen Sie einen Eintrag mit folgendem Parametersatz: **SSID**, **MAC-Adresse**, **Signal dBm**, **Kanal**, **Zuletzt gesehen**, **Gefunden durch AP**, **Angenommen**.



Hinweis

Überprüfen Sie die angezeigten Rogue APs sorgfältig, denn ein Angreifer könnte versuchen, über einen Rogue AP Daten in Ihrem Netz auszuspähen.

Sie können einen Rogue AP als vertrauenswürdig einstufen, indem Sie die Checkbox in


der Spalte **Angenommen** aktivieren. Ein eventuell konfigurierter Alarm wird dadurch gelöscht und ab sofort nicht mehr gesendet. Der rote Hintergrund verschwindet.

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

9.5.3 Rogue Clients

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

Mögliche Werte für Rogue Clients

Status	Bedeutung
MAC-Adresse des Rogue Clients	Zeigt die MAC-Adresse des Clients an, der sich auf der Blacklist befindet.
Netzwerkname (SSID)	Zeigt die beteiligten SSID an.
Angegriffener Access Point	Zeigt den betroffenen AP an.
Signal dBm	Zeigt die Signalstärke des Clients während des Zugriffsversuchs an.
Art des Angriffs	Hier wird die Art des möglichen Angriffs angezeigt, z. B. eine fehlerhafte Authentifizierung.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Zugriffsversuchs an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Zugriffsversuchs an.
Statische Black List	Sie können einen Rogue Client als nicht vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte Statische Black List aktivieren. Die Sperrung des Clients endet dann nicht automatisch, sondern muss von Ihnen manuell wieder aufgehoben werden.
Löschen	Mithilfe des  -Symbols können Sie Einträge löschen.

9.5.3.1 Neu

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Neuer Eintrag in die Blacklist

Feld	Beschreibung
MAC-Adresse des Rogue Clients	Geben Sie die MAC-Adresse des Clients ein, der der statischen Blacklist hinzugefügt werden soll.
Netzwerkname (SSID)	Wählen Sie das Drahtlosnetzwerk aus, von dem der Rogue Client ausgeschlossen werden soll.

9.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

9.6.1 Firmware-Wartung

Im Menü **Wireless LAN Controller->Wartung->Firmware-Wartung** wird eine Liste aller **Managed Access Points** angezeigt.

Für jeden managed AP sehen Sie einen Eintrag mit folgendem Parametersatz: **Firmware aktualisieren, Standort, Gerät, IP-Adresse, LAN-MAC-Adresse, Firmware-Version, Status**.

Klicken Sie auf die Schaltfläche **Alle auswählen**, um alle Einträge für eine Aktualisierung der Firmware auswählen. Klicken Sie auf die Schaltfläche **Alle deaktivieren**, um alle Einträge zu deaktivieren und danach bei Bedarf einzelne Einträge auszuwählen (z. B. wenn bei vielen Einträgen nur die Software einzelner APs aktualisiert werden soll).

Mögliche Werte für Status

Status	Bedeutung
Image bereits vorhanden.	Das Software Image ist bereits vorhanden, es ist kein Update nötig.
Fehler	Es ist ein Fehler aufgetreten..
Wird ausgeführt	Das Update wird gerade ausgeführt.
Fertig	Das Update ist beendet.

Das Menü **Wireless LAN Controller->Wartung->Firmware-Wartung** besteht aus folgenden Feldern:

Felder im Menü Firmware-Wartung

Feld	Beschreibung
Aktion	<p>Wählen Sie die Aktion aus, die Sie ausführen wollen.</p> <p>Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware initiieren. • <i>Konfiguration mit Statusinformationen sichern</i>: Sie können eine Konfiguration sichern, welche Statusinformationen der APs enthält.
Quelle	<p>Wählen Sie die Quelle für die Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>HTTP-Server</i> (Standardwert): Die Datei ist bzw. wird auf dem entfernten Server gespeichert, der in der URL angegeben wird. • <i>Aktuelle Software vom Update-Server</i>: Die Datei liegt auf dem offiziellen Update-Server. (Nur für Aktion = <i>Systemsoftware aktualisieren</i>) • <i>TFTP-Server</i>: Die Datei ist bzw. wird auf dem TFTP-Server gespeichert, der in der URL angegeben wird.
URL	<p>Nur für Quelle = <i>HTTP-Server</i> oder <i>TFTP-Server</i> Geben Sie die URL des Servers ein, von dem die Systemsoftware-Datei geladen werden soll bzw. auf dem die Konfigurationsdatei gespeichert werden soll.</p>

Kapitel 10 Netzwerk

10.1 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.

10.1.1 Konfiguration von IPv4-Routen

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

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse = 192.168.0.0**, **Netzmaske = 255.255.255.0**, **Gateway = 192.168.0.250**, **Schnittstelle = LAN_EN1-0**, **Routentyp = Netzwerkroute via Schnittstelle** angezeigt,

10.1.1.1 Bearbeiten oder Neu


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

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

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

Felder 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 Information, welches Gateway verwendet werden soll, wird per DHCP empfangen und in die Route übernommen. • <i>Vorlage für Host-Route per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Host ergänzt.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Vorlage für Netzwerkroute per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Netzwerk ergänzt. <div data-bbox="541 346 1315 633" style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <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> </div>
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> (Standardwert): 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	<p>Nur für Routentyp = <i>Standardroute über Schnittstelle, Host-Route über Schnittstelle</i> oder <i>Netzwerkroute via Schnittstelle</i></p> <p>Geben Sie die eigene IP-Adresse des Routers auf der ausgewählten Schnittstelle ein.</p>
Ziel-IP-Adresse/Netzmaske	Nur für Routentyp <i>Host-Route über Schnittstelle</i> oder <i>Netzwerkroute via Schnittstelle</i>

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

Felder im Menü Erweiterte Routenparameter

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

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


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


Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Wählen und warten</i> (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", 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.

10.1.2 Konfiguration von IPv6-Routen

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

10.1.2.1 Bearbeiten oder Neu

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

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

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

Felder im Menü Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IPv6-Route an.

Feld	Beschreibung
Route aktiv	<p>Wählen Sie, ob die Route aktiv oder inaktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Route auf den Status aktiv gesetzt.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
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>: Route zu einem Netzwerk über eine spezifische Schnittstelle. • <i>Netzwerkroute via Gateway</i> (Standardwert): Route zu einem Netzwerk über ein spezifisches Gateway.
Zielschnittstelle	<p>Wählen Sie die IPv6-Schnittstelle aus, welche für diese Route verwendet werden soll.</p> <p>Sie können unter den Schnittstellen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind und für welche die Nutzung von IPv6 aktiviert ist.</p>
Quelladresse/Länge	<p>Geben Sie die IPv6-Quelladresse mit der entsprechenden Präfixlänge ein.</p> <p>Die Eingabe <code>::</code> beschreibt eine unspezifische Adresse.</p> <p>Standardmäßig ist eine Präfixlänge von <code>64</code> vorgegeben.</p>
Zieladresse/Länge	<p>Geben Sie die IPv6-Zieladresse mit der entsprechenden Präfixlänge ein.</p> <p>Die Eingabe <code>::</code> beschreibt eine unspezifische Adresse.</p>

Feld	Beschreibung
	Standardmäßig ist eine Präfixlänge von <i>64</i> vorgegeben.
Gateway-Adresse	Geben Sie die IPv6-Adresse für den nächsten Hop ein.
Metrik	Wählen Sie die Priorität der Route aus. Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route. Wertebereich von <i>0</i> bis <i>255</i> , der Standardwert ist <i>1</i> .


10.1.3 IPv4-Routing-Tabelle

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

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse** = *192.168.0.0*, **Netzmaske** = *255.255.255.0*, **Gateway** = *192.168.0.250*, **Schnittstelle** = *LAN_EN1-0*, **Routentyp** = *Netzwerkroute via Schnittstelle*, **Protokoll** = *Lokal* angezeigt,

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.

Feld	Beschreibung
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.

10.1.4 IPv6-Routing-Tabelle

Im Menü **Netzwerk->Routen->IPv6-Routing-Tabelle** wird eine Liste aller im System aktiven IPv6-Routen angezeigt.

Felder im Menü IPv6-Routing-Tabelle

Feld	Beschreibung
Route	Zeigt die Quell- und die Zieladresse, die für diese Route verwendet wird an, sowie die Gateway IP-Adresse. 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.
Protokoll	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell (<i>Lokal</i>) oder über eins der verfügbaren Protokolle.

10.1.5 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.

Im Auslieferungszustand werden mit der Standardeinstellung *Für bestimmte Schnittstellen aktivieren* die beiden Einträge *en1-0* und *ethoa35-5* angezeigt.

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

Felder im Menü **Überprüfung der Rückroute**

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

10.2 Allgemeine IPv6-Präfixe

Allgemeine IPv6-Präfixe werden in der Regel von IPv6-Providern vergeben. Sie können statisch zugewiesen oder über DHCP bezogen werden. Meist handelt es sich um /48- oder /56-Netze. Aus diesen Allgemeinen Präfixen können Sie /64-Subnetze erzeugen und in Ihrem Netz weiterverteilen lassen.

Das Konzept der Allgemeinen Präfixe hat zwei entscheidende Vorteile:


- Zwischen Provider und Kunde genügt eine einzige Route.
- Wenn der Provider einen neuen Allgemeinen Präfix per DHCP zuteilt oder einen statisch zugewiesenen Allgemeinen Präfix ändern muss, haben Sie als Kunde keinen oder wenig Konfigurationsaufwand: Über DHCP erhalten Sie den neuen Allgemeinen Präfix automatisch. Im Falle des statisch zugewiesenen Allgemeinen Präfixes müssen Sie diesen einmal in Ihr System eingeben. Alle aus diesem Allgemeinen Präfix abgeleiteten Subnetze und IPv6-Adressen ändern sich bei einem Update des Allgemeinen Präfixes automatisch.

Um IPv6 zu verwenden, müssen Sie konfigurieren, wie Sie Subnetze und IPv6-Adressen festlegen und verteilen lassen wollen (siehe "IPv6-Adressen konfigurieren unter [Schnittstellen](#) auf Seite 94 sowie die für IPv6 relevanten Parameter im Menü **LAN->IP-Konfiguration->Schnittstellen**).

10.2.1 Konfiguration eines Allgemeinen Präfixes

Im Menü **Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes** wird eine Liste aller konfigurierten IPv6-Präfixe angezeigt.

10.2.1.1 Bearbeiten oder Neu

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

Optionen im Menü Basisparameter

Feld	Beschreibung
Aktiver Allgemeiner Präfix	Wählen Sie, ob das Präfix aktiv oder inaktiv sein soll. Mit <i>Aktiviert</i> wird das Präfix auf den Status aktiv gesetzt. Standardmäßig ist das Präfix aktiv.
Name	Geben Sie einen Namen für das Allgemeine Präfix ein.

Feld	Beschreibung
	Ein sprechender Name dient dazu, das Allgemeine Präfix aus einer Präfixliste leichter auswählen zu können.
Typ	<p>Wählen Sie, wie der Adressraum zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Dynamisch</i> (Standardwert): Der Allgemeine Präfix wird dynamisch mittels einer DHCP-Übertragung festgesetzt, z. B. von einem Provider. • <i>Statisch</i>: Das Präfix wird fest vorgegeben, z. B. durch einen Provider.
Von Schnittstelle	<p>Nur bei Typ = <i>Dynamisch</i></p> <p>Wählen Sie die IPv6-Schnittstelle aus, von welcher ein Allgemeiner Präfix bezogen werden soll.</p> <p>Sie können unter den Schnittstellen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind und die folgende Bedingungen erfüllen:</p> <ul style="list-style-type: none"> • IPv6 ist <i>Aktiviert</i>. • IPv6-Modus = <i>Host</i> • DHCP-Client ist <i>Aktiviert</i>.
Benutzter Präfix/Länge	<p>Nur bei Typ = <i>Statisch</i></p> <p>Geben Sie das Präfix ein, das verwendet werden soll. Geben Sie die zugehörige Länge ein. Dieser Präfix muss mit :: enden.</p> <p>Standardmäßig ist eine Länge von <i>48</i> vorgegeben.</p>

10.3 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in [NAT-Konfiguration](#) auf Seite 159).

Konkrete Hinweise für die Konfiguration von NAT finden Sie am Ende des Kapitels unter [NAT - Konfigurationsbeispiel](#) auf Seite 165.

10.3.1 NAT-Schnittstellen

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

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

Außerdem wird in *Portweiterleitungen* angezeigt, wie viele Portweiterleitungsregeln für diese Schnittstelle konfiguriert wurden.

Optionen im Menü NAT-Schnittstellen

Feld	Beschreibung
NAT aktiv	Wählen Sie aus, ob NAT für die Schnittstelle aktiviert werden soll. Standardmäßig ist die Funktion nicht aktiv.
Loopback aktiv	Mithilfe der NAT-Loopback-Funktion ist Network Address Translation auch bei Anschlüssen möglich, auf denen NAT nicht aktiv ist. Dies wird verwendet, um Anfragen aus dem LAN so zu interpretieren, als ob sie aus dem WAN kämen. Sie können damit Server Services testen. Standardmäßig ist die Funktion nicht aktiv.
Verwerfen ohne Rückmeldung	Wählen Sie aus, ob IP-Pakete stillschweigend durch NAT abgelehnt werden sollen. Ist diese Funktion deaktiviert, wird der Absender der abgelehnten IP-Pakete mit einer entsprechenden ICMP- oder TCP-RST-Nachricht informiert. Standardmäßig ist die Funktion nicht aktiv.
PPTP-Passthrough	Wählen Sie aus, ob auch bei aktiviertem NAT der Aufbau und Betrieb mehrerer gleichzeitiger ausgehender PPTP-Verbindungen von Hosts im Netzwerk erlaubt sein soll. Standardmäßig ist die Funktion nicht aktiv. Wenn PPTP-Passthrough aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpunkt konfiguriert werden.
Portweiterleitungen	Zeigt die Anzahl der in Netzwerk->NAT->NAT-Konfiguration

Feld	Beschreibung
	konfigurierten Portweiterleitungsregeln an.

10.3.2 NAT-Konfiguration

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

10.3.2.1 Neu

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

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

Feld im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
Schnittstelle	Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll. Mögliche Werte: <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	Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>eingehend (Ziel-NAT)</i> (Standardwert): Der Datenverkehr, der von außen kommt. • <i>ausgehend (Quell-NAT)</i>: Der Datenverkehr, der nach außen geht. • <i>exklusiv (ohne NAT)</i>: Der Datenverkehr, der von NAT ausgenommen ist.
NAT-Methode	Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i>

Feld	Beschreibung
	<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 oder port-restricted-cone</i>.</p> <p>Wählen Sie einen der vorkonfigurierten Dienste aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Benutzerdefiniert</i> (Standardwert) • <i><Dienstname></i>

Feld	Beschreibung
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> • <i>IGMP</i> • <i>IGP</i> • <i>IGRP</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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 ursprünglichen Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> bedeutet, dass der Port nicht näher spezifiziert ist.</p>
Originale Quell-	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i></p>

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

Im Menü **NAT-Konfiguration** ->**Substitutionswerte** können Sie, abhängig davon, ob es

sich um eingehenden oder ausgehenden Datenverkehr handelt, neue Adressen und Ports definieren, auf welche bestimmte Adressen und Ports aus dem Menü **NAT-Konfiguration - >Ursprünglichen Datenverkehr angeben** umgesetzt werden.

Felder im Menü Substitutionswerte

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

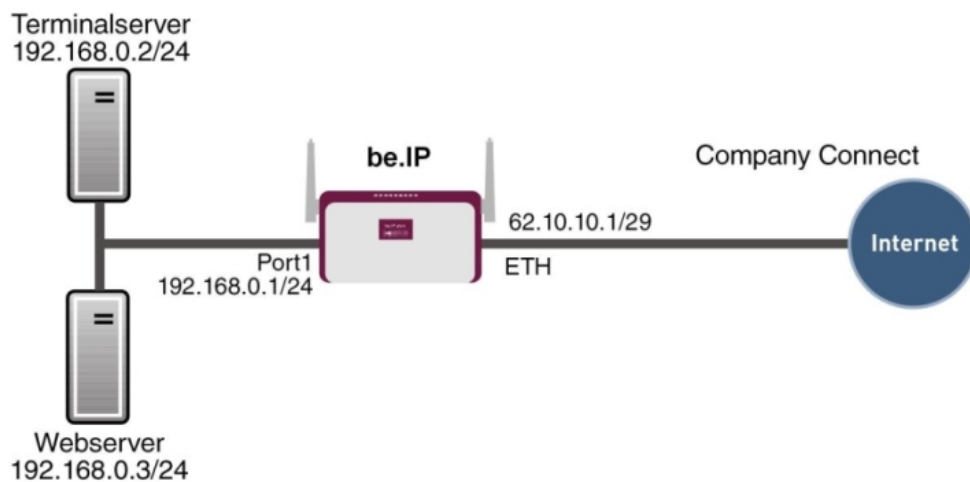
Feld	Beschreibung
	<p>Haben Sie für Original Quell-Port/Bereich <i>Portbereich angeben</i> gewählt, stehen folgende Auswahlmöglichkeiten zur Verfügung:</p> <ul style="list-style-type: none">• <i>Original Quell-Port/Bereich verwenden</i>: Der in Original Quell-Port/Bereich angegebene Bereich wird nicht 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.

10.3.3 NAT - Konfigurationsbeispiel

Voraussetzungen

- Grundkonfiguration des Gateways
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang, hier als Beispiel **Company Connect** mit acht IP-Adressen.
- Die Ethernet-Schnittstelle **ETH** Ihres Geräts ist an den Zugangsrouten zum Internet (IP-Adresse `62.10.10.1/29`) angeschlossen.
- Die IP-Adressen `62.10.10.2` bis `62.10.10.6` sind auf der Ethernet-Schnittstelle **ETH** eingetragen.

Beispielszenario



Konfigurationsziel

- Sie konfigurieren NAT-Freigaben, damit Sie per HTTP auf Ihr Gateway zugreifen können.
- Sie wollen auf Ihren Terminalserver und auf den Firmen-Webserver über das Internet zugreifen können.

Konfigurationsschritte im Überblick

NAT einschalten

Feld	Menü	Wert
NAT aktiv	Netzwerk->NAT->NAT-Schnittstellen	Aktiviert für LAN_EN5-0
Verwerfen ohne Rückmeldung	Netzwerk->NAT->NAT-Schnittstellen	Aktiviert für LAN_EN5-0

NAT-Freigaben konfigurieren

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration->Neu	z. B. GUI
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration->Neu	LAN_EN5-0
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration->Neu	eingehend (Ziel-NAT)
Dienst	Netzwerk->NAT->NAT-Konfiguration->Neu	Benutzerdefiniert

Feld	Menü	Wert
Protokoll	Netzwerk->NAT->NAT-Konfiguration->Neu	TCP
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 62.10.10.1
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration->Neu	80
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	127.0.0.1
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	Original deaktiviert, 80

Webserver

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration->Neu	z. B. <i>Webserver</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration->Neu	LAN_EN5-0
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration->Neu	eingehend (Ziel-NAT)
Dienst	Netzwerk->NAT->NAT-Konfiguration->Neu	http
Protokoll	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 62.10.10.3
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 192.168.0.3
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	Original

Terminal Server

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration->Neu	z. B. <i>Terminal-Server</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration->Neu	LAN_EN5-0
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration->Neu	eingehend (Ziel-NAT)

Feld	Menü	Wert
Dienst	Netzwerk->NAT->NAT-Konfiguration->Neu	Benutzerdefiniert
Protokoll	Netzwerk->NAT->NAT-Konfiguration->Neu	TCP
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	96
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration->Neu	3389
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 192.168.0.2
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	Original

10.4 Lastverteilung


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

Konkrete Hinweise für die Konfiguration von Lastverteilung finden Sie unter [Lastverteilung - Konfigurationsbeispiel](#) auf Seite 176.

10.4.1 Lastverteilungsgruppen

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

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

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



Hinweis

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

10.4.1.1 Neu

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

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. • <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 = Lastabhängige Bandbreite</p> <p>Wählen Sie aus, in welcher Richtung die aktuelle Datenrate berücksichtigt werden soll.</p> <p>Optionen:</p>

Feld	Beschreibung
	<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.

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>

Feld	Beschreibung
	<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
Routenselektor	<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>
IP-Adresse zur Nachverfolgung	<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 Konfigurati-</p>

Feld	Beschreibung
	<p>on 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 Überwachen berücksichtigt werden. Über die Konfiguration der IP-Adresse zur Nachverfolgung im Menü Lastverteilung->>Lastverteilungsgruppen->Erweiterte Einstellungen erfolgt die Verknüpfung zwischen der Lastverteilungsfunktion und der Host-Überwachungsfunktion. Der Lastverteilungsstatus der Schnittstelle wechselt nun in Abhängigkeit vom 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>

10.4.2 Special Session Handling

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

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

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


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

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

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

Wenn Sie unter **Unveränderliche Parameter** für die beide Parameter **Zieladresse** und **Zielport** die Standardeinstellung *aktiviert* belassen, so werden die HTTPS-Pakete mit derselben Quell-IP-Adresse wie das erste HTTPS-Paket über Port 443 zur selben **Zieladresse** über dieselbe Schnittstelle wie das erste HTTPS-Paket geroutet.

10.4.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob Special Session Handling aktiv sein soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.
Dienst	Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: <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>

Feld	Beschreibung
	Der Standardwert ist <i>Benutzerdefiniert</i> .
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.
Quellschnittstelle	Wählen Sie, falls gewünscht, die Quellschnittstelle Ihres Geräts aus.
Quell-IP-Adresse/Netzmaske	<p>Definieren Sie, falls gewünscht, die Quell-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.
Quell-Port/Bereich	Geben Sie, falls gewünscht, eine Quell-Port-Nummer bzw. einen Bereich von Quell-Port-Nummern ein.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Quell-Port ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Quell-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Quell-Port-Bereich ein.
Special Handling Timer	<p>Geben Sie ein, während welcher Zeitspanne die spezifizierten Datenpakete über den festgelegten Weg geroutet werden sollen.</p> <p>Der Standardwert ist <i>900</i> Sekunden.</p>

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

Felder im Menü **Erweiterte Einstellungen**

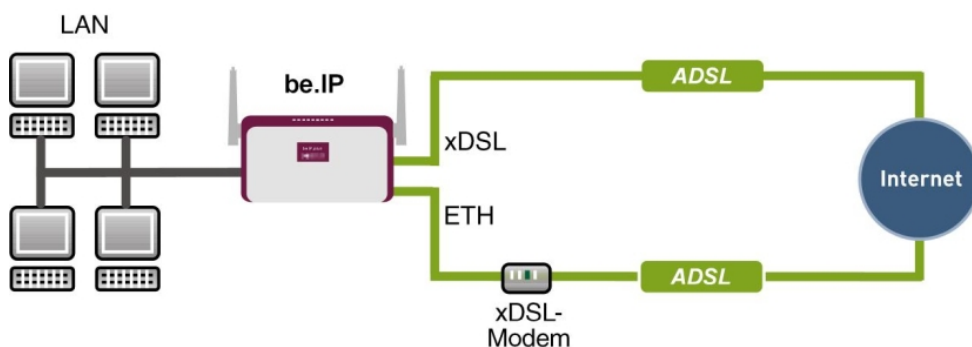
Feld	Beschreibung
Unveränderliche Parameter	<p>Legen Sie fest, ob die beiden Parameter Zieladresse und Zielport bei später gesendeten Datenpaketen denselben Wert haben müssen wie beim ersten Datenpaket, d. h. ob die nachfolgenden Datenpakete über denselben Zielport zur selben Zieladresse geroutet werden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

10.4.3 Lastverteilung - Konfigurationsbeispiel

Voraussetzungen

- Gateway mit integriertem xDSL-Modem
- Externes xDSL-Modem
- Zwei unabhängige xDSL-Internetverbindungen

Beispielszenario



Konfigurationsziel

- Der Datenverkehr wird auf Basis von IP-Sitzungen jeweils zur Hälfte auf die beiden ADSL-Leitungen verteilt.
- Wie Verbindungsabbrüche vermieden werden, welche durch die Verteilung auf verschiedene Internetzugänge auftreten können, zeigen wir Ihnen am Beispiel von verschlüsselten HTTP-Verbindungen (HTTPS).



Hinweis

Beim Aufbau der ADSL-Verbindungen bezieht das Gateway neben der öffentlichen IP-Adresse auch die IP-Adressen der DNS-Server zur Namensauflösung von dem konfigurierten Internet-Provider. Vor allem bei der Verwendung von unterschiedlichen Internet-Providern müssen die DNS-Server verbindungs-spezifisch verwendet werden. Die Konfiguration der DNS-Server wird beim Anlegen der ADSL-Verbindungen automatisch erstellt und kann im Menü **Lokale Dienste->DNS->DNS-Server** eingesehen werden.

Konfigurationsschritte im Überblick

Erste Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	Assistenten->Internetzugang->Internetverbindungen->Neu	Internes ADSL-Modem
Beschreibung	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. ADSL-1
Typ	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	Benutzerdefiniert über PPPoE (PPP über Ethernet)
Benutzername	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. fes-te_ip@provider.de
Passwort	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. test12345



Hinweis

Der Hinweis beim Anlegen der zweiten ADSL-Verbindung kann ignoriert werden. Routingkonflikte aufgrund mehrerer Standardrouten werden durch IP-Lastverteilung verhindert.

Zweite Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	Assistenten->Internetzugang->Internetverbindungen->Neu	Externes xDSL-Modem
Beschreibung	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. ADSL-2
Physischer Ethernet-Port	Assistenten -> Internetzugang->Internetverbindungen->Neu->Weiter	z. B. ETH5
Typ	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	Benutzerdefiniert
Benutzername	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. #0001@t-online.de
Passwort	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. test12345

Lastverteilungsgruppe anlegen

Feld	Menü	Wert
Gruppenbeschreibung	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu	z. B. <i>Internetzugang</i>
Verteilungsrichtlinie	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu	<i>Sitzungs-Round-Robin</i>
Verteilungsmodus	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu	<i>Immer</i>
Schnittstelle	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	<i>WAN_ADSL-1</i>
Verteilungsverhältnis	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	<i>50</i>
Schnittstelle	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	<i>WAN_ADSL-2</i>
Verteilungsverhältnis	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	<i>50</i>

Special Session Handling

Feld	Menü	Wert
Beschreibung	Netzwerk->Lastverteilung->Special Session Handling->Neu	z. B. <i>HTTPS</i>
Dienst	Netzwerk->Lastverteilung->Special Session Handling->Neu	<i>http (SSL)</i>
Special Handling Timer	Netzwerk->Lastverteilung->Special Session Handling->Neu	<i>900 Sekunden</i>

10.5 QoS

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

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen
- Daten klassifizieren
- Daten priorisieren

10.5.1 IPv4/IPv6-Filter

Im Menü **Netzwerk->QoS->IPv4/IPv6-Filter** werden IP-Filter konfiguriert.

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

10.5.1.1 Neu

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

Das Menü **Netzwerk->QoS->IPv4/IPv6-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>Der Standardwert ist <i>any</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>

Feld	Beschreibung
	<p>Mögliche Werte: <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> <p>Siehe RFC 792.</p> <p>Der 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.
IPv4-Zieladresse/-netzmaske	<p>Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.
Ziel-Port/Bereich	<p>Nur für Protokoll = <i>TCP</i>, <i>UDP</i> oder <i>TCP/UDP</i></p> <p>Geben Sie eine Zielport-Nummer bzw. einen Bereich von Zielport-Nummern ein.</p>

Feld	Beschreibung
	<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 Zielport ein. • <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.
IPv4-Quelladresse/-netzmaske	<p>Geben Sie die IPv4 Quell-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Quelladresse/-länge	<p>Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Länge ist nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
Quell-Port/Bereich	<p>Nur für Protokoll = <i>TCP, UDP</i> oder <i>TCP/UDP</i></p> <p>Geben Sie eine Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Quellport ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Quellport ein. • <i>Portbereich angeben</i>: Geben Sie einen Quellport-Bereich ein.
DSCP / Traffic Class	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p>

Feld	Beschreibung
Filter (Layer 3)	<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.
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>

10.5.2 QoS-Klassifizierung

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


10.5.2.1 Neu

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

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 angelegten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	<p>Nur für Klassenplan = Neu</p> <p>Geben Sie die Bezeichnung des Klassenplans ein.</p>
Filter	<p>Wählen Sie ein IP-Filter aus.</p> <p>Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll.</p> <p>Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll.</p> <p>Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü Netzwerk->QoS->QoS-Filter konfiguriert sein.</p>
Richtung	<p>Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen.</p> <p>Mögliche Werte:</p> <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.

Feld	Beschreibung
High-Priority-Klasse	<p>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.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Klassen-ID	<p>Nur für High-Priority-Klasse nicht aktiv.</p> <p>Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zuweist.</p> <div data-bbox="539 645 1315 833" style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <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>
DSCP/Traffic-Class-Filter setzen (Layer 3)	<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 For-

Feld	Beschreibung
	<p>mat angegeben, z. B. 63.</p> <ul style="list-style-type: none"> • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
Setze COS Wert (802.1p/Layer 2)	<p>Im Header der Ethernet-Pakete, die vom ausgewählten Filter erfasst werden, können Sie hier die Serviceklasse (Layer-2-Priorität) setzen/ändern.</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Der Standardwert ist <i>Erhalten</i>.</p>
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>

10.5.3 QoS-Schnittstellen/Richtlinien

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



Hinweis

Daten können nur ausgehend priorisiert werden.

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

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

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

10.5.3.1 Neu

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

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.
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-	Nur für Traffic Shaping = aktiviert.

Feld	Beschreibung
Geschwindigkeit	<p>Geben Sie für die ausgewählte Schnittstelle eine maximale Datenrate in kBit 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 ausgewählte Schnittstelle kann ihre 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 (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>
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-</p>

Feld	Beschreibung
	<p>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)
<p>Real Time Jitter Control</p>	<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>
<p>Kontrollmodus</p>	<p>Nur für Real Time Jitter Control = aktiviert.</p> <p>Wählen Sie den Modus für die Optimierung der Sprachübertragung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream erkannt wurde. • <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • <i>Nur kontrollierte RTP-Streams</i>: Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gate-

Feld	Beschreibung
	<p>way (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW.</p> <ul style="list-style-type: none"> • <i>Immer</i>: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.
Queues/Richtlinien	<p>Konfigurieren Sie die gewünschten QoS-Queues.</p> <p>Für jede angelegte Klasse aus dem Klassenplan, die mit der gewählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und hier angezeigt (nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr).</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu. Das Menü Queue/Richtlinie bearbeiten öffnet sich.</p> <p>Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag DEFAULT mit der niedrigsten Priorität 255 erstellt.</p>

Das Menü **Queue/Richtlinie bearbeiten** besteht aus folgenden Feldern:

Felder im Menü Queue/Richtlinie bearbeiten

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung der Queue/Richtlinie an.
Ausgehende Schnittstelle	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
Priorisierungsqueue	<p>Wählen Sie den Typ für die Priorisierung der Queue aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Klassenbasiert</i> (Standardwert): Queue für "normal"-klassifizierte Daten. • <i>Hohe Priorität</i>: Queue für "high-priority"-klassifizierte Daten. • <i>Standard</i>: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	Nur für Priorisierungsqueue = <i>Klassenbasiert</i>

Feld	Beschreibung
	<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</i> oder <i>Weighted Fair Queueing</i></p> <p>Wählen Sie die Gewichtung der Queue. Mögliche Werte sind <i>1 bis 254</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
RTT-Modus (Realtime-Traffic-Modus)	<p>Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen.</p> <p>Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.</p>
Traffic Shaping	<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>

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>Maximale Upload-Geschwindigkeit</p>	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie eine maximale Datenrate in kBit pro Sekunde für die ausgewählte Schnittstelle ein.</p> <p>Mögliche Werte sind 0 bis 1000000.</p> <p>Der Standardwert ist 0, d. h. es erfolgt keine Begrenzung, die ausgewählte Schnittstelle kann ihre maximale Bandbreite belegen.</p>
<p>Überbuchen zugelassen</p>	<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>
<p>Burst-Größe</p>	<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>

10.6 Zugriffsregeln

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

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

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

Möchten z. B. Standorte, deren LANs über ein bintec 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 (nicht für alle Geräte verfügbar) oder mit ISDN-Login auf Ihr Gateway zu.

10.6.1 Zugrifffilter

In diesem Menü werden die Access-Filter konfiguriert. Jedes Filter beschreibt einen bestimmten Teil des IP-Traffic und definiert z. B. die IP-Adressen, das Protokoll, den Quell- oder Ziel-Port.

Im Menü **Netzwerk->Zugriffsregeln->Zugriffsfiler** wird eine Liste aller Access Filter angezeigt.

10.6.1.1 Bearbeiten oder Neu

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

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.

Feld	Beschreibung
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>Der Standardwert ist <i>any</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 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>Der Standardwert ist <i>Beliebig</i>.</p> <p>Siehe RFC 792.</p>
Verbindungsstatus	<p>Nur bei Protokoll = <i>TCP</i></p>

Feld	Beschreibung
	<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.
IPv4-Zieladresse/-netzmaske	<p>Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge 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.

Feld	Beschreibung
IPv4-Quelladresse/-netzmaske	<p>Geben Sie die IPv4 Quell-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
IPv6-Quelladresse/-länge	<p>Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
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 / Traffic Class 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


Feld	Beschreibung
	<p>nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</p> <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>Der Standardwert ist <i>Nicht beachten</i>.</p>

10.6.2 Regelketten

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

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

10.6.2.1 Bearbeiten oder Neu


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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Regelkette	Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen.

Feld	Beschreibung
	<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 annehmen, wenn das Filter nicht passt. • <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.

10.6.3 Schnittstellenzuweisung

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

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

10.6.3.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.
Verwerfen ohne Rückmeldung	Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll. <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	Legen Sie fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll. <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-IPAdresse und Quell-Port-Nummer wird generiert. • <i>Dump</i>: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.

Kapitel 11 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.

11.1 Allgemein

11.1.1 Allgemein

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

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.

11.2 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.

11.2.1 IGMP

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

11.2.1.1 Bearbeiten oder Neu

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

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

Felder im Menü IGMP-Einstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der IGMP aktiviert werden soll, d.h. Queries werden versendet und Antworten akzeptiert.
Abfrage Intervall	Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen. Möglich Werte sind <i>0</i> bis <i>600</i> . Der Standardwert ist <i>125</i> .
Maximale Antwortzeit	Geben Sie für das Senden von Queries an, in welchem Zeitintervall in Sekunden Hosts auf jeden Fall antworten müssen. Die Hosts wählen aus diesem Intervall zufällig eine Verzögerung, bis die Antwort gesendet wird. Damit können Sie bei Netzen mit vielen Hosts eine Streuung und somit eine Entlastung erreichen. Möglich Werte sind <i>0,0</i> bis <i>25,0</i> . Der Standardwert ist <i>10,0</i> .
Robustheit	Wählen Sie den Multiplikator zur Steuerung interner Timer-Werte aus. Mit einem höheren Wert kann z. B. in einem verlustreichen Netzwerk ein Paketverlust kompensiert werden. Durch einen zu hohen Wert kann sich aber auch die Zeit zwischen dem Abmelden und dem Stopp des eingehenden Datenverkehrs erhöhen (Leave Latency). Möglich Werte sind <i>2</i> bis <i>8</i> . Der Standardwert ist <i>2</i> .
Antwortintervall (Letztes Mitglied)	Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet.

Feld	Beschreibung
	<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 <i>0,0</i> bis <i>25,0</i>.</p> <p>Der Standardwert ist <i>1,0</i>.</p>
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 IPGM-Proxy-Schnittstelle weitergeleitet.

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>
Fallback-	Nur für IGMP Proxy = aktiviert

Feld	Beschreibung
Proxy-Schnittstelle 1	Wählen Sie die Fallback-Schnittstelle 1 Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen. Diese wird verwendet, wenn die IGMP-Proxy-Funktion über die Proxy-Schnittstelle nicht ausgeführt werden kann.
Fallback-Proxy-Schnittstelle 2	Nur für IGMP Proxy = aktiviert Wählen Sie die Fallback-Schnittstelle 2 Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen. Diese wird verwendet, wenn die IGMP-Proxy-Funktion über die Fallback-Proxy-Schnittstelle 1 nicht ausgeführt werden kann.

11.2.2 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.

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
IGMP-Status	Wählen Sie den IGMP-Status aus. Mögliche Werte: <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	Nur für IGMP-Status = <i>Aktiv</i> oder <i>Auto</i> Wählen Sie den Multicast-Modus aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Kompatibilitätsmodus</i> (Standardwert): Der Router verwendet IGMP Version 3. Bemerkte 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	<p>Geben Sie ein, wie viele Gruppen sowohl intern als auch in Reports maximal möglich sein sollen.</p> <p>Der Standardwert ist <i>64</i>.</p>
Maximale Quellen	<p>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.</p> <p>Der Standardwert ist <i>64</i>.</p>
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 <i>0</i>, d. h. die Anzahl der IGMP-Statusmeldungen ist nicht begrenzt.</p>

11.3 Weiterleiten

11.3.1 Weiterleiten

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

11.3.1.1 Neu

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

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 <i>224.0.0.0/4</i>, von der definierten Quellschnittstelle an die definierte Zielschnittstelle weitergeleitet werden soll. Setzen Sie dazu den Haken für <i>Aktiviert</i>.</p>

Feld	Beschreibung
	<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 12 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.

12.1 Internet + Einwählen

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

Darüber hinaus können Sie Adress-Pools für die dynamische Vergabe von IP-Adressen anlegen.

Um mit Ihrem Gerät Verbindungen zu Netzwerken oder Hosts außerhalb Ihres LANs herstellen zu können, müssen Sie die gewünschten Verbindungspartner auf Ihrem Gerät einrichten. Dies gilt sowohl für ausgehende Verbindungen (z. B. Ihr Gerät wählt sich bei einem entfernten Partner ein), als auch für eingehende Verbindungen (z. B. ein entfernter Partner wählt sich bei Ihrem Gerät ein).

Wenn Sie einen Internetzugang herstellen wollen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider (ISP) einrichten. Für Breitband-Internetzugänge stellt Ihr Gerät Protokolle wie PPP-over-Ethernet (PPPoE), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung. Ein Internetzugang mittels ISDN ist, sofern von Ihrem Gerät unterstützt, 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
<input checked="" type="checkbox"/>	verbunden

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

12.1.1 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.

12.1.1.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE (<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

Feld	Beschreibung
	<p>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 PP-PoE-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>
<p>PPPoE-Ethernet-Schnittstelle</p>	<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> <p>Wählen Sie den Wert <i>Automatisch</i> um den automatischen VDSL-/ADSL-Modus zu unterstützen. In diesem Modus wird die Schnittstelle für der Internetzugang automatisch gewählt. Achten Sie darauf, dass für einen ADSL-Zugang im Menü ATM eine Schnittstelle angelegt sein muss, für einen VDSL-Zugang ist dies nicht notwendig.</p>
<p>PPPoE-Schnittstelle für Mehrfachlink</p>	<p>Nur für PPPoE-Modus= <i>Mehrfachverbindung</i></p> <p>Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die Hinzufügen-Schaltfläche, um weitere Einträge anzulegen.</p>
<p>Benutzername</p>	<p>Geben Sie den Benutzernamen ein.</p>
<p>Passwort</p>	<p>Geben Sie das Passwort ein.</p>
<p>VLAN</p>	<p>Einige Internet Service Provider erfordern eine VLAN-ID. Aktivieren Sie diese Funktion, um unter VLAN-ID einen Wert eingeben zu können.</p>
<p>VLAN-ID</p>	<p>Nur wenn VLAN aktiviert ist.</p>

Feld	Beschreibung
	Geben Sie die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.
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, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den 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 IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 283 konfigurieren.</p>

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<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). Der Standardwert ist 1.

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob die gewählte PPPoE- Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 283 konfigurieren.</p>
IPv6-Modus	<p>Nur für IPv6 = Aktiviert</p> <p>Die gewählte PPPoE-Schnittstelle wird im Host-Modus betrieben.</p>
Router Advertisement annehmen	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Host</p> <p>Wählen Sie, ob Router Advertisements über die Schnittstelle empfangen werden sollen. Mithilfe der Router Advertisements wird die Default Router List sowie die Prefix-Liste erstellt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
DHCP-Client	<p>Nur für IPv6 = Aktiviert und IPv6-Modus = Host</p>

Feld	Beschreibung
	<p>Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
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 <i>60</i>.</p>
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind <i>0</i> bis <i>100</i>.</p> <p>Der Standardwert ist <i>5</i>.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen.

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

Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die Verbindung verwendet werden darf.</p> <p>Mit dem Standardwert <i>Automatisch</i> wird der Wert beim Verbindungsaufbau durch das Link Control Protocol vorgegeben.</p> <p>Wenn Sie <i>Automatisch</i> deaktivieren, können Sie einen Wert eingeben.</p> <p>Mögliche Werte sind 1 bis 8192.</p> <p>Der Standardwert ist 0.</p>

12.1.2 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.

12.1.2.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen beliebigen Namen ein, um die Internetverbindung 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-Ethernet-Schnittstelle	<p>Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden.</p> <p>Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist.</p> <p>Bei Verwendung des internen DSL-Modems, wählen Sie hier die in Physikalische Schnittstellen->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle 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>

Feld	Beschreibung
	Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
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 IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 283 konfigurieren.</p>
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. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.

Feld	Beschreibung
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <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). Der Standardwert ist 1.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist 60.

Feld	Beschreibung
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 asymmetrische Bandbreiten (ADSL) angewendet werden.</p>

Feld	Beschreibung
	<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>Der 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>Der 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>

12.1.3 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.

12.1.3.1 Neu

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

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 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 IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 283 konfigurieren.</p>
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	<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>Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.</p>

Feld	Beschreibung
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). Der Standardwert ist 1.

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob das gewählte ATM-Profil das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung das gewählte ATM-Profil betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü</p>

Feld	Beschreibung
	<i>Firewall</i> auf Seite 283 konfigurieren.
IPv6-Modus	Nur für IPv6 = Aktiviert Das gewählte ATM-Profil wird im Host-Modus betrieben.
Router Advertisement annehmen	Nur für IPv6 = Aktiviert und IPv6-Modus = Host Wählen Sie, ob Router-Advertisements über das ATM-Profil empfangen werden sollen. Mithilfe der Router-Advertisements wird die Default Router List sowie die Prefix List erstellt. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
DHCP-Client	Nur für IPv6 = Aktiviert und IPv6-Modus = Host Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren 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
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist <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 diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte:

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

12.1.4 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.

12.1.4.1 Neu

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

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 USB-Port des Geräts.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
	Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte sind 0 bis 3600 (Sekunden). 0 deaktiviert den Short-Hold.</p> <p>Der Standardwert ist 300.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<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>

Feld	Beschreibung
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). Der Standardwert ist 1.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist 60.</p>
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte von 0 bis 100.</p> <p>Der Standardwert ist 5.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>


12.1.5 IP Pools

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

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

Eingetragene Host-Routen haben immer Vorrang vor IP-Adressen aus den Adress-Pools. Wenn also ein eingehender Ruf authentisiert wurde, überprüft Ihr Gerät zunächst, ob für den Anrufer in der Routing-Tabelle eine Host-Route eingetragen ist. Wenn dies nicht der Fall ist, kann Ihr Gerät eine IP-Adresse aus einem Adress-Pool zuweisen (falls verfügbar). Bei Adress-Pools mit mehr als einer IP-Adresse können Sie nicht festlegen, welcher Verbindungspartner welche Adresse bekommt. Die Adressen werden zunächst einfach der Reihe nach vergeben. Bei einer erneuten Einwahl innerhalb eines Intervalls von einer Stunde wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

12.1.5.1 Bearbeiten oder Neu

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

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>

12.2 ATM

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

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

In einem ATM-Netz können unterschiedliche Anwendungen wie z. B. Sprache, Video und Daten nebeneinander im asynchronen Zeitmultiplexverfahren übertragen werden. Jedem

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

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

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

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

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

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

12.2.1 Profile

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

12.2.1.1 Neu

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

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

Felder im Menü ATM-Profilparameter

Feld	Beschreibung
Provider	Wählen Sie eines der vorkonfigurierten ATM-Profilen für Ihren Provider aus der Liste aus oder definieren Sie mit <code>-- Benutzerdefiniert --</code> ein Profil.
Beschreibung	Nur für Provider = <code>-- Benutzerdefiniert --</code> 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 = <code>-- Benutzerdefiniert --</code> Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte: <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.

Feld	Beschreibung
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. Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen). • <i>LLC Bridged FCS</i>: Wird nur für Typ = <i>Ethernet über ATM</i> angezeigt. Bridged Ethernet mit LLC/SNAP-Enkapsulierung mit Frame Check Sequence (Prüfsummen). • <i>Nicht ISO</i> (Standardwert für Geroutete Protokolle über ATM): Wird nur für Typ = <i>Geroutete Protokolle über ATM</i> angezeigt. Enkapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>LLC</i>: Wird nur für Typ = PPP über ATM angezeigt. <p>Enkapsulierung mit LLC-Header.</p> <ul style="list-style-type: none"> • <i>VC-Multiplexing</i> (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Enkapsulierung (Null Enkapselung) 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 = Ethernet über ATM</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 = Ethernet über ATM</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 = Statisch</p> <p>Geben Sie die IP-Adressen (IP-Adresse) und die entsprechenden Netzmasken (Netzmaske) der ATM-Schnittstellen ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.</p>
MAC-Adresse	<p>Geben Sie der routerinternen Schnittstelle der ATM-Verbindung eine MAC-Adresse, z. B. <i>00:a0:f9:06:bf:03</i>. Ein Eintrag wird nur in speziellen Fällen benötigt.</p> <p>Für Internetverbindungen ist es ausreichend, die Option Voreingestellte verwenden (Standardeinstellung) auszuwählen. Es</p>

Feld	Beschreibung
	wird eine Adresse verwendet, die von der MAC-Adresse des <i>en1-0</i> abgeleitet ist.
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. <i>00:e1:f9:06:bf:03</i>.</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 <i>en1-0</i> 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	<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>

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

Feld	Beschreibung
Client-Typ	Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei

Feld	Beschreibung
	<p>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 221.</p>

12.2.2 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.

12.2.2.1 Neu

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

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.

Feld	Beschreibung
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. 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. • <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>

Feld	Beschreibung
Sustained Cell Rate (SCR)	<p>Nur für ATM-Dienstkatgorie = <i>Variable Bit Rate V.1 (VBR.1)</i> oder <i>Variable Bit Rate V.3 (VBR.3)</i></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-Dienstkatgorie = <i>Variable Bit Rate V.1 (VBR.1)</i> oder <i>Variable Bit Rate V.3 (VBR.3)</i></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>

12.2.3 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.

12.2.3.1 Neu

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

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

Felder im Menü OAM-Flusskonfiguration

Feld	Beschreibung
OAM-Fluss-Level	Wählen Sie den zu überwachenden OAM-Fluss-Level. Mögliche Werte: <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)	Nur für OAM-Fluss-Level = <i>F5</i> Wählen Sie die zu überwachende bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus.
Virtual Path Connection (VPC)	Nur für OAM-Fluss-Level = <i>F4</i> Wählen Sie die zu überwachende bereits konfigurierte Virtual Path Connection (angezeigt durch den VPI) aus.

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.

12.3 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.

12.3.1 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.

12.3.1.1 Neu

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

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 13 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.

13.1 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 64) 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 IPv4-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 IPv4-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 IPv4-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 IPv4-Datenverkehrs**, so wird es verworfen.

Erfüllt ein IP-Paket die Anforderungen in einem **Zusätzlicher Filter des IPv4-Datenverkehrs**, so startet die IPSec-Phase-2-Aushandlung und der Datenverkehr wird über den Tunnel übertragen.



Hinweis

Der Parameter **Zusätzlicher Filter des IPv4-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.

13.1.1 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 konfigurierten IPSec-Peers nach

Priorität sortiert angezeigt.

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 422.

13.1.1.1 Neu

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

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>Wählen Sie die IP-Version aus. Sie können wählen, ob IPv4 oder IPv6 bevorzugt verwendet werden soll oder ob nur eine der beiden IP-Versionen erlaubt sein soll.</p>
	<p> Hinweis</p> <p>Diese Auswahl ist nur relevant, wenn ein Host-Name als Peer-Adresse eingegeben wird.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IPv4 bevorzugt</i> • <i>IPv6 bevorzugt</i> • <i>Nur IPv4</i> • <i>Nur IPv6</i> <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>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	Nur für IKE (Internet Key Exchange) = <i>IKEv2</i>

Feld	Beschreibung
	<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) = IKEv2</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) = IKEv2</p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für Authentifizierungsmethode = DSA-Signatur oder <i>RSA-Signatur</i> wird die Option Subjektnamen aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektnamen aus Zertifikat verwenden aktivieren, wird der erste im Zertifikat angegebene Subjekt-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 64), 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</p>

Feld	Beschreibung
	Partner für Sie konfiguriert, identisch sind.
Preshared Key	Geben Sie das mit dem Peer vereinbarte Passwort ein. Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer <i>0x</i> am Anfang des Eintrags.
IP-Version des Tunnelnetzwerks	Wählen Sie aus, ob IPv4 oder IPv6 oder beide Versionen für den VPN-Tunnel verwendbar sein sollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i> • <i>IPv4 und IPv6</i>

Felder im Menü IPv4-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i> (Standardwert) : Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 283 konfigurieren.</p>
IPv4-Adressvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: <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

Feld	Beschreibung
	<p>IPSec-Client vom Server eine IP-Adresse erhalten soll.</p> <ul style="list-style-type: none"> • <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 IPv4-Adressvergabe = <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. <p>Dieser Wert muss für beide Seiten des Tunnels identisch sein.</p>
IP-Zuordnungspool	<p>Nur bei IPv4-Adressvergabe = <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 IPv4-Adressvergabe = <i>Statisch</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Server im IKE-Konfigurationsmodus</i></p> <p>Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.</p>

Feld	Beschreibung
Metrik	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Client</i> im <i>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>. der Standardwert ist <i>1</i>.</p>
Routeneinträge	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Client</i> im <i>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. • <i>Netzmaske</i>: Netzmaske zu <i>Entfernte IP-Adresse</i>. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich <i>0 - 15</i>). der Standardwert ist <i>1</i>.

Felder im Menü Zusätzlicher Filter des IPv4-Datenverkehrs

Feld	Beschreibung
Zusätzlicher Filter des IPv4-Datenverkehrs	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv1</i></p> <p>Legen Sie mithilfe von Hinzufügen einen neuen Filter an.</p>

Felder im Menü IPv6-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i>: Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-

Feld	Beschreibung
	<p>Pakete durchgelassen, außer denen, die explizit verboten sind.</p> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 283 konfigurieren.</p>
Lokales IPv6-Netzwerk	<p>Wählen Sie ein Netzwerk aus. Sie können unter den Link-Präfixen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind.</p> <p>Geben Sie die Lokale IPv6-Adresse mit der entsprechenden Präfixlänge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.</p>
Entferntes IPv6-Netzwerk	<p>Fügen Sie mit Hinzufügen einen neuen Präfix hinzu. Geben Sie die Adresse der Tunnelgegenstelle ein. Standardmäßig ist eine Länge von 64 und eine Priorität von 1 vorgegeben. Je niedriger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.</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 IPv4-Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port an-

geben. Ist ein **Zusätzlicher Filter des IPv4-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 IPv4-Datenverkehrs**, so wird es verworfen.

Erfüllt ein IP-Paket die Anforderungen in einem **Zusätzlicher Filter des IPv4-Datenverkehrs**, so startet die IPSec-Phase-2-Aushandlung und der Datenverkehr wird über den Tunnel übertragen.



Hinweis

Der Parameter **Zusätzlicher Filter des IPv4-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.

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Protokoll	Wählen Sie ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i> (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.

Feld	Beschreibung
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-Profile als Standard markiert ist • <i>Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü . • <i><Profilname></i>: Verwendet ein Profil, das im Menü VPN->IPSec->Phase-1-Profile für Phase 1 konfiguriert wurde.
Phase-2-Profil	Wählen Sie ein Profil für die Phase 2 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: <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

Feld	Beschreibung
	<p>Phase 2 die Proposals 3DES/MD5, AES-128/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü VPN->IPSec->Phase-2-Profile.</p> <ul style="list-style-type: none"> • <i><Profilname></i>: Verwendet ein Profil, das im Menü VPN->IPSec->Phase-2-Profile für Phase 2 konfiguriert wurde.
XAUTH-Profil	<p>Wählen Sie ein in VPN->IPSec->XAUTH-Profile angelegtes Profil aus, wenn Sie zur Authentifizierung dieses IPSec-Peers XAuth verwenden möchten.</p> <p>Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.</p>
Anzahl erlaubter Verbindungen	<p>Wählen Sie aus, 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 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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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>Nur wenn unter Öffentliche Schnittstelle eine Schnittstelle ausgewählt ist.</p> <p>Legen Sie fest, wie strikt die Einstellung gehandhabt wird.</p> <p>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>: Die Prioritäten der aktuellen Routingtabelle werden verwendet. Nur wenn mehrere gleichwertige Routen zur Verfügung stehen, wird die Route über die gewählte Schnittstelle verwendet.
Öffentliche IPv4-Quelladresse	<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 IPv4-Quelladresse 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>
Öffentliche IPv6-Quelladresse	<p>Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für</p>

Feld	Beschreibung
	<p>den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die Öffentliche IPv6-Quelladresse 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 IPv4-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>
IPv4 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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Nie einwählen</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum IP-Sec 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 IPv4 IPSec Callback* auf Seite 262 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 IPv4 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.

13.1.2 Phase-1-Profile

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

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

13.1.2.1 Neu

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

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>

Feld	Beschreibung
	<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>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

Feld	Beschreibung
	<p>verwendet.</p> <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. • <i>SHA2-256</i>: SHA 2 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus der als Nachfolger von SHA 1 standardisiert wurde. Er kann mit Hash-Längen von 256, 384 und 512 Bit verwendet werden. • <i>SHA2-384</i>: SHA-2 mit 384 Bit Hash-Länge. • <i>SHA2-512</i>: SHA-2 mit 512 Bit Hash-Länge. <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p> <p>Beachten Sie, dass die Qualität der Algorithmen relativen Gesichtspunkten unterliegt und sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern kann.</p>
DH-Gruppe	<p>Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec elmeg-Geräten unterstützt wird, steht für "modular exponentiation".</p> <p>Folgende Gruppen und zugehörige Bit-Werte der Exponentiation stehen zur Verfügung:</p> <ul style="list-style-type: none"> • 1 (768 Bit) • 2 (1024 Bit) • 5 (1536 Bit) • 14 (2048 Bit) • 15 (3072 Bit) • 16 (4096 Bit) <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>

Feld	Beschreibung
Lebensdauer	<p>Legen Sie die Lebensdauer für Phase-1-Schlüssel fest.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <ul style="list-style-type: none"> • Eingabe in Sekunden: Geben Sie die Lebensdauer für Phase-1- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der 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 = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist.</p>

Feld	Beschreibung
	<p>Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>
<p>Modus</p>	<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>
<p>Lokaler ID-Typ</p>	<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>
<p>Lokaler ID-Wert</p>	<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</p>

Feld	Beschreibung
	<p>Subjektnamen aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektnamen aus Zertifikat verwenden 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 64), 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>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden & Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • <i>Dead Peer Detection</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Erreichbarkeit des Peers nur überprüft, wenn tatsächlich Daten an ihn gesendet werden sollen. • <i>Dead Peer Detection (Idle)</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vorgenommen. <p>Nur für Phase-1-Parameter (IKEv2)</p> <p>Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Blockzeit	<p>Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche.</p> <p>Zur Verfügung stehen Werte von -1 bis 86400 (Sekunden), der Wert -1 bedeutet die Übernahme des Wertes im Standardprofil, der Wert 0, dass der Peer in keinem Fall blockiert wird.</p> <p>Der Standardwert ist 30.</p>

Feld	Beschreibung
NAT-Traversal	<p>NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.</p> <p>Ohne NAT-T kann es zwischen IPSec und NAT zu Inkompatibilitäten kommen (siehe RFC 3715, Abschnitt 2). Diese behindern vor allem den Aufbau eines IPSec-Tunnels von einem Host innerhalb eines LANs und hinter einem NAT-Gerät zu einem anderen Host bzw. Gerät. NAT-T ermöglicht derartige Tunnel ohne Konflikte mit NAT-Geräten, aktiviertes NAT wird vom IPSec-Daemon automatisch erkannt und NAT-T wird verwendet.</p> <p>Nur für <i>IKEv1-Profile</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert): NAT-Traversal ist aktiv. • <i>Deaktiviert</i>: NAT-Traversal ist deaktiviert. • <i>Erzwingen</i>: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. <p>Nur für <i>IKEv2-Profile</i></p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CA-Zertifikate	<p>Nur für 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>

13.1.3 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.

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

13.1.3.1 Neu

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

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

Felder im Menü Phase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	<p>Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
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

Feld	Beschreibung
	<p>Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet.</p> <ul style="list-style-type: none"> • <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 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. <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. • <code>-- ALLE --</code>: 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. • <i>SHA2-256</i>: SHA 2 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus der als Nachfolger von SHA 1 standardisiert wurde. Er kann mit Hash-Längen von 256, 384 und 512 Bit verwendet werden. • <i>SHA2-384</i>: SHA-2 mit 384 Bit Hash-Länge. • <i>SHA2-512</i>: SHA-2 mit 512 Bit Hash-Länge. <p>Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.</p>

Feld	Beschreibung
	<p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</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>Folgende Gruppen und zugehörige Bit-Werte der Exponentiation stehen zur Verfügung:</p> <ul style="list-style-type: none"> • 1 (768 Bit) • 2 (1024 Bit) • 5 (1536 Bit) • 14 (2048 Bit) • 15 (3072 Bit) • 16 (4096 Bit) <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
<p>Lebensdauer</p>	<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. Der Standardwert ist 7200. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-2-

Feld	Beschreibung
	<p>Schlüssel als Menge der verarbeiteten Daten in kBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist 0.</p> <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>Der Standardwert ist 80 %.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<p>IP-Komprimierung</p>	<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 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>
<p>Erreichbarkeitsprüfung</p>	<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

Feld	Beschreibung
	<p>Gegenstelle mit bintec elmeg) oder <i>Inaktiv</i> (bei Gegenstelle ohne bintec elmeg) gesetzt.</p> <ul style="list-style-type: none"> • <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>

13.1.4 XAUTH-Profile

Im Menü **XAUTH-Profile** wird eine Liste aller XAuth-Profile angezeigt.

Extended Authentication für IPSec (XAuth) ist eine zusätzliche Authentifizierungsmethode für Benutzer eines IPSec-Tunnels.

Das Gateway kann bei Nutzung von XAuth zwei verschiedene Rollen übernehmen, es kann als Server oder als Client dienen:

- Das Gateway fordert als Server einen Berechtigungsnachweis an.
- Das Gateway weist als Client seine Berechtigung nach.

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Die Berechtigung wird entweder anhand einer Liste oder über einen RADIUS Server geprüft. Bei Verwendung eines Einmalpassworts (One Time Password, OTP) kann die Passwortüberprüfung von einem Token-Server übernommen werden (z. B. beim Produkt SecOVID von Kobil), der hinter dem RADIUS-Server installiert ist. Wenn über IPSec eine Firmenzentrale mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden. Je nach Zuordnung verschiedener Profile kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechselnd in verschiedenen Filialen arbeitet, jeder Peer eine Filiale repräsentiert und der Angestellte jeweils vor Ort Zugriff auf den Tunnel haben will.

Nachdem IPSec IKE (Phase 1) erfolgreich beendet ist und bevor IKE (Phase 2) beginnt, wird XAuth realisiert.

Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.

13.1.4.1 Neu

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

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.

13.1.5 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 **IPv4-Adressvergabe Server im IKE-Konfigurationsmodus** eingestellt haben, müssen Sie hier die IP-Pools, aus denen die IP-Adressen vergeben werden, definieren.

13.1.5.1 Bearbeiten oder Neu

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

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.

Feld	Beschreibung
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>

13.1.6 Optionen

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

Felder im Menü Globale Optionen

Feld	Beschreibung
IPSec aktivieren	<p>Wählen Sie, ob Sie IPSec aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.</p>
Vollständige IPSec-Konfiguration löschen	<p>Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts.</p> <p>Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen.</p> <p>Das Löschen der Konfiguration ist nur möglich mit IPSec aktivieren = nicht aktiviert.</p>
IPSec-Debug-Level	<p>Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Benachrichtigung</i> • <i>Information</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, ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session eingebettet wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Initial Contact Message senden	<p>Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von <i>Aktiv</i> zu <i>Inaktiv</i>, <i>Ruhend</i> oder</p>

Feld	Beschreibung
	<p>geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zero Cookies verwenden	<p>Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen.</p> <p>Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall <i>Aktiviert</i>.</p>
Größe der Zero Cookies	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten und auf Null gesetzten SPI in Bytes ein.</p> <p>Der Standardwert ist 32.</p>
Dynamische RADIUS-Authentifizierung	<p>Wählen Sie aus, ob die RADIUS-Authentifizierung über IPsec aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	<p>Wählen Sie aus, ob Zertifikatsanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungs-Payloads senden	<p>Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatsanforderungen gesendet werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
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 zu unterdrücken.</p>

13.2 be.IP Secure Client

Hier können Sie die aktuelle Secure IPSec Client Software herunterladen. Weitere Informationen finden Sie auf www.bintec-elmeg.com.

Kapitel 14 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).

Konkrete Hinweise für die Konfiguration einer Stateful Inspection Firewall (SIF) finden Sie am Ende des Kapitels unter [SIF - Konfigurationsbeispiel](#) auf Seite 298.

14.1 Richtlinien

14.1.1 IPv4-Filterregeln


Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.


Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Verwerfen-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.

Dem Sicherheitskonzept liegt die Vorstellung zugrunde, dass die Infrastruktur aus vertrauenswürdigen und nicht vertrauenswürdigen Zonen besteht. Die beiden Sicherheitsrichtlinien *Vertrauenswürdig* bzw. *Nicht Vertrauenswürdig* beschreiben diese Vorstellung. Sie definieren die beiden Filterregeln **Vertrauenswürdige Schnittstellen** und **Nicht vertrauenswürdige Schnittstellen**, die standardmäßig angelegt sind und nicht gelöscht werden können.

Falls Sie die **Sicherheitsrichtlinie** *Vertrauenswürdig* verwenden, werden alle Datenpakete akzeptiert. Sie können nun zusätzliche Filterregeln definieren, die bestimmte Pakete verwerfen. Auf die gleiche Weise können Sie für die Einstellung *Nicht Vertrauenswürdig* ausgewählte Datenpakete freigeben.

Im Menü **Firewall->Richtlinien->IPv4-Filterregeln** wird eine Liste aller konfigurierten IPv4-Filterregeln angezeigt.

Mit der Schaltfläche  in der Zeile **Vertrauenswürdige Schnittstellen** können Sie festlegen, welche Schnittstellen **Vertrauenswürdig** sind. Es öffnet sich ein neues Fenster mit einer Schnittstellenliste. Sie können die einzelnen Schnittstellen als vertrauenswürdig markieren.

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 Dia-

log, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

14.1.1.1 Neu

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

Das Menü **Firewall->Richtlinien->IPv4-Filterregeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	<p>Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</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 vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i>

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

14.1.2 IPv6-Filterregeln

Das Standard-Verhalten mit der **Aktion** = *Zugriff* besteht aus zwei impliziten Filterregeln: wenn ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann und wenn eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden), wird das Paket zugelassen.

Die Abfolge der Filterregeln in der Liste ist relevant: Die Filterregeln werden der Reihe nach auf jedes Paket angewendet, bis eine Filterregel zutrifft. Kommt es zu Überschneidungen, d. h. trifft für ein Paket mehr als eine Filterregel zu, wird lediglich die erste Filterregel ausgeführt. Wenn also die erste Filterregel ein Paket zurückweist, während eine spätere Regel es zulässt, so wird es abgewiesen. Ebenso bleibt eine Verwerfen-Regel ohne Auswirkung, wenn ein entsprechendes Paket zuvor von einer anderen Filterregel zugelassen wird.


Dem Sicherheitskonzept liegt die Vorstellung zugrunde, dass die Infrastruktur aus vertrauenswürdigen und nicht vertrauenswürdigen Zonen besteht. Die beiden Sicherheitsrichtlinien *Vertrauenswürdig* bzw. *Nicht Vertrauenswürdig* beschreiben diese Vorstellung. Sie definieren die beiden Filterregeln **Vertrauenswürdige Schnittstellen** und **Nicht vertrauenswürdige Schnittstellen**, die standardmäßig angelegt sind und nicht gelöscht

werden können.

Falls Sie die **Sicherheitsrichtlinie** *Vertrauenswürdig* verwenden, werden alle Datenpakete akzeptiert. Sie können nun zusätzliche Filterregeln definieren, die bestimmte Pakete verwerfen. Auf die gleiche Weise können Sie für die Einstellung *Nicht Vertrauenswürdig* ausgewählte Datenpakete freigeben.

Datenpakete, die das Neighbour Discovery Protocol verwenden, sind grundsätzlich erlaubt, auch für die Filterregel *Nicht Vertrauenswürdig*.


Im Menü **Firewall->Richtlinien->IPv6-Filterregeln** wird eine Liste aller konfigurierten IPv6-Filterregeln angezeigt.


Mit der Schaltfläche  in der Zeile **Vertrauenswürdige Schnittstellen** können Sie festlegen, welche Schnittstellen **Vertrauenswürdig** sind. Es öffnet sich ein neues Fenster mit einer Schnittstellenliste. Sie können die einzelnen Schnittstellen als vertrauenswürdig markieren.



Hinweis

Beachten Sie, dass die Schnittstellenliste für IPv6 leer ist, solange IPv6 für keine Schnittstelle aktiviert ist.

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.

14.1.2.1 Neu

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

Das Menü **Firewall->Richtlinien->IPv6-Filterregeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus. In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstel-

Feld	Beschreibung
	<p>lengruppen (siehe Firewall->Schnittstellen->IPv6-Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl, für die IPv6 aktiviert ist.</p>
Ziel	<p>Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus.</p> <p>In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->IPv6-Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl, für die IPv6 aktiviert ist.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <i>dns</i> • <i>http</i> • <i>nntp</i> <p>Weitere Dienste werden in Firewall->Dienste->Diensteliste angelegt.</p> <p>Außerdem stehen die in Firewall->Dienste->Gruppen konfigurierten Dienstegruppen zur Auswahl.</p>
Aktion	<p>Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • <i>Verweigern</i>: Die Pakete werden abgewiesen. • <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Feh-

Feld	Beschreibung
	ermeldung wird an den Sender des Pakets ausgegeben.

14.1.3 Optionen

In diesem Menü können Sie die IPv4-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.



Hinweis

Beachten Sie, dass die IPv6-Firewall immer eingeschaltet ist und nicht ausgeschaltet werden kann.

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

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Status der IPv4-Firewall	<p>Aktivieren oder deaktivieren Sie die IPv4-Firewall-Funktion.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierte Aktionen	<p>Wählen Sie den Firewall-Syslog-Level aus.</p> <p>Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Alle Firewall-Aktivitäten werden angezeigt. • <i>Verweigern</i>: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion". • <i>Annehmen</i>: Nur Accept-Ereignisse werden angezeigt. • <i>Keiner</i>: Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige IPv4-Filterung	<p>Bei TCP-Sessions überwacht die SIF im ersten Schritt, ob eine Session korrekt und vollständig aufgebaut wird. Im zweiten</p>

Feld	Beschreibung
	<p>Schritt erfolgt die eigentliche Filterung. Für diesen "Normalfall" ist die Standardeinstellung Vollständige IPv4-Filterung <i>Aktivieren</i> vorgesehen.</p> <p>Wenn bei zweiseitiger Kommunikation eine Richtung des Datenverkehrs über den Router läuft, die Datenpakete der entgegengesetzten Richtung aber einen anderen Weg nehmen, wird der Datenverkehr vom Router nicht zugelassen, weil die Session aus Sicht der SIF unvollständig ist. Dies gilt auch, wenn es eine Regel gibt, die denselben Datenverkehr bei vollständiger Session durchlassen würde.</p> <p>Um den Datenverkehr bei solchen unvollständigen Sessions durchzulassen, müssen Sie Vollständige IPv4-Filterung deaktivieren.</p>
STUN Handler	<p>Wenn Sie Geräten (vor allem SIP Clients) in Ihrem Netzwerk erlauben wollen, über STUN den Modus der Network Address Translation sowie die öffentliche IP-Adresse zu ermitteln, so aktivieren Sie diese Option. Die Firewall erstellt dann temporäre Regeln, die den RTP-Datenverkehr für SIP-Gespräche ermöglichen.</p>
Port-STUN-Server	<p>Nur für STUN Handler = Aktiviert</p> <p>Geben Sie Nummer des Ports ein, der für die Verbindung zum STUN-Server benutzt werden soll.</p> <p>Standardmäßig ist der Wert <i>3478</i> vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.</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>

Feld	Beschreibung
	Der Standardwert ist <i>3600</i> .
PPTP-Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine PPTP-Session als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i> . Der Standardwert ist <i>86400</i> .
Andere Inaktivität	Geben Sie ein, nach welcher Zeit der Inaktivität eine Session eines anderen Typs als abgelaufen betrachtet werden soll (in Sekunden). Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i> . Der Standardwert ist <i>30</i> .

Felder im Menü Firewall auf Werkseinstellungen zurücksetzen

Feld	Beschreibung
Firewall auf Werkseinstellungen zurücksetzen	Klicken Sie auf Zurücksetzen um die Firewall auf Werkseinstellungen zurückzusetzen.

14.2 Schnittstellen

14.2.1 IPv4-Gruppen

Im Menü **Firewall->Schnittstellen->IPv4-Gruppen** wird eine Liste aller konfigurierten IPv4-Schnittstellen-Gruppen angezeigt.

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

14.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv4-Schnittstellen-Gruppen einzurichten.

Das Menü **Firewall->Schnittstellen->IPv4-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv4-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 .

14.2.2 IPv6-Gruppen

Im Menü **Firewall->Schnittstellen->IPv6-Gruppen** wird eine Liste aller konfigurierten IPv6-Schnittstellen-Gruppen angezeigt.

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

14.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IPv6-Schnittstellen-Gruppen einzurichten.

Das Menü **Firewall->Schnittstellen->IPv6-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv6-Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

14.3 Adressen

14.3.1 Adressliste

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

14.3.1.1 Neu

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

Das Menü **Firewall->Adressen->Adressliste->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adresse ein.
IPv4	Erlaubt die Konfiguration von IPv4-Adresslisten. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Adresstyp	Nur für IPv4 = Aktiviert Wählen Sie aus, welche Art von Adresse Sie angeben wollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Adresse/Subnetz</i> (Standardwert): Sie geben eine IP-Adresse mit Subnetzmaske ein. • <i>Adressbereich</i>: Sie geben einen IP-Adressbereich mit Anfangs- und Endadresse ein.
Adresse/Subnetz	Nur für IPv4 = Aktiviert und Adresstyp = Adresse/Subnetz Geben Sie die IP-Adresse des Hosts oder eine Netzwerk-Adresse und die zugehörige Netzmaske ein. Standardwert ist jeweils <i>0.0.0.0</i> .
Adressbereich	Nur für IPv4 = Aktiviert und Adresstyp = Adressbereich Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein.
IPv6	Erlaubt die Konfiguration von IPv6-Adresslisten. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
Adresse/Präfix	Nur für IPv6 = <i>Aktiviert</i> Geben Sie die IPv6-Adresse und das zugehörige Präfix ein.

14.3.2 Gruppen

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

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

14.3.2.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adressgruppe ein.
IP-Version	Wählen Sie die verwendete IP-Version aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i> Standardmäßig ist <i>IPv4</i> ausgewählt.
Auswahl	Wählen Sie aus den zur Verfügung stehenden Adressen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

14.4 Dienste

14.4.1 Dienstliste

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

14.4.1.1 Neu

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

Das Menü **Firewall->Dienste->Dienstliste->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protokoll	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
Zielportbereich	<p>Nur für Protokoll = <i>TCP, UDP/TCP</i> oder <i>UDP</i></p> <p>Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll.</p> <p>Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>.</p>
Quellportbereich	<p>Nur für Protokoll = <i>TCP, 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</p>

Feld	Beschreibung
	<p>Obergrenze einzutragen.</p> <p>Mögliche Werte sind 1 bis 65535.</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> <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 Ad-</i>

Feld	Beschreibung
	<i>ministratively Prohibited</i> <ul style="list-style-type: none"> • <i>Communication with Destination Host is Administratively Prohibited</i>

14.4.2 Gruppen

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

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

14.4.2.1 Neu

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

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 .

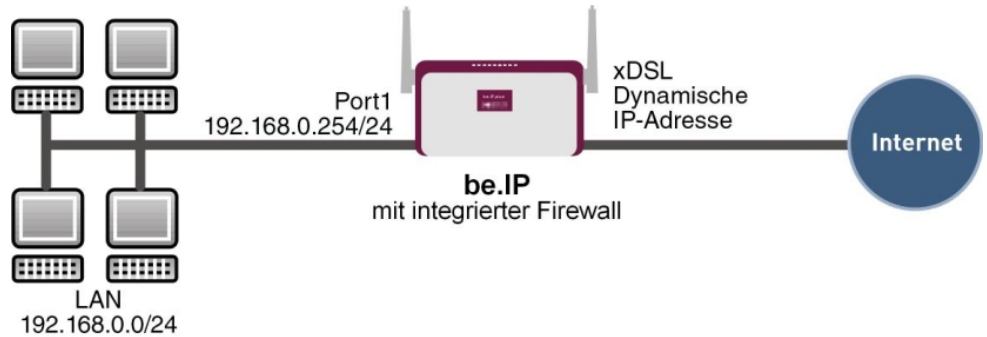
14.5 Konfiguration

14.5.1 SIF - Konfigurationsbeispiel

Voraussetzungen

- Verbindung zum Internet
- Ihr LAN muss mit dem Port 1, 2, 3 oder 4 Ihres Gateways (z. B. RS232bw) verbunden sein

Beispielszenario



Konfigurationsziel

- Den Mitarbeitern eines Unternehmens sollen nur bestimmte Dienste im Internet zur Verfügung stehen (HTTP, HTTPS, FTP, DNS).
- Das Gateway soll als DNS-Proxy arbeiten, das heißt, die Clients verwenden die als DNS-Server.
- Nur der Systemadministrator und der Geschäftsführer sollen eine HTTP- und eine Telnetverbindung zum Gateway herstellen können.
- Der Geschäftsführer soll alle Dienste im Internet nutzen können.
- Jeglicher anderer Datenverkehr soll geblockt werden.



Wichtig

Bei einer Fehlkonfiguration der Firewall kann die Funktionalität des Routers bzw. der Verbindungen mitunter stark beeinträchtigt oder sogar unterbrochen werden.

Es gilt der bei Firewalls übliche Grundsatz: Was nicht explizit erlaubt ist, ist verboten.

Daher ist eine genaue Planung der Filterregeln und der Filterregelkette erforderlich um eine korrekte Arbeitsweise sicherzustellen.

Konfigurationsschritte im Überblick

Aliasnamen für IP-Adressen und Netzadressen

Feld	Menü	Wert
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Administrator</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>

Feld	Menü	Wert
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.2</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Geschäftsführer</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.3</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>be.IP</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.254</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Netzwerk-Intern</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.0.0</i> mit <i>255.255.255.0</i>

Adressgruppen

Feld	Menü	Wert
Beschreibung	Firewall->Adressen->Gruppen->Neu	z. B. <i>be.IP</i>
IP-Version	Firewall->Adressen->Gruppen->Neu	<i>IPv4</i>
Auswahl	Firewall->Adressen->Gruppen->Neu	z. B. <i>Administrator und Geschäftsführer</i>

Dienstgruppen

Feld	Menü	Wert
Beschreibung	Firewall->Dienste->Gruppen->Neu	z. B. <i>Internetports</i>
Mitglieder	Firewall->Dienste->Gruppen->Neu	z. B. <i>http, http (SSL)</i>

Feld	Menü	Wert
	pen->Neu	und <i>ftp</i>
Beschreibung	Firewall->Dienste->Gruppen->Neu	z. B. <i>Administrationsports</i>
Mitglieder	Firewall->Dienste->Gruppen->Neu	z. B. <i>http</i> und <i>telnet</i>

Filterregel 1: Gateway verwalten (Systemadministrator)

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>be.IP</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>be.IP</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Administrationsports</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>

Filterregel 2: Gateway als DNS-Proxy verwenden

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LOCAL</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>dns</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Netzwerk_Intern</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>be.IP</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>dns</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>

Filterregel 3: Zugriff von außen auf das Gateway verweigern

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>ANY</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>be.IP</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Verweigern</i>

Filterregel 4: Zugriff auf alle Dienste im Internet erlauben (Geschäftsführer)

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Geschäftsführer</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>

Filterregel 5: Zugriff auf das Internet erlauben (Mitarbeiter)

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Netzwerk_Intern</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>ANY</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Internetports</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>

Kapitel 15 VoIP

Voice over IP (VoIP) nutzt das IP-Protokoll für Sprach- und Bildübertragung.

Der wesentliche Unterschied zur herkömmlichen Telefonie besteht darin, dass die Sprachinformationen nicht über eine geschaltete Verbindung in einem Telefonnetz übertragen werden, sondern durch das Internet-Protokoll in Datenpakete aufgeteilt, die auf nicht festgelegten Wegen in einem Netzwerk zum Ziel gelangen. Diese Technologie macht sich so für die Sprachübertragung die Infrastruktur eines bestehenden Netzwerks zu Nutze und teilt sich dieses mit anderen Kommunikationsdiensten.

Das Session Initiation Protocol (SIP) dient dabei zum Aufbau, zum Abbau und zur Steuerung einer Kommunikationssitzung.


15.1 Einstellungen

15.1.1 Teilnehmer

Hier können Sie die Rufnummern der Endgeräte (=Teilnehmer) konfigurieren, die an das Media Gateway angebunden sind, d.h. die Rufnummern der SIP-Endgeräte sowie der angeschalteten ISDN-Endgeräte abhängig von den verfügbaren Schnittstellen.

Im Menü **VoIP->Einstellungen->Teilnehmer** wird eine Liste aller vorhandenen Teilnehmer angezeigt.

15.1.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Teilnehmers ein.
Teilnehmer / Benutzername	ISDN-Endgeräte: Geben Sie die Rufnummer des Teilnehmers. SIP-Endgeräte: Geben Sie den Benutzernamen ein.

Feld	Beschreibung
	Maximal können 40 Zeichen eingegeben werden.
Schnittstellentyp	<p>Wählen Sie den Schnittstellentyp aus, welcher verwendet werden soll.</p> <p>Die Auswahl ist von den verfügbaren Schnittstellen abhängig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SIP</i>: Ein SIP-Endgerät wird für den Ruf verwendet. • <i>ISDN</i>: Ein ISDN-Endgerät wird für den Ruf verwendet. Nur wählbar, wenn ISDN-Schnittstellen konfiguriert mit Euro-ISDN Punkt-zu-Mehrpunkt (NT Mode) zur Verfügung stehen. • <i>Analog</i>: Ein analoges Endgerät wird für den Ruf verwendet. Nur wählbar, wenn analoge Schnittstellen vorhanden sind.
ISDN-Schnittstelle auswählen	<p>Nur für Schnittstellentyp = <i>ISDN</i></p> <p>Wählen Sie eine ISDN-Schnittstelle aus. Welche ISDN-Schnittstellen Sie auswählen können, hängt vom verwendeten Gerät ab.</p>
Analoge Schnittstelle auswählen	<p>Nur für Schnittstellentyp = <i>Analog</i></p> <p>Wählen Sie eine analoge Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • fxs5-1 • fxs5-2 • fxs5-3 (Standardwert) • fxs5-4
Registrierung	<p>Nur für Schnittstellentyp = <i>SIP</i></p> <p>Wählen Sie, ob der Registrierungsmechanismus per SIP REGISTER Meldung benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.</p>

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Abgesehen von diesem Standard-Vorgehen können die relevanten Daten auch an eine bestimmte IP-Adresse geschickt werden, die den Verbindungspartnern bereits bekannt ist. Dann entfallen Registrierung und Authentisierung, in diesem Fall muss die Funktion Registrierung deaktiviert sein. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP.</p>
Gültigkeit	<p>Nur wenn Registrierung aktiviert ist.</p> <p>Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird.</p> <p>Bei Clients wird der externe Port automatisch erkannt und sollte nicht geändert werden.</p> <p>Zur Verfügung stehen Werte von 0 bis 3600.</p> <p>Der Standardwert ist 60.</p>
SIP-Endpunkt-IP-Adresse	<p>Nur wenn Registrierung deaktiviert ist.</p> <p>Für Konfigurationen, bei denen keine Registrierung vorgesehen ist (z. B. Anbindung an einen Microsoft Exchange Communication Server), kann die Verbindung als statischer Host eingerichtet werden. Hierzu ist es nötig, die statische IP-Adresse des Endgeräts anzugeben.</p>
Authentifizierungs-ID	<p>Nur für Schnittstellentyp = SIP</p> <p>Tragen Sie einen Namen ein, der zur Authentifizierung verwendet wird.</p> <p>Maximal können 20 Zeichen eingegeben werden.</p> <p>Den hier vergebenen Namen müssen Sie auch auf dem SIP-Telefon eingeben.</p> <p>Wenn Sie keinen Namen eingeben, wird der Name im Feld Teilnehmer / Benutzername verwendet.</p>
Passwort	<p>Nur für Schnittstellentyp = SIP</p>

Feld	Beschreibung
	<p>Geben Sie hier ein Passwort ein.</p> <p>Maximal können 20 Zeichen eingegeben werden.</p> <p>Das hier vergebene Passwort müssen Sie auch auf dem SIP-Telefon eingeben.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches für die Datenübertragung verwendet werden soll.</p> <p>Mögliche Werte: <i>UDP</i> (Standardwert), <i>TCP</i> oder <i>TLS</i>.</p> <p>Wenn ein Protokoll automatisch erkannt wurde, sollte es nicht geändert werden.</p>
Port	<p>Geben Sie die Nummer des UDP, TCP bzw. TLS Ports, der für die Verbindung zum Server bzw. Proxy benutzt werden soll.</p> <p>Mögliche Werte sind <i>0</i> bis <i>65535</i>.</p> <p>Der Standardwert ist <i>5060</i>.</p>

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

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Reihenfolge	<p>Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich. • <i>Qualität</i>: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • <i>Niedrigste</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • <i>Höchste</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.

Feld	Beschreibung
Sortierreihenfolge	<p>Wählen sie die Codecs aus, die für die Verbindung vorgeschlagen werden sollen. Abhängig von der Einstellung im Feld Co- dec-Reihenfolge werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>G. 711 uLaw</i>: ISDN Codec nach US Kennlinie • <i>G. 711 aLaw</i>: ISDN Codec nach EU Kennlinie • <i>G. 729</i>: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • <i>G. 726-40</i>: Komprimiert von 63 auf 40 KBit/s • <i>G. 726-32</i>: Komprimiert von 55 auf 32 KBit/s • <i>G. 726-24</i>: Komprimiert von 47 auf 24 KBit/s • <i>G. 726-16</i>: Komprimiert von 39 auf 16 KBit/s • <i>DTMF Outband</i>: DTMF Outband. Zuerst wird versucht RFC 2833 zu verwenden. Wenn die Gegenstelle diesen Standard nicht "beherrscht", wird SIP Info verwendet. • <i>T. 38 Fax</i>: Ermöglicht den Versand von Faxmitteilungen über Datennetzwerke. • <i>SRTP</i>: SRTP ist eine verschlüsselte Variante des Real-Time Transport Protokolls (RTP). • <i>Daten (RFC 4040)</i>: Ermöglicht den Transport eines 64-kbit/s-Datenstroms in RTP-Paketen. <p>Standardmäßig sind <i>G. 711 uLaw</i>, <i>G. 711 aLaw</i> und <i>G. 729</i> aktiviert.</p> <p>Die tatsächlich verwendeten Codecs sind die Schnittmenge der hier festgelegten und der vom Provider signalisierten Codecs. Von diesen Codecs fallen bei ausgehenden Rufen noch diejenigen weg, welche mehr als die verfügbare Bandbreite benötigen würden.</p>

Felder im Menü Sprachqualitätseinstellungen

Feld	Beschreibung
Echounterdrückung	<p>Wählen Sie aus, ob Echounterdrückung verwendet werden soll.</p> <p>Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-</p>

Feld	Beschreibung
	<p>Rückkopplungen unterdrückt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Comfort Noise Generation (CNG)	<p>Wählen Sie aus, ob Comfort Noise Generation (CNG) verwendet werden soll.</p> <p>Bei digitaler Sprachübertragung sorgt dieses Verfahren durch das Erzeugen eines leichten Hintergrundrauschens dafür, dass während Gesprächspausen beim Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Paketgröße	<p>Geben Sie an, wieviel Millisekunden Sprache ein RTP-Datenpaket enthält.</p> <p>Zur Verfügung stehen Werte von <i>5</i> bis <i>500</i>.</p> <p>Der Standardwert ist <i>20</i>.</p>

15.1.2 SIP-Konten

Wenn Sie Ihr Gerät an andere SIP-Server (z. B. Server von Internet SIP Service Providern) anbinden wollen, können Sie hier die notwendigen Einträge konfigurieren. In diesem Fall fungiert das Media Gateway als SIP-Client.

Außerdem können Sie hier die Einträge für SIP-Trunking-Szenarios konfigurieren. In diesem Fall fungiert das Media Gateway als SIP-Server für andere SIP-Server. Ein Beispiel hierfür ist die Anbindung einer SIP-PBX (z. B. Asterisk) an das Media Gateway.

Das bedeutet, dass sowohl alle SIP-Provider-Accounts hier konfiguriert werden als auch mit dem Media Gateway verbundene durchwahlfähige Telefonanlagen (Direct Dial-in).




Hinweis

Verwenden Sie dieses Menü auf keinen Fall zur Konfiguration von SIP-Nebenstellen, d.h. für SIP-Clients oder PSTN-Clients wie z. B. SIP-Telefone, Terminal Adapter oder ISDN-Telefone!

SIP-Nebenstellen können Sie im Menü **VoIP->Teilnehmer** konfigurieren.

Im Menü **VoIP->Einstellungen->SIP-Konten** wird eine Liste aller vorhandenen SIP-Konten (SIP Client Modus und SIP Server Modus) angezeigt.

15.1.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um neue SIP-Konten hinzuzufügen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. In diesem Menü werden sowohl SIP-Konten im SIP Client Modus als auch im SIP Server Modus konfiguriert.

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des SIP-Kontos ein.
Administrativer Status	Wählen Sie aus, ob das SIP-Konto aktiv sein soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Trunk-Modus	Wählen Sie aus, ob und in welchem Trunk-Modus das SIP-Konto betrieben werden soll. Durch den Trunk-Modus (DDI, Direct Dial In) wird ermöglicht, dass ein eingehender Ruf genau einem Endgerät zugeordnet werden kann (Durchwahl). Bei einem ausgehenden Ruf kann der Anrufer dem Angerufenen angezeigt werden. Welche Einstellung verwendet werden kann, hängt vom Provider ab. Mögliche Werte: <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Der Trunk-Modus wird nicht verwendet. Das SIP-Konto hat nur eine Nummer. • <i>Client</i>: Das Media Gateway wird als DDI-Client betrieben. Es erhält eine Durchwahl. • <i>Server</i>: Das Media Gateway wird als DDI-Server betrieben,

Feld	Beschreibung
	<p>so daß sich DDI-Clients verbinden können.</p> <ul style="list-style-type: none"> • <i>gw-trunk</i>: Das Media Gateway wird als DDI-Client betrieben, aber als Trunk verwendet. Diese Einstellung dient zum Anschluss einer softwarebasierten IP-Telefonanlage von Swyx.
Registrar	<p>Nur für Trunk-Modus = <i>Aus</i>, <i>Client</i> und <i>gw-trunk</i>. Tragen Sie die IP-Adresse oder den Domännennamen (FQDN) des SIP Registrars ein. Maximale Zeichenzahl ist 40.</p> <p>Einträge mit Leerzeichen sind nicht erlaubt.</p>
SIP-Endpunkt-IP-Adresse	<p>Nur für Trunk-Modus = <i>Server</i> und Registrierung deaktiviert</p> <p>Tragen Sie die IP-Adresse oder den Domännennamen (FQDN) des SIP Proxy Servers ein.</p>
Ausgehender Proxy	<p>Nur für Trunk-Modus = <i>Aus</i>, <i>Client</i> oder <i>gw-trunk</i></p> <p>Geben Sie den Namen oder die IP-Adresse des SIP Outbound Proxy Servers ein.</p> <p>Maximal können 32 Zeichen eingegeben werden.</p> <p>Hier müssen Sie nur dann einen Eintrag vornehmen, wenn bei allen SIP Sessions die Kommunikation nicht direkt sondern über einen weiteren Proxy erfolgen soll.</p> <p>Im SIP Client Modus: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dies explizit vom Provider vorgegeben wird.</p>
Realm	<p>Tragen Sie einen weiteren Domännennamen oder eine weitere IP-Adresse des SIP Proxy Servers ein.</p> <p>Wenn Sie keine Angaben machen, wird der Eintrag im Feld Registrar verwendet.</p> <p>Im SIP Client Modus: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dieser explizit vom Provider vorgegeben wird.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches zum Datentransport verwendet werden soll.</p>

Feld	Beschreibung
	<p>Mögliche Werte: <i>UDP</i> (Standardwert) oder <i>TCP</i></p> <p>Geben Sie den Port ein, über den die Daten transportiert werden sollen.</p> <p>Der Standardwert ist <i>5060</i>.</p> <p>Im SIP Client Modus: Die Ports können Provider-spezifisch sein.</p>
Benutzername	<p>Im SIP Client Modus: Tragen Sie hier den Benutzernamen für die Authentifizierung ein, wenn Ihnen Ihr VoIP-Provider einen solchen zugewiesen hat.</p> <p>Im SIP Server Modus: Sie müssen den Benutzernamen festlegen.</p> <p>Maximal können 40 Zeichen eingegeben werden.</p>
Authentifizierungs-ID	<p>Tragen Sie einen Namen ein, der zur Authentifizierung beim Outbound Proxy verwendet wird.</p> <p>Wenn Sie keinen Namen eingeben, wird der Name im Feld Benutzername verwendet.</p> <p>Im SIP Client Modus: Tragen Sie nur dann einen Namen ein, wenn dieser explizit vom Provider vorgegeben wird.</p>
Passwort	<p>Im SIP Client Modus: Der VoIP-Provider weist Ihnen eine PIN bzw. Passwort für die Authentifizierung zu. Diesen Wert müssen Sie hier eingeben.</p> <p>Im SIP Server Modus: Legen Sie eine PIN bzw. ein Passwort fest.</p> <p>Maximal können 40 Zeichen eingegeben werden.</p>
Registrierung	<p>Wählen Sie aus, ob der Registrierungsmechanismus per SIP REGISTER Meldung benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.</p>

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Abgesehen von diesem Standard-Vorgehen können die relevanten Daten auch an eine bestimmte IP-Adresse geschickt werden, die den Verbindungspartnern bereits bekannt ist. Dann entfallen Registrierung und Authentisierung, in diesem Fall muss die Funktion Registrierung deaktiviert sein. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP.</p>
Gültigkeit	<p>Nur wenn Registrierung aktiviert ist.</p> <p>Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird.</p> <p>Zur Verfügung stehen Werte von <i>0</i> bis <i>38400</i>.</p> <p>Der Standardwert ist <i>600</i>.</p> <p>Ein Server kann in seiner Antwort auf eine REGISTER Anfrage eine andere Gültigkeit festlegen, welche die hier festgelegte überschreibt.</p>
Angerufene Adresse	<p>Legt fest, aus welchem Parameter der angerufenen Adresse die Rufnummer extrahiert wird.</p> <p>Die angerufene Adresse hat folgendes Format: Adresse = "Anzeige" <Benutzer>, z. B. "+49911987543" <sip:+49911987543@tel.telekom.de></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Extrahiert die Rufnummer aus dem ersten Teil der Adresse. Wenn dies fehlschlägt, wird die Rufnummer aus dem zweiten Teil der Adresse extrahiert. • <i>Benutzer</i>: Extrahiert die Rufnummer aus dem zweiten Teil der Adresse, z. B. aus <sip:+49911987543@tel.telekom.de>. • <i>Anzeige</i>: Extrahiert die Rufnummer aus dem ersten Teil der Adresse, z. B. aus "+49911987543".

Felder im Menü Trunk-Einstellungen

Feld	Beschreibung
SIP-Header-Feld(er) für Anruferadresse	<p>Nur für Trunk-Modus = <i>Client</i>, <i>Server</i> oder <i>gw-trunk</i></p> <p>Wählen Sie für ausgehende Rufe die Position der Absender-ID (z.B. Rufnummer) im SIP-Header aus. (Bei eingehenden Rufen wird automatisch die Rufnummer aus dem SIP Header ermittelt.)</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i> (Standardwert): Die Absender-ID wird nicht übertragen. • <i>Anzeige und Benutzername</i>: Die Absender-ID wird im SIP Header im Feld "Display" und im Feld "User" übertragen. • <i>Nur Anzeige</i>: Die Absender-ID wird im SIP Header im Feld "Display" übertragen. • <i>Nur Benutzer</i>: Die Absender-ID wird im SIP Header im Feld "User" übertragen. • <i>P-Preferred</i>: Der SIP Header wird durch das sogenannte "p-preferred-identity" Feld erweitert, um dort die Absender-ID zu übertragen. • <i>P-Asserted</i>: Der SIP Header wird durch das sogenannte "p-asserted-identity" Feld erweitert, um dort die Absender-ID zu übertragen.
Rufnummer	<p>Nur für Trunk-Modus = <i>Server</i></p> <p>Sie können eine Nummer setzen, die bei ausgehenden Rufen der Absenderrufnummer als Prefix vorangestellt wird und bei eingehenden Rufen von den führenden Stellen der Zielrufnummer abgeschnitten wird. Das entspricht der Rumpfnr einer TK-Anlage.</p>

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Reihenfolge	<p>Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich. • <i>Qualität</i>: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • <i>Geringe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • <i>Hohe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.
Sortierreihenfolge	<p>Wählen sie die Codecs aus, die für die Verbindung vorgeschlagen werden sollen. Abhängig von der Einstellung im Feld Codec-Reihenfolge werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>G. 711 uLaw</i>: ISDN Codec nach US Kennlinie • <i>G. 711 aLaw</i>: ISDN Codec nach EU Kennlinie • <i>G. 729</i>: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • <i>G. 726-40</i>: Komprimiert von 63 auf 40 KBit/s • <i>G. 726-32</i>: Komprimiert von 55 auf 32 KBit/s • <i>G. 726-24</i>: Komprimiert von 47 auf 24 KBit/s • <i>G. 726-16</i>: Komprimiert von 39 auf 16 KBit/s • <i>DTMF Outband</i>: DTMF Outband. Zuerst wird versucht RFC 2833 zu verwenden. Wenn die Gegenstelle diesen Standard nicht "beherrscht", wird SIP Info verwendet. • <i>T. 38 Fax</i>: Ermöglicht den Versand von Faxmitteilungen über Datennetzwerke. • <i>SRTP</i>: SRTP ist eine verschlüsselte Variante des Real-Time Transport Protokolls (RTP). • <i>Daten (RFC 4040)</i>: Ermöglicht den Transport eines 64-kbit/s-Datenstroms in RTP-Paketen. <p>Standardmäßig sind <i>G. 711 uLaw</i>, <i>G. 711 aLaw</i> und <i>G. 729</i> aktiviert.</p> <p>Die tatsächlich verwendeten Codecs sind die Schnittmenge der hier festgelegten und der vom Provider signalisierten Codecs.</p>

Feld	Beschreibung
	Von diesen Codecs fallen bei ausgehenden Rufen noch diejenigen weg, welche mehr als die verfügbare Bandbreite benötigen würden.

Felder im Menü Sprachqualitätseinstellungen

Feld	Beschreibung
Echounterdrückung	<p>Wählen Sie aus, ob Echounterdrückung verwendet werden soll.</p> <p>Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Comfort Noise Generation (CNG)	<p>Wählen Sie aus, ob Comfort Noise Generation (CNG) verwendet werden soll.</p> <p>Bei digitaler Sprachübertragung sorgt dieses Verfahren durch das Erzeugen eines leichten Hintergrundrauschens dafür, dass während Gesprächspausen beim Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Paketgröße	<p>Geben Sie an, wieviel Millisekunden Sprache ein RTP-Datenpaket enthält.</p> <p>Zur Verfügung stehen Werte von 5 bis 500.</p> <p>Der Standardwert ist 20.</p>

15.1.3 Standorte

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

Zur Verwendung des Bandbreitenmanagements können einzelne Standorte eingerichtet werden. Ein Standort wird anhand seiner festen IP-Adresse bzw. DynDNS-Adresse oder


mittels der Schnittstelle, an der das Gerät angeschlossen ist, identifiziert. Für jeden Standort kann die verfügbare VoIP-Bandbreite (Up- und Downstream) eingestellt werden.

Nur für Kompaktsysteme: Ein vordefinierter Eintrag mit den Parametern **Beschreibung** = LAN, **Beinhalteter Standort (Parent)** = Keiner, **Typ** = Schnittstellen, **Schnittstellen** = LAN_EN1-0 wird angezeigt.

Felder im Menü Registrierungsverhalten für VoIP-Teilnehmer ohne definierten Standort

Feld	Beschreibung
Standardverhalten	<p>Legen Sie fest, wie das System bei der Registrierung von VoIP-Teilnehmern verfahren soll, für die kein Standort definiert wurde.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Registrierung nur in privaten Netzwerken</i> (Standardwert): Der VoIP-Teilnehmer wird nur registriert, wenn er sich innerhalb des privaten Netzwerks befindet. • <i>Nicht erlaubt</i>: Der VoIP-Teilnehmer wird nie registriert. • <i>Uneingeschränkte Registrierung</i>: Der VoIP-Teilnehmer wird immer registriert.

15.1.3.1 Bearbeiten oder Neu

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie die Beschreibung des Eintrags ein.
Beinhalteter Standort (Parent)	Sie können die SIP-Standorte beliebig kaskadieren. Definieren Sie hier, welcher schon definierte SIP-Standort für den hier zu konfigurierenden SIP-Standort den übergeordneten Knoten bildet.
Typ	Wählen Sie aus, ob der Standort mittels IP-Adressen/DNS-Namen oder Schnittstellen definiert werden soll.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Adressen</i> (Standardwert): Der SIP-Standort wird über IP-Adressen bzw. DNS-Namen definiert. • <i>Schnittstellen</i>: Der SIP-Standort wird über die verfügbaren Schnittstellen definiert.
Adressen	<p>Nur für Typ = <i>Adressen</i></p> <p>Geben Sie die IP-Adressen der Geräte an den SIP-Standorten ein.</p> <p>Klicken Sie auf Hinzufügen um neue Adressen zu konfigurieren.</p> <p>Geben Sie unter IP-Adresse/DNS-Name die gewünschte IP-Adresse bzw. den DNS-Namen ein.</p> <p>Geben Sie ebenfalls die erforderliche Netzmaske ein.</p>
Schnittstellen	<p>Nur für Typ = <i>Schnittstellen</i></p> <p>Geben Sie die Schnittstellen an, an denen die Geräte eines SIP-Standorts angeschlossen sind.</p> <p>Klicken Sie auf Hinzufügen, um neue Schnittstelle auszuwählen.</p> <p>Wählen Sie unter Schnittstelle die gewünschte Schnittstelle aus.</p>
Bandbreitenbegrenzung Upstream	<p>Legen Sie fest, ob die Upstream-Bandbreite begrenzt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Bandbreite reduziert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upstream-Bandbreite	<p>Geben Sie die maximale Datenrate in Senderichtung in kBits pro Sekunde ein.</p>
Bandbreitenbegrenzung Downstream	<p>Legen Sie fest, ob die Downstream-Bandbreite begrenzt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Bandbreite reduziert.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Maximale Down-stream-Bandbreite	Geben Sie die maximale Datenrate in Empfangsrichtung in kBits pro Sekunde ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
DSCP-Einstellungen für RTP-Daten	<p>Wählen Sie die Art des Dienstes für RTP-Daten aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DSCP-Binärwert</i> (Standardwert): Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). Der vorkonfigurierte Wert ist <code>101110</code> • <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.

15.1.4 ISDN-Trunks

Für die Konfiguration im Menü **ISDN-Trunks** muss Ihr Gerät über mindestens zwei ISDN-Anschlüsse im Punkt-zu-Punkt-Modus (BRI oder PRI) verfügen, die als TE (Sammelanschluss) oder NT konfiguriert sind.




Hinweis

Beachten Sie, dass bei BRI-Anschlüssen der Anschlussmodus (NT Mode oder TE Mode) per Jumper im Gerät umgeschaltet werden muss.

In diesem Menü werden ISDN-Sammelanschlüsse (Bundles) festgelegt.

15.1.4.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Sammelanschlusses ein. Maximale Zeichenzahl ist 40.
ISDN-Modus	Wählen Sie den Modus aus, in welchem der Sammelanschluss betrieben wird. Mögliche Werte: <ul style="list-style-type: none"> • <i>Extern</i> (Standardwert): Punkt-zu-Punkt TE-Anschluss (Telekom Sammelanschluss) • <i>Trunk</i>: Punkt-zu-Punkt NT-Anschluss (für den Anschluss einer TK-Anlage).
Mitglieder	Wählen Sie die gewünschten ISDN-Schnittstellen aus, die zu diesem Sammelanschluss gehören sollen. Sie können diejenigen ISDN-Schnittstellen auswählen, die im Punkt-zu-Punkt-Modus konfiguriert sind.

15.1.5 Optionen

Im Menü **VoIP->Einstellungen->Optionen** können Sie globale Einstellungen für das Media Gateway vornehmen.

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


Felder im Menü Basisparameter

Feld	Beschreibung
Status des Media Gateways	<p>Wählen Sie aus, ob die Funktion Media Gateway aktiviert sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Session Border Controller Modus	<p>Wählen Sie aus, wie sich das Media Gateway in Verbindung mit einem Session Border Controller verhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Die Anrufkontrolle wird für alle Nebenstellen, die mit einem existierenden SIP-Konto exakt übereinstimmen, vom Session Border Controller durchgeführt, d.h. alle SIP-Meldungen, die für das entsprechende SIP-Konto konfiguriert sind, werden an den Session Border Controller weitergeleitet. Für alle anderen Nebenstellen wird die Anrufkontrolle vom Media Gateway entsprechend der unter Anrufkontrolle konfigurierten Einträge durchgeführt. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup). • <i>Aus</i>: Die Anrufkontrolle wird ausschließlich vom Media Gateway entsprechend der unter Anrufkontrolle konfigurierten Einträge und der lokalen Nebenstellen durchgeführt. Für Rufe, die über einen bestimmten Provider (SIP-Konto) geroutet werden sollen, müssen Sie einen entsprechenden Anrufkontrolle-Eintrag konfigurieren. Interne Rufe (von interner Nebenstelle zu interner Nebenstelle), die nur lokal geroutet werden müssen, benötigen keinen zusätzlichen Anrufkontrolle-Eintrag. • <i><SIP Trunk></i>: Wählen Sie ein unter VoIP->Einstellungen->SIP-Konten konfiguriertes SIP Trunk Konto aus. Die Anrufkontrolle wird in diesem Fall für alle Nebenstellen vom Session Border Controller ausgeführt, alle SIP-Meldungen werden an den Session Border Controller weitergeleitet. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup).

Feld	Beschreibung
	Hinweis: Einträge in Anrufkontrolle haben Vorrang vor der Session Border Controller Konfiguration!
Anrufkontrolle für lokale Nummern	<p>Legen Sie fest, ob Routing-Einträge vor Durchwahlnummern favorisiert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Media Stream Termination	<p>Wählen Sie aus, wie RTP-Sessions vom System kontrolliert werden sollen.</p> <p>Wenn die Funktion aktiv ist, werden die RTP-Sessions auf dem Media Gateway terminiert, d.h. alle RTP Streams werden vom Media Gateway kontrolliert und über das Media Gateway geroutet. Die beteiligten Endgeräte (z. B. SIP-Telefone) sind nicht direkt miteinander verbunden. Beachten Sie, dass das Media Gateway bei VoIP-zu-VoIP-Verbindungen unterschiedliche Codecs der beteiligten VoIP-Endgeräte nicht übersetzt. Daher müssen die Codecs von Media Gateway und VoIP-Endgeräten übereinstimmen.</p> <p>Wenn die Funktion nicht aktiv ist, werden die RTP-Sessions nicht auf dem Media Gateway terminiert, d.h. alle RTP Streams werden ohne Terminierung vom Media Gateway geroutet. Die RTP-Datenpakete können in komplexen Netzen somit auch über andere Gateways gerouted werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Standard-Abwurfnebenstelle	Sie können eine Nebenstelle angeben, zu der eingehende Telefonate geleitet werden, die keiner Extension oder angeschlossenen TK-Anlage zugeordnet werden können.
Wahlpause	<p>Geben Sie die maximale Verzögerungszeit ein bis das System die eingegebene Telefonnummer als vollständig wertet und der SIP-Wählvorgang (Senden der SIP INVITE Message) startet. Diese Zeitspanne wird mit jedem Tastendruck zurückgesetzt.</p> <p>Mögliche Werte sind 0 bis 15.</p>

Feld	Beschreibung
	<p>Der Standardwert ist 5.</p> <p>Wenn Sie die Rufnummer mit # abschließen, wird sofort gewählt.</p>

Felder im Menü SIP-Provider-Einstellungen

Feld	Beschreibung
DSCP-Einstellungen für SIP-Daten	<p>Wählen Sie die Art des Dienstes für SIP-Daten aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DSCP-Binärwert</i> (Standardwert): Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). Der Standardwert ist <i>101110</i>. • <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.
SIP Port	<p>Geben Sie den Port an, über den die SIP-Daten geleitet werden sollen.</p> <p>Standardmäßig ist der Wert <i>5060</i> vorgegeben.</p>
	<p> Hinweis</p> <p>Falls Sie den Port im laufenden Betrieb ändern, wird die Änderung erst nach dem nächsten Neustart der Anlage wirksam.</p>

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
ISDN Anrufsignalisierung	<p>tbw ...</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard: Immer als unbekannte Nummer</i> • <i>Spezifisch: International, National oder Teilnehmer</i>
Kurzwahl	<p>Definieren Sie kurze Ziffernfolgen, die anstatt der kompletten Nummer gewählt werden können.</p> <p>Klicken Sie auf Hinzufügen um neue Kurzwahlen zu konfigurieren.</p> <p>Geben Sie unter Abkürzung die gewünschte Kurzwahl für den Benutzer ein, z. B. <i>123</i>.</p> <p>Geben Sie unter Ersetzen durch die Rufnummer ein, welche anstelle der Kurzwahl gewählt werden soll, z. B. <i>09119673</i>.</p> <p>Wenn in obigem Beispiel ein Benutzer <i>*123</i> eintippt, wählt das Gerät <i>09119673</i>.</p> <p>Möchte der Benutzer die Nebenstelle <i>111</i> erreichen, so tippt er <i>*123111</i> ein. Das Gerät wählt <i>09119673111</i>.</p> <p>Ein Punkt am Ende der Nummer zeigt eine komplette Nummer an. Diese wird nach dem Einsetzen sofort gewählt.</p>

Wenn Sie eine Kurzwahl aus dieser Liste nutzen wollen, müssen Sie * und dann die Kurzwahl wählen.

15.2 Media Gateway

Ein Media Gateway dient als Übersetzungsinstanz zwischen verschiedenen Telekommunikationsnetzen wie z. B. zwischen dem herkömmlichen Telefonnetz und den Next Generation Networks (IP-Netzwerken).

Mit dem bintec elmeg Media Gateway kann ein Unternehmen, das mit einer durchwahlfähigen Telefonanlage an einem leitungsvermittelten Telefonnetz ausgestattet ist, mit einem SIP Trunking Service Provider im Internet verbunden werden und somit IP-Telefonie nutzen.

Das bintec elmeg Media Gateway unterstützt die Anbindung mehrerer SIP Provider Accounts. Sie können mit diesem Gateway Nebenstellen einrichten, einen Rufnummernplan anlegen und Telefonanlagen-Funktionen konfigurieren sowie die Sprachdaten-Übertragung bei geringer Bandbreite der Upload-Verbindung optimieren.



Hinweis


Ihr Gerät muss mit einem DSP-Modul ausgestattet sein, um die Media Gateway Funktionen nutzen zu können. Informationen zum Einbau des DSP-Moduls finden Sie in der Einbauanleitung, die dem Modul beiliegt.

15.2.1 Anrufkontrolle

Hier können Sie die Bedingungen für das Weiterleiten von Anrufen (Routing) festlegen. Sie legen hier eine Liste mit Regeln oder Regelketten fest, die dazu dienen, die signalisierte Zielrufnummer zu manipulieren.

Im Menü **VoIP->Media Gateway->Anrufkontrolle** wird eine Liste aller vorhandenen Einträge angezeigt.

15.2.1.1 Bearbeiten oder Neu

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

Das Menü **VoIP->Media Gateway->Anrufkontrolle->  ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Eintrags ein.
Administrativer Status	Wählen Sie aus, ob der Eintrag aktiv sein soll. Mit <i>Aktivieren</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Typ	Wählen Sie aus, wie der Ruf weitergeleitet werden soll. Mögliche Werte:

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Erlauben</i>: Für Rufe, die vom Media Gateway an eine Telefonanlage oder einen ISDN-TE-Anschluss oder einen SIP DDI Client weitergeleitet werden sollen. Dazu können verwendet werden: PRI-Schnittstellen im NT-Modus, BRI-Schnittstellen im NT-Modus, SIP-Konten im Trunk-Modus (Server Modus) . • <i>Verweigern</i>: Für Rufe, die nicht weitergeleitet (gesperrt) werden sollen.
Anrufende Leitung	<p>Sie können die Anwendung des Eintrags auf die Leitung begrenzen, auf welcher der Ruf ankommt.</p> <p>Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP-Konten ab.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>pri<Schnittstellen-Index></i>: Begrenzt den Routing-Eintrag auf die gewählte PRI-Schnittstelle. • <i>bri<Schnittstellen-Index></i>: Begrenzt den Routing-Eintrag auf die gewählte BRI-Schnittstelle. • <i><SIP-Konto></i>: Begrenzt den Routing-Eintrag auf das gewählte SIP-Konto. • <i>Beliebig</i>: Keine Begrenzung des Eintrags.
Anrufende Adresse	<p>Sie können die Anwendung des Eintrags auf einen bestimmten Anrufer begrenzen. Dazu müssen Sie die Rufnummer exakt angeben (keine Wildcards).</p>
Angerufene Adresse	<p>Geben Sie die angerufene Adresse ein, auf die die Regel angewendet werden soll.</p> <p>Dazu geben Sie eine Adresse numerisch (z. B. eine Rufnummer) oder alphanumerisch (z. B. für einen Trunk) ein, die mit der gewählten Adresse verglichen wird.</p> <p>Dabei können Sie folgende Wildcards verwenden:</p> <ul style="list-style-type: none"> • * bedeutet, dass am Ende einer Zeichenfolge beliebige weitere Zeichen folgen können. • ? dient als Platzhalter für ein beliebiges Zeichen. <p>Wenn die konfigurierte Adresse mit der signalisierten Adresse übereinstimmt, wird der Eintrag angewandt.</p>

Im Bereich **Routing-Regeln** definieren Sie Regeln, die bestimmen, wie die Rufnummer manipuliert wird, bevor sie für den Wahlvorgang verwendet wird.

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

Felder im Menü **Routing-Regeln** (Nur für Typ = Erlauben)

Feld	Beschreibung
Priorität	<p>Geben Sie eine ganze Zahl beginnend mit 1 in aufsteigender Reihenfolge ein, um die Reihenfolge der Filterregeln festzulegen.</p> <p>Die Regeln werden in der Liste in der angegebenen Reihenfolge "abgearbeitet".</p> <p>Ist eine Leitung bzw. ein SIP-Konto nicht verfügbar, wird automatisch die nächste Regel verwendet.</p>
Administrativer Status	<p>Wählen Sie aus, ob die Regel aktiv sein soll.</p> <p>Mit <i>Aktivieren</i> wird die Regel aktiv.</p> <p>Standardmäßig ist die Regel aktiv.</p>
Leitung	<p>Wählen Sie die ISDN-Leitung (PRI, BRI) oder das SIP-Konto für den ausgehenden Ruf aus.</p>
Transformation der gerufenen Adresse	<p>Geben Sie ein, wie die Rufnummer manipuliert werden soll, bevor sie für den Wahlvorgang verwendet wird.</p> <p>Notation: <a:b>; d.h. a wird durch b ersetzt. Jede Regel muss durch einen Strichpunkt abgeschlossen sein. Mehrere Regeln können zu einer Regelkette zusammengefasst werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>;. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert.</p> <p>Numerische und alphanumerische Werte sind zulässig.</p> <p>? dient als Platzhalter für ein beliebiges Zeichen.</p>


Feld	Beschreibung
	<p>Beispiel 15.1. Beispiel für eine Regel</p> <ul style="list-style-type: none"> • Regel: <:+49911>; • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

15.2.2 CLID-Umwandlung

Hier legen Sie die Bearbeitung der Rufnummer des Anrufers (Calling Party Number) bei eingehenden Anrufen fest. Sie können z. B. zu einer empfangenen Telefonnummer einen Prefix hinzufügen, um entsprechende ausgehende Gespräche über ein bestimmtes SIP-Konto zu routen.

Im Menü **VoIP->Media Gateway->CLID-Umwandlung** wird eine Liste aller vorhandenen Einträge angezeigt, bei denen die empfangene Rufnummer bearbeitet wird.

15.2.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Einträge für CLID-Umwandlung hinzuzufügen.

Das Menü **VoIP->Media Gateway->CLID-Umwandlung->  ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Eintrags ein.
Rufnummer	<p>Wählen Sie die ISDN-Leitung oder das SIP-Konto, von welcher bzw. von welchem der Anruf kommt.</p> <p>Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP-Konten ab.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>pri</i><Schnittstellen-Index>: Begrenzt den Eintrag auf die gewählte PRI-Schnittstelle. • <i>bri</i><Schnittstellen-Index>: Begrenzt den Eintrag auf

Feld	Beschreibung
	<p>die gewählte BRI-Schnittstelle.</p> <ul style="list-style-type: none"> • <i><SIP-Konto></i>: Begrenzt den Eintrag auf das gewählte SIP-Konto. • <i>Beliebig</i>: Keine Begrenzung des Eintrags.
Angerufene Leitung	<p>Sie können optional die Zielleitung des Anrufs angeben.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>pri<Schnittstellen-Index></i>: Begrenzt den Eintrag auf die gewählte PRI-Schnittstelle. • <i>bri<Schnittstellen-Index></i>: Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • <i><SIP-Konto></i>: Begrenzt den Eintrag auf das gewählte SIP-Konto. • <i>Beliebig</i>: Keine Begrenzung des Eintrags. <p>Geben Sie entweder Angerufene Leitung oder Angerufene Adresse ein.</p> <p>Wird ein Wert gewählt, der nicht <i>Beliebig</i> ist, so sollte Angerufene Adresse nicht benutzt werden. Ist Angerufene Leitung = <i>Beliebig</i> gesetzt und wird Angerufene Adresse nicht benutzt, so werden alle Anrufe für Angerufene Leitung behandelt.</p>
Angerufene Adresse	<p>Sie können optional die Zieladresse des Anrufs angeben.</p> <p>Geben Sie entweder Angerufene Leitung oder Angerufene Adresse ein. Wird Angerufene Adresse benutzt, so sollte Angerufene Leitung = <i>Beliebig</i> gesetzt sein.</p>
Transformation der rufenden Adresse	<p>Geben Sie die Transformationsregel an, die auf die Rufnummer angewendet werden soll.</p> <p>Notation: <a:b>; d.h. a wird durch b ersetzt. Jede Regel muss durch einen Strichpunkt abgeschlossen werden. Mehrere Regeln können zu einer Regelkette zusammengefaßt werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>;. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert.</p> <p>? dient als Platzhalter für eine beliebige Ziffer.</p>

Feld	Beschreibung
	<p>Beispiel 15.2. Beispiel für eine Regel</p> <ul style="list-style-type: none"> • Regel: <:+49911>; • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

15.2.3 Rufnummertransformation

Hier können Sie eine Liste zum Umsetzen von Rufnummern erstellen, d.h. in dieser Liste werden externe und interne Nummern einander zugeordnet.




Hinweis

Welche Rufnummer (Called Party Number oder Calling Party Number) umgesetzt wird, hängt von der Richtung (eingehend oder ausgehend) des jeweiligen Rufs ab. Bei eingehenden Rufen wird die Called Party Number, bei ausgehenden Rufen die Calling Party Number umgesetzt.

Sie können z. B. die interne Rufnummer 340 nach außen als 09119673900 darstellen oder einen Ruf von außen, der an die Nummer 09119673200 gehen soll, intern an die Nummer 340 weiterleiten.

Im Menü **VoIP->Media Gateway->Rufnummertransformation** wird eine Liste vorhandenen Transformationen angezeigt.

15.2.3.1 Bearbeiten oder Neu

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

Das Menü **VoIP->Media Gateway->Rufnummertransformation->  ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen der Rufnummertransformation ein.

Feld	Beschreibung
Richtung	<p>Wählen Sie die Rufrichtung für den Eintrag.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): Für eingehende und ausgehende Rufe (bidirektional). • <i>Eingehend</i>: Für eingehende Rufe. • <i>Ausgehend</i>: Für ausgehende Rufe.
Zugeordnete Leitung	<p>Wählen Sie die ISDN-Leitung oder das SIP-Konto, über die bzw. über das Rufe geleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>pri<Schnittstellen-Index></i>: Begrenzt den Ruf auf die gewählte PRI-Schnittstelle. • <i>bri<Schnittstellen-Index></i>: Begrenzt den Ruf auf die gewählte BRI-Schnittstelle. • <i><SIP-Konto></i>: Begrenzt den Ruf auf das gewählte SIP-Konto.
Lokale Adresse	<p>Geben Sie die interne Rufnummer (z. B. Nummer einer Nebenstelle oder TK-Anlage) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld Externe Adresse) auf die Lokale Adresse umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld Lokale Adresse) auf die Externe Adresse umgesetzt.</p> <p>Numerische und alphanumerische Zeichen sind zulässig.</p> <p>? dient als Platzhalter für eine beliebige Ziffer.</p> <p>Beachten Sie, dass Lokale Adresse und Externe Adresse dieselbe Anzahl von Wildcards enthalten müssen.</p>
Externe Adresse	<p>Geben Sie die externe Rufnummer (z. B. ISDN MSN oder die Rufnummer des SIP-Kontos) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld Externe Adresse) auf die Lokale Adresse umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld Lokale Adresse) auf die Externe Adresse umgesetzt.</p>

Feld	Beschreibung
	<p>Das Feld Externe Adresse ist nicht sichtbar, wenn das Feld Zugeordnete Leitung = <i><SIP-Konto></i> gesetzt ist. Als Externe Adresse wird in diesem Fall wird der Benutzername des gewählten SIP-Kontos verwendet.</p>

Kapitel 16 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)
- 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
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)
- Ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten (Wake-On-LAN)
- Eine Aufzeichnung des Datenverkehrs über eine bestimmte Schnittstelle (Trace-Schnittstelle)

16.1 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.

16.1.1 Globale Einstellungen

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
WINS-Server Primär Sekundär	Geben Sie die IP-Adresse des ersten und, falls erforderlich, des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Negativer Cache	Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Cache-Größe	Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein. Wird dieser Wert erreicht, wird bei einem neu hinzukommenden

Feld	Beschreibung
	<p>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>Der 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>Der 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>Der Standardwert ist <i>86400</i>.</p>
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>Der 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>Keiner</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.

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

16.1.2 DNS-Server

Im Menü **Lokale Dienste->DNS->DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

16.1.2.1 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.

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<p>Wählen Sie aus, ob der DNS-Server aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.
Priorität	<p>Weisen Sie dem DNS-Server eine Priorität zu.</p> <p>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 Priorität, wenn die Schnittstelle im Zustand "up" ist.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 9 (niedrigste Priorität).</p> <p>Der 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>
IP-Version	<p>Wählen Sie die verwendete IP-Version aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IPv4</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IPv6</i> <p>Standardmäßig ist <i>IPv4</i> ausgewählt.</p>
Primärer IPv4-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie die IPv4-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer IPv4-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie optional die IPv4-Adresse eines alternativen Name-Servers ein.</p>
Primärer IPv6-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie die IPv6-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer IPv6-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie optional die IPv6-Adresse eines alternativen Name-Servers ein.</p>

16.1.3 Statische Hosts

Im Menü **Lokale Dienste->DNS->Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

16.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü BasisparameterStandarddomäne

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>

Feld	Beschreibung
	<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. • <i>Keine</i>: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IPV4-Adresse	<p>Nur bei Antwort = <i>Positiv</i></p> <p>Geben Sie die IPv4-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>
IPv6-Adresse	<p>Nur bei Antwort = <i>Positiv</i></p> <p>Geben Sie die IPv6-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>

16.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste->DNS->Domänenweiterleitung** wird eine Liste aller konfigurierter Weiterleitungen für definierte Domänen angezeigt.

16.1.4.1 Neu

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

Das Menü **Lokale Dienste->DNS->Domänenweiterleitung->Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	<p>Wählen Sie aus, ob Anfragen bezüglich eines Hosts oder einer Domäne weitergeleitet 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> und Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie den Namen des Hosts ein, für den Anfragen weitergeleitet werden sollen.</p> <p>Bei Eingabe eines Namens ohne "." wird nach Bestätigung mit OK der Eintrag mit dem im Menü Lokale Dienste->DNS->Globale Einstellungen unter Domänenname eingetragenen Namen ergänzt.</p>
Domäne	<p>Nur für Weiterleiten = <i>Domäne</i> und Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie den Namen der Domäne ein, für die Anfragen weitergeleitet werden sollen.</p> <p>Der Eintrag kann mit der Wildcard "*" beginnen, z. B. "*.mustermann.lan".</p> <p>Bei Eingabe eines Namens ohne führende Wildcard "*" wird nach Bestätigung mit OK automatisch eine führende Wildcard "*" eingefügt.</p>
Weiterleiten an	<p>Wählen Sie aus, ob zutreffende DNS-Anfragen an den DNS-Server einer Schnittstelle oder an einen manuell konfigurierten DNS-Server weitergeleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnittstelle</i> (Standardwert): Anfragen werden an den DNS-Server entweder einer automatisch gewählten oder einer manuell konfigurierten Schnittstelle weitergeleitet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>DNS-Server</i>: Anfragen werden an den definierten DNS-Server weitergeleitet.
Schnittstelle	<p>Nur für Weiterleiten an = <i>Schnittstelle</i></p> <p>Wählen Sie die Schnittstelle aus, an deren DNS-Server Anfragen weitergeleitet werden sollen.</p>
Primärer DNS-Server (IPv4/IPv6)	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie die IPv4/IPv6-Adresse des primären DNS-Servers ein.</p>
Sekundärer DNS-Server (IPv4/IPv6)	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie IPv4/IPv6-Adresse des sekundären DNS-Servers ein.</p>

16.1.5 Dynamische Hosts

Im Menü **Lokale Dienste->DNS->Dynamische Hosts** sehen Sie die relevanten Angaben zu den Dynamischen DNS-Einträgen.

16.1.6 Cache

Im Menü **Lokale Dienste->DNS->Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

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.

16.1.7 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.

16.2 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.

16.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

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>Der 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 möchten. • <i><Zertifikatsname></i>: Wählen Sie ein unter Systemverwaltung->Zertifikate->Zertifikatsliste eingetragenes Zertifikat aus.

16.3 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.

16.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

16.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internet Service Providers).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	<p>Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind.</p> <p>Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden.</p> <p>Weitere DynDNS-Provider können im Menü Lokale Dienste->DynDNS-Client->DynDNS-Provider konfiguriert werden.</p> <p>Der Standardwert ist <i>DynDNS</i>.</p>
Aktualisierung aktivieren	Wählen Sie aus, ob der hier konfigurierte DynDNS-Eintrag aktiviert werden soll.

Feld	Beschreibung
	Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Mail-Exchanger (MX)	Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll. Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.
Wildcard	Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von Hostname zur aktuellen IP-Adresse von Schnittstelle aktiviert werden soll (Erweiterte Namensauflösung). Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

16.3.2 DynDNS-Provider

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

16.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

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.

Feld	Beschreibung
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	<p>Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist.</p> <p>Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.</p>
Port	<p>Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll.</p> <p>Erfragen Sie den entsprechenden Port bei Ihrem Provider.</p> <p>Der Standardwert ist <i>80</i>.</p>
Protokoll	<p>Wählen Sie eines der implementierten Protokolle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DynDNS</i> (Standardwert) • <i>Static DynDNS</i> • <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>Der Standardwert ist <i>300</i> Sekunden.</p>

16.4 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.

Konkrete Hinweise für die Konfiguration eines DHCP-Servers, eines DHCP-Clients oder eines DHCP-Relay-Servers (siehe auch [DHCP-Relay-Einstellungen](#) auf Seite 353) finden Sie am Ende des Kapitels unter [DHCP - Konfigurationsbeispiel](#) auf Seite 354.

16.4.1 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.

16.4.1.1 Bearbeiten oder Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevor-

Feld	Beschreibung
	zugt verwendet werden soll. Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

16.4.2 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 konfigurierten DHCP-Pools 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.

16.4.2.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, über welche die in IP-Adressbereich definierten Adressen an anfragende DHCP-Clients vergeben werden. Wenn eine DHCP-Anfrage über diese Schnittstelle eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.
IP-Poolname	Wählen Sie einen im Menü Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration konfigurierten

Feld	Beschreibung
	IP-Poolnamen aus.
Pool-Verwendung	<p>Wählen Sie aus, ob der DHCP-Pool für Anfragen von DHCP-Clients in einem direkt an die Schnittstelle angeschlossenen Ethernet verwendet werden soll oder für DHCP-Anfragen, die aus einem über Gateways erreichbaren Ethernet stammen und über eine DHCP-Relaisstation an Ihr Gerät weitergeleitet wurden.</p> <p>In letzterem Fall ist es möglich, einen IP-Adresspool für ein entfernt liegendes Netz zu verwenden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal</i> (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen aus einem direkt an die Schnittstelle angeschlossenen Ethernet verwendet. • <i>Relais</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus einem über Gateways erreichbaren Ethernet verwendet. • <i>Lokal/Relais</i>: Der DHCP-Pool kann für lokale und für weitergeleitete DHCP-Anfragen aus direkt angeschlossenen bzw. über Gateways erreichbaren Ethernets verwendet werden.

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


Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Gateway	<p>Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Router als Gateway verwenden</i> (Standardwert): Hier wird die für die Schnittstelle definierte IP-Adresse übertragen. • <i>Kein Gateway</i>: Hier wird keine IP-Adresse übermittelt. • <i>Angeben</i>: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	<p>Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll.</p> <p>Nachdem Lease Time abgelaufen ist, kann die Adresse durch</p>

Feld	Beschreibung
	<p>den Server neu vergeben werden.</p> <p>Der 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 Zeitserver ein, die dem Client übermittelt werden soll. • <i>DNS-Server</i>: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • <i>DNS-Domänenname</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. • <i>Vendor String</i>: Mit dieser Option können die Konfigurationsparameter (z. B. PIN und Access Point Name (APN) der SIM-Karte) übertragen werden. <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche Hinzufügen ein.</p>

Herstellergruppe

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	<p>Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Siemens</i> (Standardwert) • <i>Sonstige</i>
Provisioning-Server	<p>Nur für Hersteller auswählen = Siemens</p> <p>Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll.</p> <p>Für die Einstellung Hersteller auswählen = Siemens wird der Standardwert <i>sdlp</i> angezeigt.</p> <p>Sie können die IP-Adresse des gewünschten Servers ergänzen.</p>
Herstellerbeschreibung	<p>Nur für Hersteller auswählen = Sonstige</p> <p>Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.</p>
Benutzerdefinierte DHCP-Optionen	<p>Nur für Hersteller auswählen = Sonstige</p> <p>Fügen Sie mit Hinzufügen weitere Einträge hinzu.</p> <p>Sie können DHCP-Optionen hinzufügen.</p>

Vendor String

Gehen Sie im Menü **Lokale Dienste**->**DHCP-Server**->**DHCP-Konfiguration**->**Erweiterte Einstellungen** folgendermaßen vor, um die entsprechenden Parameter einzugeben:

Klicken Sie im Feld **DHCP-Optionen** auf die Schaltfläche **Hinzufügen** und wählen Sie **Option = Vendor String**. Klicken Sie auf die Schaltfläche , um den Eintrag zu bearbeiten.

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>Sonstige</i> (Standardwert) • <i>-bintec-</i>
APN	Nur für Hersteller auswählen = <i>-bintec-</i> Geben Sie den Access Point Namen (APN) der SIM-Karte ein.
PIN	Nur für Hersteller auswählen = <i>-bintec-</i> Geben Sie die PIN der SIM-Karte ein.
Herstellerbeschreibung	Nur für Hersteller auswählen = <i>Sonstige</i> Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Vendor Option String	Nur für Hersteller auswählen = <i>Sonstige</i> Geben Sie die Hersteller spezifischen Konfigurationsparameter ein.

16.4.3 IP/MAC-Bindung

Im Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.



Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration** IP-Adressbereiche konfiguriert wurden, und im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration** ein gültiger IP-Pool zugewiesen ist.

16.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

Das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen MAC-Adresse die IP-Adresse gebunden wird. Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.
IP-Adresse	Geben Sie die IP-Adresse ein, die der in MAC-Adresse angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in IP-Adresse angegebene IP-Adresse zugewiesen werden soll.

16.4.4 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.

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

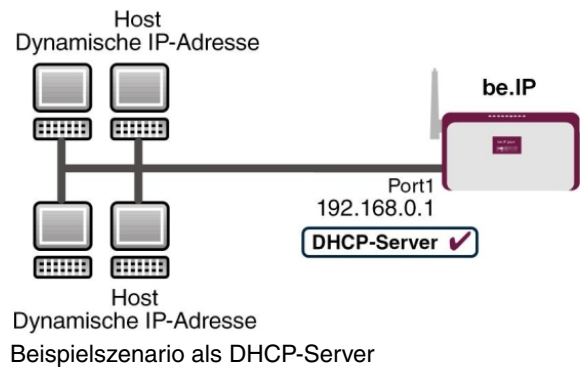
Feld	Beschreibung
Primärer DHCP-Server	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen. Der Standardwert ist <code>0.0.0.0</code> .
Sekundärer DHCP-Server	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein. Der Standardwert ist <code>0.0.0.0</code> .

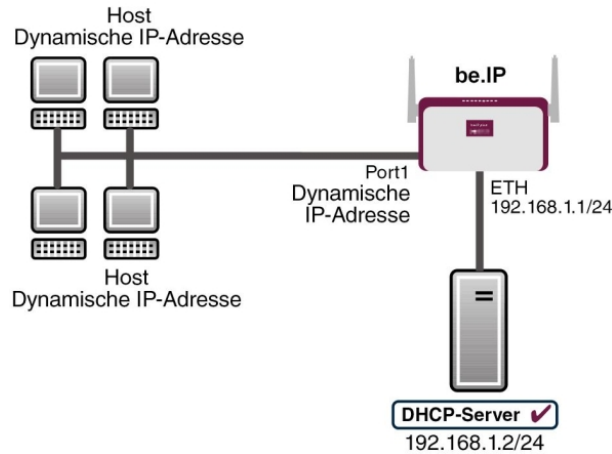
16.4.5 DHCP - Konfigurationsbeispiel

Voraussetzungen

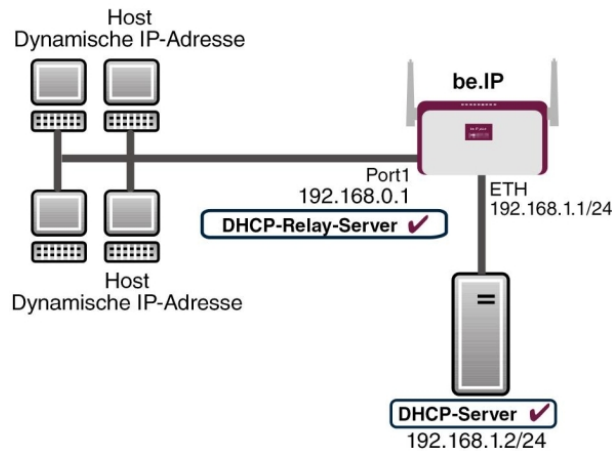
- Optional ein DHCP-Server

Beispiel-Szenarien





Beispielszenario als DHCP-Client



Beispielszenario als DHCP-Relay-Server

Konfigurationsziel

Sie können Ihr Gerät als DHCP-Server, als DHCP-Client oder als DHCP-Relay-Server einsetzen.



Konfigurationsschritte im Überblick

DHCP-Server

Feld	Menü	Wert
IP-Poolname	Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration ->Neu	z. B. <i>IP-Pool-1</i>
IP-Adressbereich	Lokale Dienste->DHCP-Server->IP-	z. B. <i>192.168.0.2</i> und

Feld	Menü	Wert
	Pool-Konfiguration ->Neu	192.168.0.10
Schnittstelle	Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu	z. B. en1-0
IP-Poolname	Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu	IP-Pool-1
Pool-Verwendung	Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu	Lokal
Gateway	Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu->Erweiterte Einstellungen	Router als Gateway verwenden
Lease Time	Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu->Erweiterte Einstellungen	z. B. 120
Für DNS- / WINS-Serverzuordnung zu verwendende IP-Adresse	Lokale Dienste->DNS->Globale Einstellungen->Erweiterte Einstellungen	z. B. Eigene IP-Adresse

DHCP-Client

Feld	Menü	Wert
Adressmodus	LAN->IP-Konfiguration->Schnittstellen-> <en1-4>-> 	DHCP
DHCP-MAC-Adresse (optional)	LAN->IP-Konfiguration->Schnittstellen-> <en1-4> ->  ->Erweiterte Einstellungen	MAC-Adresse eines bestimmten DHCP-Servers

DHCP-Relay-Server

Feld	Menü	Wert
Primärer DHCP-Server	Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen	z. B. 192.168.1.2
Sekundärer DHCP-Server (optional)	Lokale Dienste->DHCP-Server->DHCP-Re-	falls vorhanden

Feld	Menü	Wert
	lay-Einstellungen	

16.5 DHCPv6-Server

Sie können Ihr Gerät als DHCPv6-Server verwenden. Dieser DHCPv6-Server kann IP-Adressen und DHCP-Optionen an Clients verteilen oder auch nur DHCP-Optionen ohne Adressen. Diese Parameter werden in einem sogenannten "Option Set" zusammengefasst. Ein Option Set kann an eine Schnittstelle gebunden werden (siehe unter **Lokale Dienste->DHCPv6-Server->DHCPv6-Server->Neu**) oder es kann global konfiguriert werden (siehe unter **Lokale Dienste->DHCPv6-Server->Globale DHCPv6-Optionen->Neu**). DHCP-Optionen können zum Beispiel Informationen über DNS-Server oder Zeitserver enthalten.



Hinweis

Ein IPv6-Adress-Pool entsteht durch die Zuweisung eines IPv6-Link-Präfixes (Subnetz mit der Länge /64) zu einem DHCPv6 Option Set. Die Definition eines eigenen Abschnitts von IPv6-Adressen, wie z. B. fc00:1:2:3::1..fc00:1:2:3::100 ist anders als im DHCPv4 nicht vorgesehen.

Für die Konfiguration eines IPv6-Adress-Pools müssen folgende Voraussetzungen erfüllt sein:

- (a) IPv6 muss auf der betreffenden Schnittstelle aktiviert sein.
- (b) Ein IPv6-Link-Präfix (Subnetz) mit der Länge /64 muss auf der gewünschten Schnittstelle konfiguriert sein. Ein IPv6-Link-Präfix kann auf zwei Arten definiert sein:
 - Der IPv6-Link-Präfix ist von einem Allgemeinen IPv6-Präfix (Präfix mit einer Länge von zum Beispiel /56 oder /48) abgeleitet. In diesem Fall muss der Allgemeine IPv6-Präfix im Menü **Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes** konfiguriert sein.
 - Der IPv6-Link-Präfix mit Länge /64 wird manuell auf der entsprechenden Schnittstelle konfiguriert und nicht von einem Allgemeinen IPv6-Präfix abgeleitet.
- (c) Die Option **DHCP-Server** muss für die Schnittstelle aktiviert sein.


Darüber hinaus sind folgende Einstellungen empfehlenswert:

- Die Werte für die Optionen **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer** sollten auf Werte gesetzt werden, die größer sind als der Wert für **Router-Gültigkeitsdauer**.

Bei einer **Router-Gültigkeitsdauer** von 600 Sekunden, empfehlen sich z. B. eine **Bevor-**

zulte Gültigkeitsdauer von 900 Sekunden und eine **Gültigkeitsdauer** von 1800 Sekunden.

- Die Option **DHCP-Modus** sollte aktiviert sein.


Zur Einstellung der o.g. Optionen wählen Sie das Menü **LAN->IP-Konfiguration->Schnittstellen**. Mit dem Symbol  wählen Sie die gewünschte Schnittstelle. Aktivieren Sie IPv6 und setzen den **IPv6-Modus** auf *Router (Router-Advertisement übermitteln)*. Klicken Sie im Feld **IPv6-Adressen** auf **Hinzufügen** und konfigurieren Sie den Link-Präfix. Bestätigen Sie Ihre Konfiguration mit **Übernehmen**. Die Konfiguration der empfohlenen Einstellungen erfolgt dann in folgenden Menüs:

- **Router-Gültigkeitsdauer:** LAN->IP-Konfiguration->Schnittstellen->Neu->Erweiterte Einstellungen->Erweiterte IPv6-Einstellungen
- **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer:** LAN->IP-Konfiguration->Schnittstellen->Neu->Grundlegende IPv6-Parameter->Hinzufügen->Erweitert

16.5.1 DHCPv6-Server

Hier können Sie - bezogen auf eine Schnittstelle - in einem Option Set Adresspools anlegen und DHCP-Options definieren.


16.5.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Name	Geben Sie einen Namen für das Option Set ein.
Schnittstelle	<p>Wählen Sie die IPv6-Schnittstelle, an die das Option Set gebunden sein soll.</p> <p>Zur Auswahl stehen Schnittstellen mit folgender Konifguration:</p> <ul style="list-style-type: none"> • IPv6 ist aktiviert. • Die Option DHCP-Server ist aktiviert. <p>Im Auslieferungszustand ist IPv6 für alle Schnittstellen deakti-</p>

Feld	Beschreibung
	<p>viert. Erscheint die gewünschte Schnittstelle nicht in der Auswahl, konfigurieren Sie sie im Menü LAN->IP-Konfiguration->Schnittstellen gemäß den in der Einleitung genannten Vorgaben.</p>
Address assignment	<p>Die Definition eines IPv6-Adresspools erfolgt durch Zuweisung eines IPv6-Link-Präfixes (Subnetz mit Länge /64) zu einem DHCPv6 Option Set. Der IPv6-Adress-Pool umfasst immer den kompletten 64-Bit-Adressraum des gewählten IPv6-Link-Präfixes. Die Adressvergabe erfolgt zufällig.</p> <p>Mit Hinzufügen können Sie dem IPv6 Option Set einen oder mehrere IPv6-Link-Präfixe zuordnen.</p>
	<p> Hinweis</p> <p>Bitte beachten Sie, dass hier ausschließlich die IPv6-Link-Präfixe zur Auswahl stehen, die der gewählten Schnittstelle zugewiesen sind.</p>


Felder im Menü Server-Optionen

Feld	Beschreibung
DNS-Domänen-Suchliste	<p>Mit Hinzufügen können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt.</p>

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

Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
DNS-Server	<p>Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server").</p> <p>In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im</p>

Feld	Beschreibung
	<p>Feld DNS-Propagation im Menü LAN->IP-Konfiguration->Schnittstellen->  ->Erweiterte Einstellungen mit IPv6 = Aktiviert konfiguriert.)</p> <p>Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option RA oder globalen Fallback-DNS-Server verwenden und erstellen Sie mit Hinzufügen die gewünschten DNS-Server-Einträge.</p>
SNTP-Server	<p>Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit Hinzufügen können Sie die gewünschten Zeitserver-Einträge anlegen.</p>

16.5.2 Globale DHCPv6-Optionen

In diesem Menü können Sie die für den DHCPv6-Server global gültigen DHCPv6-Optionen konfigurieren. Eine hier konfigurierte Option wird immer dann propagiert, wenn für diese Option keine exaktere Definition (z.B. keine schnittstellenspezifische oder Vendor-ID-spezifische Definition) existiert.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DNS-Domänen-Suchliste	<p>Mit Hinzufügen können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt. Der Domain-Name (z. B. dev.bintec.de.) muss mit Punkt (.) enden.</p>


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

Felder im Menü Server-Priorität

Feld	Beschreibung
Server-Priorität	<p>In den vom DHCPv6 Server an die Clients gesendeten DHCPv6 Advertisements kann die DHCPv6-Option 7 Preference enthal-</p>

Feld	Beschreibung
	<p>ten sein.</p> <p>Mögliche Werte sind $0 \dots 255$. In einem Netzwerk mit mehreren DHCPv6 Servern wird über diese Option gesteuert, welcher DHCPv6-Server im Netzwerk die höchste Priorität besitzt. Empfängt ein Client DHCPv6 Advertisements mit unterschiedlicher Priorität von verschiedenen Servern, so wird der Client in der Regel die Werte des Servers mit der höchsten Priorität übernehmen. Der Client kann jedoch auch DHCPv6 Advertisements mit niedrigerer Priorität akzeptieren, wenn der im DHCPv6 Advertisement enthaltene Parametersatz mehr den vom Client angeforderten Optionen entspricht.</p> <p>Der Wert 0 bedeutet "nicht spezifiziert" (niedrigste Priorität), 255 bedeutet höchste Priorität.</p>

Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
DNS-Server	<p>Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server").</p> <p>In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld DNS-Propagation im Menü LAN->IP-Konfiguration->Schnittstellen->->Erweiterte Einstellungen mit IPv6 = Aktiviert konfiguriert.)</p> <p>Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option RA oder globalen Fallback-DNS-Server verwenden und erstellen Sie mit Hinzufügen die gewünschten DNS-Server-Einträge.</p>
SNTP-Server	<p>Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit Hinzufügen können Sie die gewünschten Zeitserver-Einträge anlegen.</p>


16.5.3 Zustandsbehaftete Clients

Hier sehen Sie Informationen zu zustandsbehafteten Clients, sobald diese eine IPv6-Adresse bezogen haben.

16.5.4 Konfiguration von zustandsbehafteten Clients

Bei einer zustandsbezogenen Konfiguration von IPv6 Clients, wird dem Client neben den DHCP-Optionen auch der IPv6-Präfix übermittelt.

16.5.4.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um Einträge für Stateful Clients anzulegen. Normalerweise müssen Sie keine Einträge anlegen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Sie sollten jeden automatisch angelegten Eintrag einmal aufrufen, um den Inhalt zu prüfen und gegebenenfalls anzupassen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DUID	Ein Client verwendet das Feld DUID (DHCP Unique Identifier), um sich zu identifizieren und eine IP-Adresse vom DHCPv6-Server zu beziehen. Wenn Sie mit der Schaltfläche Neu einen Eintrag anlegen, können Sie die DUID als 16- bis 20-stellige HEX-Zahl eingeben. Sie können sie mit den Trennzeichen Minus eingeben wie unter Windows oder als Block ohne Trennzeichen wie unter Linux.
Client FQDN akzeptieren	Wenn Client FQDN akzeptieren aktiviert ist, wird der Client mit dem Parameter FQDN (Fully Qualified Domain Name) im Cache des Domain Name Servers eingetragen.
Administrative FQDNs	Mit Hinzufügen können Sie - auch bei automatisch angelegten Einträgen - den Parameter FQDN (Fully Qualified Domain Name) eingeben.
Kennung der statischen Schnittstelle	Das Feld Kennung der statischen Schnittstelle ist der Host-Anteil der IPv6-Adresse, d.h. die letzten 64 Bit der

Feld	Beschreibung
	IPv6-Adresse. Dieser Präfix muss mit :: anfangen.

16.6 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.

16.6.1 Benutzer

Im Menü **Lokale Dienste->CAPI-Server->Benutzer** wird eine Liste aller konfigurierten CAPI Benutzer angezeigt.

16.6.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

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.

16.6.2 Optionen

Das Menü **Lokale Dienste->CAPI-Server->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Server aktivieren	Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Faxkopfzeile	Nur für Geräte der RTxxx2 -Serie Wählen Sie aus, ob am oberen Seitenrand von ausgehenden Faxen die Faxkopfzeile gedruckt werden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-Port des CAPI-Servers	Das Feld ist nur editierbar, wenn Server aktivieren aktiviert ist. Geben Sie die TCP-Port-Nummer für Remote-CAPI-Verbindungen ein. Der Standardwert ist <i>2662</i> .

16.7 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.

Konkrete Hinweise für die Konfiguration des Aufgabenplaners finden Sie am Ende des Kapitels unter [Konfigurationsbeispiel - Zeitgesteuerte Aufgaben \(Scheduling\)](#) auf Seite 384.



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.

16.7.1 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.

16.7.1.1 Neu

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

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> <ul style="list-style-type: none"> • <i>Zeit</i> (Standardwert): Die in Aktionen konfigurierten und zugewiesenen Aktionen werden zu bestimmten Zeitpunkten ausgelöst. • <i>MIB/SNMP</i>: Die in Aktionen konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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>Funktionstaste</i> (nicht für alle Geräte verfügbar): Mit der Option <i>Funktionstaste</i> legen Sie fest, dass das Drücken der Funktionstaste am Gerät als Auslöser für konfigurierte Aktionen dienen kann. Durch einen Druck von gut einer Sekunde (aber weniger als drei Sekunden) auf die Taste wird der Zustand der Taste auf <i>Aktiv</i> gesetzt, durch einen Druck von mehr als drei Sekunden wird er auf <i>Inaktiv</i> gesetzt. Aktionen, die vom Zustand der Taste abhängen, werden dann bei der nächsten zyklischen Abfrage gemäß dem Schedule-Intervall ausgelöst. Es kann also z. B. eine WLAN-Schnittstelle aktiviert werden, wenn die Funktionstaste eine Sekunde lang gedrückt wird. Bei einem Druck auf die Taste vom mehr als drei Sekunden wird die Schnittstelle wieder deaktiviert. • <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.

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

Feld	Beschreibung
	<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.
<p>Richtung des Datenverkehrs</p>	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>RX</i> (Standardwert): Der eingehende Datenverkehr wird überwacht. • <i>TX</i>: Der ausgehende Datenverkehr wird überwacht.
<p>Bedingung des Schnittstellenverkehrs</p>	<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>
<p>Übertragener Datenverkehr</p>	<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>Der Standardwert ist <i>0</i>.</p>
<p>Ziel-IP-Adresse</p>	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
<p>Quell-IP-Adresse</p>	<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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Status	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Wählen Sie aus, ob Ziel-IP-Adresse <i>Erreichbar</i> (Standardwert) oder <i>Nicht erreichbar</i> sein muss, um die Aktion auszulösen.</p>
Intervall	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Der Standardwert ist <i>60</i> Sekunden.</p>
Erfolgreiche Versuche	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p> <p>Der Standardwert ist <i>3</i>.</p>
Fehlgeschlagene Versuche	<p>Nur für Ereignistyp <i>Ping-Test</i></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 <i>1</i> bis <i>65536</i>.</p> <p>Der Standardwert ist <i>3</i>.</p>
Überwachtes Zertifikat	<p>Nur für Ereignistyp <i>Lebensdauer eines Zertifikats</i></p> <p>Wählen Sie das Zertifikat aus, dessen Gültigkeit überprüft werden soll.</p>

Feld	Beschreibung
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.
Status der Funktionstaste	Nur für Ereignistyp <i>Funktionstaste</i> Beim Anlegen des Auslösers können Sie über die Auswahl des Status der Funktionstaste festlegen, bei welchem Zustand der Funktionstaste der Auslöser aktiv sein soll. Setzen Sie den Status auf <i>An</i> , so wird der Auslöser aktiv, wenn der Zustand der Funktionstaste <i>Aktiv</i> ist, und inaktiv, wenn der Zustand der Funktionstaste <i>Inaktiv</i> ist. Setzen Sie ihn auf <i>Aus</i> , so wird der Auslöser aktiv, wenn der Zustand der Funktionstaste <i>Inaktiv</i> ist, und inaktiv, wenn der Zustand der Funktionstaste <i>Aktiv</i> ist. Die Zustandsprüfung erfolgt zyklisch im Abstand des konfigurierten Schedule-Intervalls.

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 Bedingungseinstellungen einen Wochentag aus. • <i>Perioden</i> (Standardwert): Wählen Sie in Bedingungseinstellungen einen bestimmten Turnus aus. • <i>Tag des Monats</i>: Wählen Sie in Bedingungseinstellungen einen bestimmten Tag im Monat aus. Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Wochentag</i> : <i>Montag</i> (Standardwert) ... <i>Sonntag</i> . Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Perioden</i> : <ul style="list-style-type: none"> • <i>Täglich</i>: Der Auslöser wird täglich aktiv (Standardwert).

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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 Bedingungeinstellungen bei Bedingungstyp = Tag des Monats:</p> <p>1... 31.</p>
Startzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.
Stoppzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine Stoppzeit eingeben oder Stoppzeit = Startzeit setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.

16.7.2 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.

16.7.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Aktionen zu konfigurieren.

Das Menü **Lokale Dienste->Scheduling->Aktionen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Bezeichnung für die Aktion ein.
Befehlstyp	Wählen Sie die gewünschte Aktion aus. Mögliche Werte:

Feld	Beschreibung
	<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 LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt. • <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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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>Der Standardwert ist <i>60</i> Sekunden.</p>
Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Tabelle aus, in der die MIB-Variable gespeichert ist, deren Wert verändert werden soll. Wählen Sie zunächst das System aus und dann die MIB-Tabelle. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
Befehlsmodus	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie aus, auf welche Weise der MIB-Eintrag manipuliert werden soll.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Vorhandenen Eintrag ändern</i> (Standardwert): Ein bestehender Eintrag soll verändert werden. • <i>Neuen MIB-Eintrag erstellen</i>: Ein neuer Eintrag soll angelegt werden.
Indexvariablen	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in MIB-Tabelle eindeutig zu kennzeichnen, z.B. <i>ConnIfIndex</i>. Aus der Kombination von Indexvariable (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und Indexwert ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere Indexvariablen mit Hinzufügen an.</p>

Feld	Beschreibung
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 beschrieben.</p> <p>Ist der Auslöser inaktiv, Status des Auslösers <i>Inaktiv</i>), wird die MIB-Variable mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (Status des Auslösers <i>Beide</i>), wird sie mit einem aktiven Auslöser mit dem in Aktiver Wert eingetragenen Wert und mit einem inaktiven Auslöser mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Legen Sie weitere Einträge mit Hinzufügen an.</p>
Schnittstelle	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.</p>
Schnittstellenstatus festlegen	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll.</p>

Feld	Beschreibung
	<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>
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>

Feld	Beschreibung
	<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> <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</i></p>

Feld	Beschreibung
	<p><i>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>
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</i>, <i>Konfiguration umbenennen</i> oder <i>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>

Feld	Beschreibung
	<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</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Konfiguration verschlüsseln	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Nach Ausführung neu starten	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, ob Ihr Gerät nach der gewünschten Aktion neu gestartet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Versionsprüfung	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i></p> <p>Wählen Sie aus, ob beim Import einer Konfigurationsdatei über-</p>

Feld	Beschreibung
	<p>prüft 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.
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>Der 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>Der 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 Zertifikatsbe-	<p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion =</p>

Feld	Beschreibung
Beschreibung	<p><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> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikat in Konfiguration schreiben	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungsbeschreibung	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.</p>
SCEP-Server-URL	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B.</p>

Feld	Beschreibung
	<p><code>http://scep.bintec-elmeg.com:8080/scep/scep.dll</code></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Subjektname	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</p> <p>Geben Sie einen Subjektnamen mit Attributen ein.</p> <p>Beispiel: "CN=VPNServer, DC=mydomain, DC=com, c=DE"</p>
CA-Name	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</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 = Zertifikatverwaltung und Aktion = SCEP</p> <p>Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.</p>
Schlüsselgröße	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</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 = Zertifikatverwaltung und Aktion = SCEP</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</p>

Feld	Beschreibung
	<p>Konfiguration Ihres Geräts gespeichert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CRL verwenden	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Werte:</p> <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	<p>Nur bei Befehlstyp = <i>5 GHz-WLAN-Bandscan, 5,8 GHz-WLAN-Bandscan</i> und <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>
Betriebsmodus (Inaktiv)	<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></p>

Feld	Beschreibung
	<i>tiv</i> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.

16.7.3 Optionen

Im Menü **Lokale Dienste->Scheduling->Optionen** konfigurieren Sie das Schedule-Intervall.

Das Menü **Lokale Dienste->Scheduling->Optionen** besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

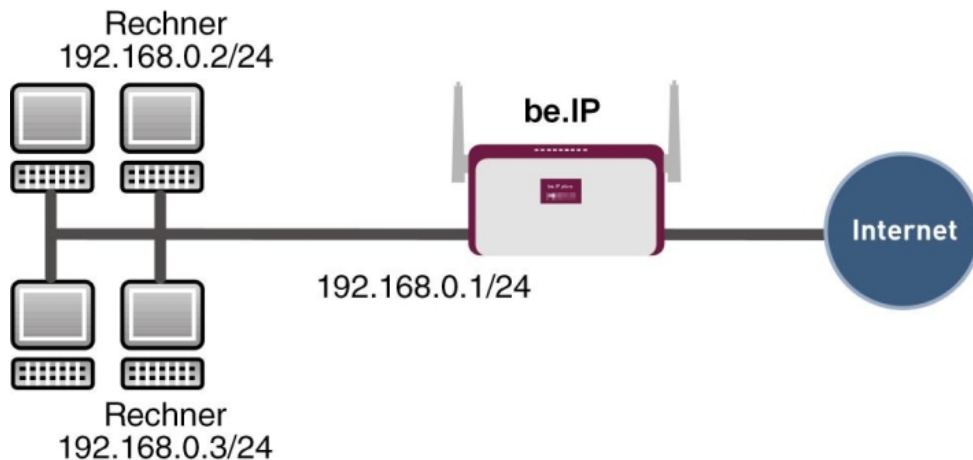
Feld	Beschreibung
Schedule-Intervall	<p>Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll.</p> <p>Standardmäßig ist das Schedule-Intervall nicht aktiv.</p> <p>Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind.</p> <p>Möglich sind Werte zwischen <i>0</i> und <i>65535</i>.</p> <p>Empfohlen wird der Wert <i>300</i> (5 Minuten Genauigkeit).</p>

16.7.4 Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling)

Voraussetzungen

- Grundkonfiguration des Gateways

Beispielszenario



Beispielszenario Zeitgesteuerte Aufgaben

Konfigurationsziel

- Das Gateway soll täglich während der Nacht neu starten.
- Am Wochenende soll die WLAN-Schnittstelle abgeschaltet werden.
- Einmal im Monat soll die Konfiguration automatisch auf einen TFTP-Server gesichert werden.

Konfigurationsschritte im Überblick

Täglicher Neustart

Feld	Menü	Wert
Ereignisliste	Lokale Dienste->Scheduling->Auslöser->Neu	Neu
Beschreibung	Lokale Dienste->Scheduling->Auslöser->Neu	z. B. <i>Neustart auslösen</i>
Ereignistyp	Lokale Dienste->Scheduling->Auslöser->Neu	Zeit
Zeitbedingung	Lokale Dienste->Scheduling->Auslöser->Neu	Bedingungstyp = <i>Perioden</i> , Bedingungeinstellungen = <i>Täglich</i>
Startzeit	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde 02 Minute 00
Beschreibung	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>Neustart des Geräts</i>

Feld	Menü	Wert
Befehlstyp	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Neustart</i>
Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Neustart auslösen</i>
Bedingung für Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Alle</i>
Neustart des Geräts nach	Lokale Dienste->Scheduling->Aktionen->Neu	<i>z. B. 60 Sekunden</i>
Schedule-Intervall	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

WLAN-Schnittstelle abschalten

Feld	Menü	Wert
Ereignisliste	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Neu</i>
Beschreibung	Lokale Dienste->Scheduling->Auslöser->Neu	<i>z. B. WLAN-Schnittstelle abschalten auslösen</i>
Ereignistyp	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Zeit</i>
Zeitbedingung	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Bedingungstyp = Perioden, Bedingungseinstellungen = Samstag Sonntag</i>
Startzeit	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Stunde 00 Minute 00</i>
Stopzeit	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Stunde 23 Minute 59</i>
Beschreibung	Lokale Dienste->Scheduling->Aktionen->Neu	<i>z. B. WLAN-Schnittstelle abschalten</i>
Befehlstyp	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Schnittstellenstatus</i>
Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>WLAN-Schnittstelle abschalten auslösen</i>
Bedingung für Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Alle</i>

Feld	Menü	Wert
Schnittstelle	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>vssl-0</i>
Schnittstellenstatus festlegen	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Inaktiv</i>
Schedule-Intervall	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

Konfiguration monatlich sichern

Feld	Menü	Wert
Ereignisliste	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Neu</i>
Beschreibung	Lokale Dienste->Scheduling->Auslöser->Neu	z. B. <i>Konfigurationssicherung auslösen</i>
Ereignistyp	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Zeit</i>
Zeitbedingung	Lokale Dienste->Scheduling->Auslöser->Neu	Bedingungstyp = <i>Tag des Monats</i> , Bedingungseinstellungen = <i>1</i>
Startzeit	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde <i>03</i> Minute <i>00</i>
Beschreibung	Lokale Dienste->Scheduling->Aktionen->Neu	Konfiguration sichern
Befehlstyp	Lokale Dienste->Scheduling->Aktionen->Neu	Konfigurationsmanagement
Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	Konfigurationssicherung auslösen
Bedingung für Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	Alle
Aktion	Lokale Dienste->Scheduling->Aktionen->Neu	Konfiguration exportieren
Server-URL	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>tftp://192.168.2.5</i>
CSV-Dateiformat	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Aktiviert</i>
Dateiname auf Server	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>monthly-backup.cf</i>

Feld	Menü	Wert
Dateiname in Flash	Lokale Dienste->Scheduling->Aktionen->Neu	<i>boot</i>
Konfiguration enthält Zertifikate/Schlüssel	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Aktiviert</i>
Schedule-Intervall	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

16.8 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.

16.8.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

16.8.1.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Überwachung->Hosts->Neu** besteht aus folgenden Feldern:

Feld im Menü Hostparameter

Feld	Beschreibung
Gruppen-ID	Wenn die Erreichbarkeit einer Gruppe von Hosts bzw. des Standard-Gateways von Ihrem Gerät überwacht werden soll, wählen Sie eine ID für die Gruppe bzw. für das Standard-Gateway. Die Gruppen-IDs werden automatisch von 0 bis 255 angelegt.

Feld	Beschreibung
	<p>Ist noch kein Eintrag angelegt, wird durch die Option <i>Neue ID</i> eine neue Gruppe angelegt. Sind Einträge vorhanden, kann man aus den angelegten Gruppen auswählen.</p> <p>Jeder zu überwachende Host muss einer Gruppe zugeordnet werden.</p> <p>Die in Schnittstelle konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied erreichbar ist.</p>

Felder im Menü Trigger


Feld	Beschreibung
Überwachte IP-Adresse	<p>Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.</p> <p>Mögliche Werte:</p> <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>Der 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, da-</p>

Feld	Beschreibung
	<p>mit der Host als erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 3.</p>
Fehlgeschlagene Versuche	<p>Geben Sie ein, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 3.</p>
Auszuführende Aktion	<p>Wählen Sie aus, welche Aktion ausgeführt werden soll. Für die meisten Aktionen wählen Sie eine Schnittstelle, auf die sich die Aktion bezieht.</p> <p>Auswählbar sind alle physikalischen und virtuellen Schnittstellen.</p> <p>Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (<i>Aktivieren</i>), deaktiviert (<i>Deaktivieren</i>, Standardwert) oder zurückgesetzt (<i>Zurücksetzen</i>) werden soll oder ob die Verbindung erneut aufgebaut (<i>Erneut wählen</i>) werden soll.</p> <p>Mit Aktion = Überwachen können Sie die IP-Adresse überwachen, die unter Überwachte IP-Adresse angegeben ist. Diese Information kann für andere Funktionen, wie die IP-Adresse zur Nachverfolgung, genutzt werden.</p>

16.8.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

16.8.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Das Menü **Lokale Dienste->Überwachung->Schnittstellen->Neu** besteht aus folgenden Feldern:


Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
Trigger	Wählen Sie den Status bzw. Statusübergang von Überwachte Schnittstelle aus, der eine bestimmte Schnittstellenaktion auslösen soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Schnittstelle wird aktiviert.</i> (Standardwert) • <i>Schnittstelle wird deaktiviert.</i>
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in Trigger definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in Schnittstelle ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert): Aktivierung der Schnittstelle(n) • <i>Deaktivieren</i>: Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter Schnittstelle festgelegte Aktion ausgeführt werden soll. Wählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle IPSec-Schnittstellen</i> .

16.8.3 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

16.8.3.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Überwachung->Ping-Generator->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein. Mögliche Werte: <ul style="list-style-type: none"> • <i>Automatisch</i>: Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i> (Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in Entfernte IP-Adresse angegebene Adresse abgesetzt werden soll. Mögliche Werte sind <i>1</i> bis <i>65536</i> . Der 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. Der Standardwert ist <i>3</i> .

16.9 UPnP

Universal Plug and Play (UPnP) ermöglicht die Nutzung aktueller Messenger-Dienste (z. B. Realtime-Video/Audiokonferenzen) als Peer-to-Peer Kommunikation, wobei einer der Peers hinter einem Gateway mit aktiver NAT-Funktion liegt.

UPnP befähigt (meist) Windows-basierte Betriebssysteme, die Kontrolle über andere Geräte im lokalen Netzwerk mit UPnP Funktionalität zu übernehmen und diese zu steuern. Dazu zählen u.a. Gateways, Access Points und Printserver. Es sind keine speziellen Gerätetreiber notwendig, da gemeinsame und bekannte Protokolle genutzt werden wie TCP/IP, HTTP und XML.

Ihr Gateway ermöglicht die Nutzung des Subsystems des Internet Gateway Devices (IGD) aus dem UPnP-Funktionsspektrum.

In einem Netzwerk hinter einem Gateway mit aktiver NAT Funktion agieren die UPnP-konfigurierten Rechner als LAN UPnP Clients. Dazu muss die UPnP Funktion auf dem PC aktiviert sein.

Der auf dem Gateway voreingestellte Port, über den die UPnP-Kommunikation zwischen LAN UPnP Clients und dem Gateway läuft, ist *5678*. Der LAN UPnP Client dient hierbei als sogenannter Service Control Point, d.h. er erkennt und kontrolliert die UPnP-Geräte im Netzwerk.

Die z. B. vom MSN Messenger dynamisch zugewiesenen Ports liegen im Bereich von *5004* bis *65535*. Die Ports werden gatewayintern bei Anforderung freigegeben, d.h. beim Start einer Audio-/Videoübertragung im Messenger. Nach Beenden der Anwendung werden die Ports sofort wieder geschlossen.

Die Peer-to-Peer-Kommunikation wird über öffentliche SIP Server initiiert, wobei lediglich die Informationen beider Clients weitergereicht werden. Anschließend kommunizieren die Clients direkt miteinander.

Weitere Informationen zu UPnP erhalten Sie auf www.upnp.org.

16.9.1 Schnittstellen

In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Sie können festlegen, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle angenommen werden (für Anfragen aus dem lokalen Netzwerk) und/oder ob die Schnittstelle über UPnP-Anfragen kontrolliert werden kann.

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.

16.9.2 Allgemein

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

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 Clients beinhaltenen Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients. Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.

Feld	Beschreibung
UPnP TCP Port	Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht. Mögliche Werte sind 1 bis 65535, der Standardwert ist 5678.


16.10 Wake-On-LAN

Mit der Funktion **Wake-On-LAN** können Sie ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten. Die Netzwerkkarte muss weiterhin mit Strom versorgt werden, auch wenn der Computer ausgeschaltet ist. Sie können die Bedingungen, die zum Versenden des sog. Magic Packets erfüllt sein müssen, über Filter und Regelketten definieren sowie diejenigen Schnittstellen auswählen, die auf die definierten Regelketten hin überwacht werden sollen. Die Konfiguration der Filter und Regelketten entspricht weitgehend der Konfiguration von Filtern und Regelketten im Menü **Zugriffsregeln**.

16.10.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

16.10.1.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Der Standardwert ist <i>any</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>Der 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.
IPv4-Zieladresse/-netzmaske	<p>Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.
Ziel-Port/Bereich	<p>Nur für Protokoll = <i>TCP, UDP</i> oder <i>TCP/UDP</i></p> <p>Geben Sie eine Zielport-Nummer bzw. einen Bereich von Zielport-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 Zielport ein. • <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.
IPv4-Quelladresse/-netzmaske	<p>Geben Sie die IPv4 Quell-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
IPv6-Quelladresse/-länge	<p>Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.


Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
Quell-Port/Bereich	<p>Nur für Protokoll = <i>TCP</i>, <i>UDP</i> oder <i>TCP/UDP</i></p> <p>Geben Sie eine Quellport-Nummer bzw. einen Bereich von Quellport-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Quellport ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Quellport ein. • <i>Portbereich angeben</i>: Geben Sie einen Quellport-Bereich ein.
DSCP / Traffic Class 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). • <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>

Feld	Beschreibung
	<p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7. Wertebereich 0 bis 7.</p> <p>Der Standardwert ist <i>Nicht beachten</i>.</p>

16.10.2 WOL-Regeln

Im Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln** wird eine Liste aller konfigurierter WOL-Regeln angezeigt.

16.10.2.1 Bearbeiten oder Neu

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

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>

Feld	Beschreibung
	Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü Lokale Dienste->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 Aktion = <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 Aktion = <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</p>


Feld	Beschreibung
	Passwort korrekt sind, wird das Gerät aktiviert.

16.10.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten einzelnen Schnittstellen zugeordnet, die auf diese Regelketten hin überwacht werden.

Im Menü **Lokale Dienste->Wake-On-LAN->Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

16.10.3.1 Bearbeiten oder Neu

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

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.

16.11 Trace-Schnittstelle

Das Menü **Trace-Schnittstelle** ermöglicht Ihnen eine Aufzeichnung des Datenverkehrs über eine bestimmte Schnittstelle und, nach Ende der Aufzeichnung, das Abspeichern des Mitschnitts als PCAP-Datei.

16.11.1 Trace-Schnittstelle

Felder im Menü Trace-Einstellungen

Feld	Beschreibung
Schnittstellenauswahl	Wählen Sie die Schnittstelle aus, deren Datenverkehr Sie aufzeichnen wollen.
Trace-Modus	Hier können Sie auswählen, auf welchen Ebenen der Datenver-

Feld	Beschreibung
	<p>kehr der ausgewählten Schnittstelle aufgezeichnet werden soll. Zur Auswahl stehen:</p> <ul style="list-style-type: none"><li data-bbox="639 274 758 300">• <i>Layer 2</i><li data-bbox="639 321 705 346">• <i>PPP</i><li data-bbox="639 367 758 392">• <i>Layer 3</i><li data-bbox="639 413 691 438">• <i>IP</i>

Sobald Sie die Aufzeichnung mit der Schaltfläche **START** beginnen, wird ein Fenster angezeigt, das über die laufende Aufzeichnung informiert. Sie können während der Aufzeichnung das Menü verlassen und das GUI wie gewohnt verwenden. Wenn Sie eine Aufzeichnung mit **STOPP** beenden, werden Informationen zu der erstellten Datei angezeigt, und Sie erhalten die Möglichkeit, diese zu löschen oder im PCAP-Format herunterzuladen.

Kapitel 17 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.

17.1 Benutzer ausloggen

Es kann vorkommen, dass durch eine nicht vollständig abgebaute Konfigurationssitzung Funktionen der Konfigurationsoberfläche beeinträchtigt werden. In diesem Fall können in diesem Menü alle noch bestehenden Verbindungen zum GUI eingesehen und ggf. beendet werden.

17.1.1 Benutzer ausloggen

In diesem Menü sehen Sie zunächst eine Auflistung aller aktiven Konfigurationsverbindungen.

Felder im Menü Benutzer ausloggen

Feld	Beschreibung
Klasse	Zeigt die Benutzerklasse an, der der angemeldete Benutzer angehört.
Benutzer	Zeigt den Benutzernamen an.
Entfernte IP-Adresse	Zeigt die IP-Adresse an, von der die Verbindung aufgebaut wurde. Die kann die Adresse eines PCs sein, aber auch die Adresse eines zwischengelagerten Routers.
Läuft ab	Zeigt an, wann die Verbindung automatisch getrennt wird.
Sofort ausloggen	Wenn sie das Kontrollkästchen aktivieren, wird dieser Benutzer mit einm klick auf Ausloggen vom System abgemeldet.

17.1.1.1 Logout-Optionen

Nachdem Sie die Auswahl der zu beendenden Verbindungen mit Ausloggen bestätigt haben, können Sie wählen ob und welche Konfigurationen, die mit den entsprechenden Sitzungen zusammenhängen, vor dem Abmelden der Benutzer gespeichert werden.

17.2 Diagnose

Im Menü **Wartung**->**Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

17.2.1 Ping-Test

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind.

Felder im Menü Ping-Test

Feld	Beschreibung
Test-Ping-Modus	Wählen Sie die für den Ping-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i>
Ping-Befehl testweise an Adresse senden	Geben Sie die zu testende IP-Adresse ein.
Zu verwendende Schnittstelle	Nur für Test-Ping-Modus = <i>IPv6</i> Wählen Sie für Link-Lokale-Adressen die Schnittstelle, die für den Ping-Test verwendet werden soll. Für globale Adressen kann <i>Standard</i> verwendet werden.

Durch Anklicken der **Los**-Schaltfläche wird der Ping-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an.

17.2.2 DNS-Test

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domännennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

17.2.3 Traceroute-Test

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese erreichbar ist.

Felder im Menü Traceroute-Test

Feld	Beschreibung
Traceroute-Modus	Wählen Sie die für den Traceroute-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i>
Traceroute-Adresse	Geben Sie die zu testende IP-Adresse ein.

Durch Anklicken der **Los**-Schaltfläche wird der Traceroute-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an.

17.3 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

17.3.1 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 problem-

los 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.

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):

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Konfiguration exportieren</i>: Die Konfigurationsdatei Aktueller Dateiname im Flash wird zu Ihrem lokalen Host transferiert. Wenn Sie die Los-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. • <i>Konfiguration importieren</i>: Wählen Sie in Dateiname eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken auf Los wird die Datei zunächst unter dem Namen <i>boot</i> in den Flash-Speicher des Geräts geladen. Zum Aktivieren müssen Sie das Gerät neu starten. 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>Konfigurationssicherung 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, sofern von Ihnen

Feld	Beschreibung
	<p>Gerät unterstützt): Wählen Sie in Dateiname die Datei <i>vms_wavfiles.zip</i> aus, die Sie importieren wollen.</p> <ul style="list-style-type: none"> • <i>Konfiguration mit Statusinformationen exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die Los-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.
Aktueller Dateiname im Flash	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.</p>
Zertifikate und Schlüssel einschließen	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Verschlüsselung der Konfiguration	<p>Nur für Aktion = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Passwort eingeben.</p>
Dateiname	<p>Nur für Aktion = <i>Konfiguration importieren, Sprache importieren, Systemsoftware aktualisieren</i></p> <p>Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.</p>
Name der Quelldatei	<p>Nur für Aktion = <i>Konfiguration kopieren</i></p>

Feld	Beschreibung
	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.
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.

17.4 Neustart

17.4.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **GUI** neu aufrufen und sich wieder anmelden.

Beobachten Sie dazu die LEDs an Ihrem Gerät. Für die Bedeutung der LEDs lesen Sie bitte in dem Handbuch-Kapitel **Technische Daten**.



Hinweis

Stellen Sie vor einem Neustart sicher, dass Sie Ihre Konfigurationsänderungen durch Klicken auf die Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.

Wenn Sie Ihr Gerät neu starten wollen, klicken Sie auf die **OK**-Schaltfläche. Der Neustart wird ausgeführt.

17.5 Factory Reset

Im Menü **Wartung->Factory Reset** können Sie Ihr Gerät über das GUI in den Auslieferungszustand versetzen.

Kapitel 18 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.

18.1 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 *Information* 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).

18.1.1 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.

18.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.

Das Menü **Externe Berichterstellung ->Systemprotokoll ->Syslog-Server ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	<p>Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Information</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>

Feld	Beschreibung
	<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> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System & Accounting</i> (Standardwert) • <i>System</i> • <i>Accounting</i>

18.2 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.

18.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

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.

18.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

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

Feld	Beschreibung
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen:

```
INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

18.3 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.

18.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

18.3.1.1 Neu

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

Das Menü **Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungsempfänger -> Neu** besteht aus folgenden Feldern:

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungsdienst	Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen. Mögliche Werte: <ul style="list-style-type: none"> • E-Mail • SMS
Empfänger	Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Nachrichtenkomprimierung	Wählen Sie aus, ob der Text der Benachrichtigungsmail ver-

Feld	Beschreibung
	<p>kürzt 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 Rogue AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • <i>Neuer Slave-AP (WTP) gefunden</i>: Eine neuer unkonfiguriertes AP hat sich beim WLAN Controller gemeldet. • <i>Verwalteter AP offline</i>: Ein managed AP ist nicht mehr erreichbar.
Enthaltene Zeichenfolge	<p>Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms.</p> <p>Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "**") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.</p>

Feld	Beschreibung
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, Information, 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. Der 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, der Standardwert ist 1.</p>

18.3.2 Benachrichtigungseinstellungen

Das Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungseinstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	<p>Wählen Sie aus, ob der Benachrichtigungsdienst aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
Maximale E-Mails pro Minute	Begrenzen Sie die Anzahl der ausgehenden Mails pro Minute. Zur Verfügung stehen Werte von <i>1</i> bis <i>15</i> , der Standardwert ist <i>6</i> .

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. Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Port	Verschlüsselung von E-Mails (SSL/TLS). Das Feld SMTP-Port ist Standardmäßig auf <i>25</i> voreingestellt und SSL Encryption aktiviert.
SMTP-Authentifizierung	Authentifizierung, die der SMTP-Server erwartet. Mögliche Werte: <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung. • <i>ESMTP</i>: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt. • <i>SMTP after POP</i>: Der Server verlangt, dass vor dem Versenden einer Mail Mails per POP3 von der sendenden IP aus mit dem richtigen POP3-Benutzernamen/Passwort abgerufen werden.
Benutzername	Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i> Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.
Passwort	Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i> Geben Sie das Passwort dieses Benutzers an.

Feld	Beschreibung
POP3-Server	Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i> Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.
POP3-Timeout	Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i> Geben Sie ein, wie lange der Router nach dem POP3-Abruf maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird. Der Standardwert ist <i>600</i> Sekunden.

Felder im Menü SMS Parameter (nur für Geräte mit UMTS)

Feld	Beschreibung
SMS-Gerät	Sie können sich über Systemmeldungen per SMS informieren lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
Maximale SMS pro Tag	Begrenzen Sie hier die Anzahl der an einem Tag versendeten SMS. Die Aktivierung von <i>Uneingeschränkt</i> erlaubt eine beliebige Anzahl an versendeten SMS. Der Standardwert beträgt 10 SMS pro Tag. Hinweis: Die Eingabe des Wertes 0 ist gleichbedeutend mit der Aktivierung von <i>Uneingeschränkt</i> .

18.4 SIA

18.4.1 SIA

Im Menü **Externe Berichterstellung**->**SIA**->**SIA** können Sie eine Datei erstellen lassen, die dem Support umfassende Informationen zum Zustand des Geräts liefert, wie z. B. zur aktuellen Konfiguration, dem verfügbaren Speicherplatz, der Betriebszeit des Geräts u.s.w.

Kapitel 19 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.

19.1 Internes Protokoll

19.1.1 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.

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.



19.2 IPSec


19.2.1 IPSec-Tunnel

Im Menü **Monitoring->IPSec->IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.

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.

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.

19.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

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 (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.

19.3 ISDN/Modem

19.3.1 Aktuelle Anrufe

Im Menü **Monitoring->ISDN/Modem->Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

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.

Feld	Beschreibung
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> .

19.3.2 Anrufliste

Im Menü **Monitoring->ISDN/Modem->Anrufliste** wird eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

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.

19.4 Schnittstellen

19.4.1 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.

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.

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.

Feld	Beschreibung
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.

19.4.2 Netzwerk-Status

Im Menü **Monitoring->Schnittstellen->Netzwerk-Status** finden Sie eine Übersicht über alle IP-Schnittstellen, die auf dem Gerät konfiguriert sind. Sie können den Status der Schnittstelle sowie wesentliche Parameter wie die IPv4- bzw. IPv6-IP-Adresse, die MAC-Adresse der Schnittstelle sowie die aktuell gültige MTU ablesen.

19.5 WLAN

19.5.1 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.

Werte in der Liste WLAN

Feld	Beschreibung
Mbit/s	Zeigt die möglichen Datenraten auf diesem Funkmodul an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete für die in Mbit/s angezeigte Datenrate an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete für die in Mbit/s angezeigte Datenrate an.

Über die Schaltfläche **Erweitert** gelangen Sie in eine Übersicht über weitere Details.

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 erfolgreich erhalten	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Unicast-Adresse versandt wurden.
MSDUs, die nicht übertragen werden konnten	Zeigt die Anzahl der MSDUs an, die nicht gesendet werden konnten.
Frame-Übertragungen ohne ACK	Zeigt die Anzahl der gesendeten Frames an, für die kein Acknowledgement-Frame empfangen wurde.
Doppelte empfangene MSDUs	Zeigt die Anzahl von doppelt empfangenen MSDUs an.
CTS Frames als Antwort auf RTS empfangen	Zeigt die Anzahl der empfangenen CTS (Clear to send)-Frames an, die als Antwort auf RTS (Request to send) empfangen wurden.
Nicht entschlüsselbare MPDUs erhalten	Zeigt die Anzahl der empfangenen MPDUs an, die nicht entschlüsselt werden konnten. Ein Grund dafür könnte sein, dass kein passender Schlüssel eingetragen wurde.
RTS Frames ohne CTS	Zeigt die Anzahl der RTS-Frames an, für die kein CTS empfangen wurde.
Fehlerhafte Erhaltene Pakete	Zeigt die Anzahl der Frames an, die unvollständig oder fehlerhaft empfangen wurden.

19.5.2 VSS

Im Menü **Monitoring->WLAN->VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.

Werte in der Liste VSS

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	<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>
Rx Discards	Zeigt die Anzahl der empfangenen Datenpakete, die verworfen wurden, wenn im Menü Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)->  im Feld Rx Shaping die Bandbreite für eingehenden Datenverkehr begrenzt wurde.
Tx Discards	Zeigt die Anzahl der gesendeten Datenpakete, die verworfen wurden, wenn im Menü Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)->  im Feld Rx Shaping die Bandbreite für ausgehenden Datenverkehr begrenzt wurde.

VSS - Details für Verbundene Clients

Im Menü **Monitoring->WLAN->VSS-><Verbundener Client>->**  werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt. Dabei werden die Werte für

den Drahtlos-Modus 802.11n separat aufgeführt.

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	<p>Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen 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	Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.
Rate	Zeigt die möglichen Datenraten auf dem Funkmodul an.
Tx-Pakete	Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.
Rx-Pakete	Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.

19.5.3 Client-Verwaltung

Im Menü **Monitoring->WLAN->Client-Verwaltung** wird eine Übersicht des **Client-Verwaltung** angezeigt. Sie sehen für jedes VSS u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die in vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

Werte in der Liste Client-Verwaltung

Feld	Beschreibung
VSS-Beschreibung	Zeigt die eindeutige Beschreibung des Drahtlosnetzwerks (VSS) an.
Netzwerkname (SSID)	Zeigt den Namen des Wireless Netzwerks (SSID) an.
MAC-Adresse	Zeigt die MAC Adresse, die für dieses VSS verwendet wird, an.
Aktive Clients	Zeigt die Anzahl der aktiven Clients.
2,4/5-GHz-Übergang	Zeigt die Anzahl der Clients, die über die Funktion 2,4/5-GHz-Übergang in ein anderes Frequenzband verschoben worden sind.
Abgewiesene Clients soft/hard	Zeigt die Anzahl der abgewiesenen Clients, nachdem die absolute Anzahl an zulässigen Clients erreicht wurde.

19.5.4 Bridge-Links

Im Menü **Monitoring->WLAN->Bridge-Links** werden die aktuellen Werte und Aktivitäten der Bridge-Links angezeigt.

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Tx Data Rate mbps	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link gesendeten Daten in Mbit/s an.
Rx Data Rate mbps	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.

Feld	Beschreibung
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Bridge-Link aktiv ist.

Bridge-Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Bridge-Links.

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link gesendeten Daten in Mbit/s an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

19.6 Bridges

19.6.1 br<x>

Im Menü **Monitoring->Bridges-> br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

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.

19.7 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

19.7.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

Glossar

2G	Siehe GSM.
3DES	Siehe DES.
3G	Siehe UMTS.
4G	Siehe LTE.
802.11	Die Norm 802.11 beschreibt Wireless LAN (WLAN). Es existieren verschiedene Erweiterungen: 802.11a: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 5 GHz, 802.11b: Brutto-Datentransferrate: 11 Mbit/s, Frequenzband: 2,4 GHz, 802.11g: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 2,4 GHz, 802.11n: Brutto-Datentransferrate: 600 Mbit/s, Frequenzband: 2,4 GHz (optional: 5 GHz)
A-Teilnehmer	Der A-Teilnehmer ist der Anrufer.
a/b-Schnittstelle	Eine a/b-Schnittstelle dient zum Anschluss eines analogen Endgeräts. Bei einem ISDN-Endgerät (Terminaladapter) mit a/b-Schnittstelle wird ein angeschlossenes analoges Endgerät in die Lage versetzt, die unterstützten ISDN-Leistungsmerkmale zu nutzen.
Abwurf / Abwurf-funktion	Bei der Wahl einer nicht-eingerichteten Rufnummer innerhalb der Telefonanlage oder falls der Anschluss des angerufenen Teilnehmers besetzt ist oder dieser den Anruf nicht entgegennimmt, bestimmt die Abwurf-funktion, wie mit dem Gespräch verfahren wird. Der Anruf kann zu einem anderen Ziel weitergeleitet oder verworfen werden.
Access Client	Der Client Mode ist eine Betriebsart eines Wireless Access Points (AP), bei dem sich dieser gegenüber dem übergeordneten AP wie ein Wireless Adapter verhält. Mit einem im Client Mode betriebenen AP können einzelne Rechner oder ganze Subnetze an übergeordnete Netze angebunden werden.
Access Point	Ein Access Point (AP) ist ein Gerät zur drahtlosen Verbindung von Clients (Computern). Der AP dient somit zum Aufbau eines Funknetzwerks (WLAN) sowie der Verbindung dieses WLANs mit einem kabelgebundenen Ethernet-Netzwerk (Bridging).
Accounting	Beim Accounting werden Verbindungsdaten aufgezeichnet, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und An-

zahl der übertragenen Datenpakete.

- Activity Monitor** Mithilfe des Activity Monitors kann der Status physikalischer und virtueller Geräteschnittstellen überwacht werden.
- Ad-Hoc-Netzwerk** In einem Ad-Hoc-Netzwerk verbinden sich einzelne Clients über einen Wireless Adapter zu einem unabhängiges Wireless LAN. Ad-Hoc-Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer-Basis. Der Ad-Hoc-Modus wird auch als IBSS-Modus (Independent Basic Service Set) bezeichnet und ist in kleinsten Netzen sinnvoll, z. B. bei der Vernetzung zweier Notebooks ohne Access Point.
- ADSL** Asymmetric Digital Subscriber Line. Siehe DSL.
- AES** Advanced Encryption Standard (AES, Rijndael) ist ein Verschlüsselungsverfahren (siehe Cipher). AES verwendet eine feste Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit. AES ist ein sehr schneller und sicherer Algorithmus.
- Agent** Der Callcenter-Agent ist Mitglied eines Callcenters.
- Aggressive Mode** Beim Aufbau einer IPSec-Verbindung wird der Aggressive Mode zur Realisierung eines Phase-1-Austausches verwendet. Der Aggressive Mode bietet keinen Schutz der Identität für aushandelnde Knoten, da sie ihre Identitäten übertragen müssen, bevor sie einen sicheren Kanal aufbauen können. Siehe auch Main Mode.
- AH** Der Authentication Header (AH) wird bei IPSec verwendet, um die Authentizität und Integrität der übertragenen Pakete sicherzustellen sowie den Sender zu authentisieren.
- Amtsberechtigung** In der Telefonanlage werden die folgenden Amtsberechtigungen unterschieden: Uneingeschränkt: Alle internationalen, nationalen und internen Verbindungen sind erlaubt. Nationale Ferngespräche: Es dürfen nur Verbindungen ins Inland aufgebaut werden - also die Wahl aller Rufnummer die mit 0 aber nicht mit 00 beginnen. Von extern eingehende Anrufe können ohne Einschränkung entgegengenommen werden. Ort: Es dürfen nur Verbindungen zur gleichen Ortsvorwahl aufgebaut werden. Die Rufnummer darf also nicht mit einer 0 beginnen. Von extern eingehende Anrufe können ohne Einschränkung entgegengenommen werden. Kommend: Es dürfen nur Verbindungen zu anderen Endgeräten der Telefonanlage aufgebaut werden. Von extern eingehende Anrufe können ohne Einschränkung entgegengenommen werden. Intern: Nur Verbindungen innerhalb der Telefonanlage sind erlaubt.

Analog	Analoge Signale werden zur Datenübertragung eingesetzt. Im Gegensatz zu digitalen Signalen sind sie stör anfälliger.
Analoge Endgeräte	Endgeräte, die Sprache oder andere Informationen analog übertragen, z. B. Telefone, Faxgeräte, Anrufbeantworter und Modems. Leistungsmerkmale lassen sich nur mit Endgeräten nutzen, die mit dem MFV-Wahlverfahren wählen und eine R- bzw. eine Flash-Taste besitzen.
Anklopfen	Anklopfen ist ein Leistungsmerkmal. Während eines Telefonats wird ein weiterer Anrufer signalisiert.
Anklopf Sperre	Bei aktiviertem Anklopfschutz wird ein weiterer Anrufer nicht am Endgerät signalisiert. Der Anrufer hört den Besetztton.
Anlagenanschluss	Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummernblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...) Siehe auch Mehrgeräteanschluss.
Anlagenanschluss-Rufnummer	Siehe Anlagenanschluss.
Annex A	Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.
Annex B	Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.
Annex J	Annex J ist eine DSL-Variante zur reinen Datenübertragung, ohne Sprachinformationen (entbündelter Anschluss). Annex J ist eine Ergänzung zur Spezifikation G.992. Diese DSL-Anschlüsse benötigen keinen Splitter und haben eine höhere Reichweite und eine schnellere Übertragungsgeschwindigkeit.
Annex L	Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrate vergrößert.
Annex M	Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.
Anrufbeantworter	Analoge Anrufbeantworter werden als analoges Endgerät konfigu-

riert und über den Endgerätetyp ausgewählt. Daneben dient das Voice Mail System der TK-Anlage als Anrufbeantworter.

Anruferliste	In Systemtelefonen werden entgangene Anrufe in einer Anruferliste gespeichert. Dazu muss die Übermittlung der Telefonnummer des Anrufers (CLIP) aktiviert sein.
Anrufschutz	Bei aktiviertem Anrufschutz ist die akustische Anrufsignalisierung ausgeschaltet. Diese Funktion wird auch als Ruhe vor dem Telefon bezeichnet.
Anrufvariante	Die Anrufvariante legt fest, an welchen Endgeräten ein Anruf signalisiert wird. Die einzelnen Anrufvarianten können über den Kalender zeitgesteuert umgeschaltet werden.
Anrufweitschaltung	Anrufweitschaltung ist ein Leistungsmerkmal. Mithilfe der Anrufweitschaltung (AWS) können ankommende Anrufe zu einer anderen, internen oder externen Telefonnummer weitergeleitet werden. Die Anrufweitschaltung kann in der Telefonanlage oder in der Vermittlungsstelle bzw. beim SIP-Provider erfolgen.
ANSI T1.413	ANSI T1.413 ist eine ADSL-Variante.
ARP	Das Address Resolution Protocol (ARP) liefert zu IPv4-Adressen die zugehörigen MAC-Adressen. Die notwendigen Informationen werden zwischen den Netzwerkknoten ausgetauscht, im Cache des Geräts gespeichert und nach Ablauf der ARP Lifetime wieder gelöscht. Für IPv6 wird diese Funktionalität durch das Neighbor Discovery Protocol (NDP) bereitgestellt.
ARS	Mithilfe der Automatic Route Selection (ARS) bestimmt die TK-Anlage die optimale Route zum angerufenen Teilnehmer, in Abhängigkeit von Provider, Dienst, QoS, ...
ATM	Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge kodiert und über asynchrones Zeitmultiplexing übertragen wird.
Authentifikation	Überprüfung der Identität des Nutzers (Authentisierung).
Automatische Amtsholung	Bei automatischer Amtsholung kann sofort (ohne Eingabe einer Kennziffer) die Telefonnummer eines externen Gesprächspartners gewählt werden.
Automatische Wahlwiederholung	Ist der Anschluss der angerufenen Seite besetzt, kann eine automatische Wahlwiederholung eingeleitet werden. Diese informiert den

Anrufer sobald die Leitung frei ist.

- Automatischer Rückruf bei besetzt (CCBS)** Rückruf bei besetzt ist ein Leistungsmerkmal. Ist der Anschluss des angerufenen Teilnehmers besetzt, kann ein Rückruf angefordert werden. Sobald das Gespräch des angerufenen Teilnehmers beendet ist, wird der Anrufer gerufen und automatisch mit dem Angerufenen verbunden.
- Automatischer Rückruf bei Nichtmelden (CCNR)** Rückruf bei Nichtmelden ist ein Leistungsmerkmal. Nimmt der angerufene Teilnehmer den Anruf nicht entgegen, kann ein Rückruf angefordert werden. Sobald der angerufene Teilnehmer ein Gespräch beendet, wird der Anrufer gerufen und automatisch mit dem Angerufenen verbunden.
- Autorisierung** Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
- AUX** AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.
- B-Kanal** Siehe Basisanschluss und Primärmultiplexanschluss.
- B-Teilnehmer** Der B-Teilnehmer ist der angerufene Teilnehmer.
- Backbone Area** Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.
- Basisanschluss** Der Basisanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Basic Rate Interface (BRI). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle) mit je 64 kbit/s und einen Steuerkanal (D-Kanal) mit 16 kbit/s. Für den Basisanschluss existieren zwei Betriebsarten: Anlagenanschluss und Mehrgeräteanschluss. Für größere Installationen wird der Primärmultiplexanschluss verwendet.
- Beacon** Zum Aufbau eines Wireless LAN im Infrastruktur-Modus versendet der zentrale Access Point Beacons. Diese Mitteilungen enthalten den Netzwerknamen (SSID), eine Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung.
- Berechtigungsklasse** Siehe CoS.
- Besetzt bei besetzt** Siehe Busy on Busy.
- Bit** Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.

Black / White List	Einträge in der Black List werden blockiert, Einträge in der White List werden durchgelassen. (Beispiel: Alle Telefonnummern, die mit 01234 beginnen, werden in der Black List blockiert. Die Telefonnummer 01234987 kann trotzdem in der White List freigegeben werden.)
Blowfish	Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.
BootP	Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrates.
BRI	Siehe Basisanschluss.
Bridge	Eine Bridge ist eine Netzwerkkomponente zum Verbinden gleichartiger Netze auf Schicht 2 des OSI-Modells. Datenpakete werden anhand von MAC-Adressen übertragen. Durch Bridges wird das Netzwerk aufgeteilt und entlastet.
Broadcast	Bei einem Broadcast werden Datenpakete von einem Punkt an alle Teilnehmer eines Netzes übertragen, z. B. falls der Empfänger noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP und DHCP. Die Kommunikation erfolgt über Broadcast-Adressen: MAC-Netzwerke: FF:FF:FF:FF:FF:FF, IPv4-Netzwerke: 255.255.255.255, IPv6-Netzwerke: ff00::/8
BRRP	BRRP ist eine Implementierung des Virtual Router Redundancy Protocol (VRRP). Ziel des Verfahrens ist es den Ausfall des Standardgateways zu kompensieren. Mehrere Router werden zu einem virtuellen Router zusammengefasst. Fällt einer dieser Router aus, können die Restlichen diesen ersetzen.
Bündel	Die externen Anschlüsse einer Telefonanlage können zu Bündeln zusammengefasst werden.
Busy On Busy	Ist Busy On Busy (Besetzt bei besetzt) aktiviert, hört ein Anrufer eines besetzten Teilnehmers den Besetztton. Anklopfen oder Anrufweiterschaltung an ein Team ist nicht möglich.
CA	Certificate Authority. Siehe Zertifikat.
Cache	Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.
Call Deflection (CD)	Siehe Rufumleitung.

Call Through	Unter Call Through versteht man die Einwahl über einen externen Anschluss in das System und die Weiterwahl aus dem System zu einem anderen externen Anschluss. Dies kann zur Senkung der Gesprächskosten führen.
Callcenter	Ein Callcenter bietet Beratung, Informationsaustausch und Verkauf über das Telefon.
Called Party's Number	Rufnummer des angerufenen Teilnehmers.
Calling Party's Number	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.
CFB	Call Forwarding Busy (CFB) ist ein Leistungsmerkmal. CFB schaltet Anrufer an einen anderen Anschluss weiter, wenn der Anschluss des Angerufenen besetzt ist (Anrufweiserschaltung bei besetzt).
CFNR	Call Forwarding No Reply (CFNR) ist ein Leistungsmerkmal. CFNR schaltet Anrufer an einen anderen Anschluss weiter, wenn der Anruf nicht entgegengenommen wird (Anrufweiserschaltung bei Nichtmelden).
CHAP	Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentifizierungsprotokoll für PPP-Verbindungen. Neben dem Standard-CHAP existieren noch die Varianten MS-CHAPv1 und MS-CHAPv2 der Firma Microsoft. Man wählt sich über PPP in ein Netzwerk ein und authentifiziert sich mit Benutzername und Passwort. Benutzername und Passwort werden verschlüsselt übertragen. Siehe auch PAP.

Cipher	Eine Blockchiffre (Block Cipher) ist ein Verschlüsselungsalgorithmus. In diesem Verschlüsselungsverfahren wird ein Datenblock mit fester Größe (normalerweise 64 Bit) mithilfe eines sogenannten Schlüssels zu einem Block derselben Größe umgeschrieben. Je länger der Schlüssel ist, umso sicherer ist der Algorithmus.
CLID	Calling Line Identification (CLID), auch Caller ID, wird zur Authentifizierung verwendet. Ein Anrufer wird anhand seiner ISDN-Rufnummer erkannt, bevor die Verbindung aufgebaut wird.
Client	Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.
CLIP	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).
CLIP no Screening	Siehe auch Telefonnummer des Anrufers anzeigen (CLIP / CLIR). Bei CLIP no Screening wird neben der normalen Rufnummer des Anrufers eine weitere Rufnummer, z. B. Rufnummer der Telefonzentrale oder eine Servicrufnummer, mitgesendet. Die normale Rufnummer kann zusätzlich über CLIR unterdrückt werden, sodass der Angerufene nur die weitere Rufnummer sieht.
CLIP off Hook	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).
CLIR	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).
COLP	Siehe Telefonnummer des Angerufenen anzeigen (COLP / COLR).
COLP no Screening	Siehe auch Telefonnummer des Angerufenen anzeigen (COLP / COLR). Bei COLP no Screening wird neben der normalen Rufnummer des Angerufenen eine weitere Rufnummer, z. B. Rufnummer der Telefonzentrale oder eine Servicrufnummer, mitgesendet. Die normale Rufnummer kann zusätzlich über COLR unterdrückt werden, sodass der Anrufer nur die weitere Rufnummer sieht.
COLR	Siehe Telefonnummer des Angerufenen anzeigen (COLP / COLR).
CoS	Der Begriff Class of Service (CoS) hat je nach Anwendungsgebiet verschiedene Bedeutungen. In der Telekommunikation wird unter CoS die dem Benutzer zugeteilte Berechtigungsklasse verstanden. Die Berechtigungsklasse legt die Rechte des Benutzers fest, wie z. B. Amtsberechtigung, nutzbare Leistungsmerkmale, Zugriff auf Anwendungen, ... In der Netzwerktechnologie versteht man unter CoS die Klassifizierung bestimmter Dienste gemäß IEEE 802.1p. CoS ermöglicht eine gezielte Priorisierung, während mit Quality of Service (QoS) explizite Bandbreitengarantien oder -beschränkungen einge-

	richtet werden. Die Einteilung der Datenpakete erfolgt mittels eines DSCP-Werts (Differentiated Services Code Point).
CRC	Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.
CRL	Siehe Zertifikat.
D-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.
Daemon	Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.
Datagramm	Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.
Datenkompression	Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.
DDI	Direct Dial In (DDI) bedeutet Durchwahl. Siehe Anlagenanschluss und Durchwahl (VoIP).
Dead Peer Detection	In IPsec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.
DECT	Digital Enhanced Cordless Telecommunications (DECT) ist ein Standard für Schnurlostelefone sowie für kabellose Telefonanlagen.
Default Gateway	An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.
Default Route	Siehe Standardroute.
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.
Digital	Digitale Signale werden zur Datenübertragung eingesetzt. Im Gegensatz zu analogen Signalen sind sie weniger stör anfällig.
DIME	Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.
Direktruf	Falls die Funktion Direktruf eingerichtet ist, muss lediglich der Telefontaster abgehoben werden, um nach einer kurzen Wartezeit eine Verbindung zu einer bestimmten Telefonnummer automatisch einzuleiten.
DISA	DISA steht für Direct Inward System Access. Ein Anruf wird, nachdem er von der Telefonanlage angenommen wurde, nach Eingabe einer Kennziffer automatisch weitervermittelt. Der Kennziffer ist in der Telefonanlage eine Telefonnummer zugeordnet.
DNS	Mithilfe des Domain Name System (DNS) wird der Domänenname (z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).
Domäne	Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).
Downstream	Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.
Dreierkonferenz	Die Dreierkonferenz ist ein Leistungsmerkmal. Drei Teilnehmer können gleichzeitig miteinander telefonieren.
DSA	Mithilfe des Digital Signature Algorithm (DSA) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über Signaturen können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. DSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch RSA. DSA ist schneller in der Schlüsselerzeugung aber langsamer in der Schlüsselverarbeitung

	als RSA.
DSCP	Datenpakete können mit einem Differentiated Services Codepoint (DSCP) ausgezeichnet werden. DSCP-Werte teilen Datenpakete in Klassen ein, sodass wichtige Pakete schneller durch das Netzwerk geleitet werden können. Siehe auch QoS.
DSL-Modem	Siehe Modem.
DSP	Ein digitaler Signalprozessor (DSP) wandelt analoge, ISDN- und VoIP-Signale ineinander um. Analoge Endgeräte können somit z. B. auch an einem SIP-Anschluss verwendet werden.
DSS1	Digital Subscriber Signalling System No. 1 (DSS1) ist ein Signalisierungsprotokoll für den D-Kanal des ISDN. Es ist auch bekannt als Euro-ISDN.
DTIM	Eine Delivery Traffic Indication Message informiert die Clients über auf dem Access Point vorhandene Multicast- bzw. Broadcast-Daten.
DTMF	Siehe Mehrfrequenzwahlverfahren.
DTMF Inband / Outband	Siehe auch Mehrfrequenzwahlverfahren. Bei Inband wird das DTMF-Signal im Sprachband übertragen (G.711). Bei Outband wird das DTMF-Signal entsprechend RFC 2833 übertragen.
Durchsage	Die Durchsage ist ein Leistungsmerkmal. Die Durchsage-Funktion ermöglicht es, eine Verbindung zu anderen Telefonen aufzubauen, die von den angerufenen Teilnehmern automatisch angenommen wird. Der Anrufer spricht und die Angerufenen hören die Durchsage. Hebt ein Angerufener den Hörer ab, wird eine normale Verbindung hergestellt.
Durchwahl (VoIP)	Beim Durchwahl-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer IP-TK-Anlage. Man erhält eine Basisrufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Basisrufnummer: 1234, 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	Enkapsulierung (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.
Encryption	Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.
ESP	Encapsulating Security Payload (ESP) ist ein Protokoll für IPsec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.
Ethernet	Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.
Euro-ISDN	In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.
Eurofile-Transfer	EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.
Fax	Mithilfe eines Telefax (Kurzform Fax) können Texte, Grafiken und Dokumente über das Telefonnetz übertragen werden. Man unterscheidet zwischen Faxgeräten der Gruppe 3 für das analoge Netz (Übertragungsrate: 9,6 bzw. 14,4 kbit/s) und Faxgeräten der Gruppe 4 für das ISDN (Übertragungsrate: 64 kbit/s). Für den Anschluss von Faxgeräten der Gruppe 3 an ISDN benötigt man einen Terminaladapter oder eine entsprechende Telefonanlage.
Filter	Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll,

	<p>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.</p>
Filterregel	<p>Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.</p>
Firmware	<p>Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts bereitgestellt.</p>
Flash-Taste	<p>Die Flash-Taste bei Telefonen entspricht der R-Taste. Die Taste unterbricht die Leitung für einen kurzen Moment, um bestimmte Funktionen wie z. B. eine Rückfrage einzuleiten.</p>
Follow-me	<p>Follow-me ist ein Leistungsmerkmal. Mit dieser Funktion können eingehende Anrufe einer anderen Nebenstelle zum eigenen Endgerät umgeleitet werden.</p>
Fragmentierung	<p>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.</p>
Frame	<p>Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells</p>
Frame Relay	<p>Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.</p>
Freisprechen	<p>Beim Freisprechen kann man bei aufgelegtem Hörer telefonieren. Dabei können weitere Personen im Raum über Mikrofon und Lautsprecher am Gespräch teilnehmen.</p>
FTP	<p>Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.</p>
Full-Duplex	<p>Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.</p>
Funktionstasten	<p>Funktionstasten sind spezielle Tasten bei Systemtelefonen, die mit Telefonnummern oder Funktionen belegt werden können.</p>

FXO	Foreign Exchange Office (FXO) bezeichnet den Anschluss am analogen Endgerät. Siehe auch FXS.
FXS	Foreign Exchange Station (FXS) bezeichnet den analogen Anschluss an der Anschlussdose oder der Telefonanlage. Siehe auch FXO.
G.711	G.711 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 300 Hz bis 3400 Hz werden mit einer Abtastrate von 8 kHz erfasst. Der Codec erreicht bei einer Datenübertragungsrate von 64 kbit/s eine sehr gute Sprachqualität (MOS-Wert: 4,4). In Europa wird das alaw- und in den USA das μ law-Quantisierungsverfahren verwendet.
G.722	G.722 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 50 Hz bis 7000 Hz werden mit einer Abtastrate von 16 kHz erfasst. Der Codec erreicht bei einer Datenübertragungsrate von 64 kbit/s eine hervorragende Sprachqualität (MOS-Wert: 4,5).
G.726	G.726 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 200 Hz bis 3400 Hz werden mit einer Abtastrate von 8 kHz erfasst. Der Codec erreicht eine ordentliche Sprachqualität. MOS-Wert: 3,7 (16 kbit/s), 3,8 (24 kbit/s), 3,9 (32 kbit/s), 4,2 (40 kbit/s). Es existieren zwei unterschiedliche Kodierverfahren: I.366 und X.420
G.729	G.729 ist ein Audio-Codec. Audio-Signale aus dem Frequenzbereich zwischen 300 Hz bis 2400 Hz werden mit einer Abtastrate von 16 kHz erfasst. Der Codec erreicht bei einer Datenübertragungsrate von 8 kbit/s eine ordentliche Sprachqualität (MOS-Wert: 3,9).
G.991.1	Datenübertragungsempfehlung für HDSL.
G.991.2	Datenübertragungsempfehlung für SHDSL.
G.992.1	Datenübertragungsempfehlung für ADSL (G.DMT). Es existieren zwei länderspezifische Ausprägungen G.992.1 Annex A und G.992.1 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.2	Datenübertragungsempfehlung für ADSL (G.LITE / ADSL-Lite). Es existieren zwei Varianten G.992.2 Annex A und G.992.2 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.3	Datenübertragungsempfehlung für xDSL2. Es existieren drei Varianten: G.992.3 Annex A/B (G.DMT bis ADSL2) mit Datenübertra-

gungsraten von 12 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.3 Annex L (RE-ADSL2) mit Datenübertragungsraten von 5 Mbit/s im Downstream und 0,8 Mbit/s im Upstream und G.992.3 Annex M (ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 2,5 Mbit/s im Upstream.

G.992.4	Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)
G.992.5	Datenübertragungsempfehlung für xDSL2+. Es existieren drei Varianten: G.992.5 Annex A/B (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.5 Annex L (RE-ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream und G.992.5 Annex M (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 3,5 Mbit/s im Upstream.
G.993.1	Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)
G.993.2	Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)
G.DMT	Siehe F.992.1.
G.Lite	Siehe F.992.2.
G.SHDSL	Siehe G.991.2.
Gateway	Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.
GPRS	General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.
GRE	Generic Routing Encapsulation (GRE) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. GRE verwendet die Protokollnummer 47.
GSM	Das Global System for Mobile Communications (GSM), auch als 2G bezeichnet, ist ein Mobilfunkstandard. Dieser erreicht zusammen mit GPRS eine spezifizierte max. Datenübertragungsrate von 171,2 kbit/s.
Half-Duplex	Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.

Halten	Ein Telefongespräch wird auf Wartestellung geschaltet, ohne die Verbindung zu verlieren (Rückfragen/Makeln). Man unterscheidet zwischen dem Halten der Verbindung in der Telefonanlage (Halten im System) und der Wartestellung in der Vermittlungsstelle bzw. beim SIP-Provider.
Hash	Zur Sicherstellung der Datenintegrität muss die Information vor unautorisierter Manipulation während der Übertragung geschützt werden. Um dies zu gewährleisten, muss jede empfangene Kommunikation mit der ursprünglich gesendeten Information übereinstimmen. Deshalb werden mathematische Streuwertfunktionen (Hashfunktionen) zur Berechnung von Prüfsummen (Hashwerten) verwendet. Diese werden verschlüsselt und mit der Nachricht als digitale Signatur versendet. Der Empfänger prüft wiederum die Signatur, bevor er das Paket öffnet. Falls sich die Signatur und damit der Inhalt des Datenpakets geändert hat, wird das Paket verworfen. Die am häufigsten verwendeten Hash-Algorithmen sind Message Digest Version 5 (MD5) und Secure Hash Algorithm (SHA1).
HDSL	High Data Rate Digital Subscriber Line. Siehe DSL.
Heartbeat	Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.
Heranholen von Rufen	Siehe Pick-Up
Hop	Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.
Host	Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.
Host-Name	Domänenname eines Host. Siehe DNS.
Hostroute	Eine Hostroute bezeichnet die Route zu einem einzelnen Host.
Hotspot	Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.
HSDPA	High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.
HTTP	Das HyperText Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. Es verwendet standardmäßig den Port 80.

HTTPS	Das HyperText Transfer Protocol Secure (HTTPS) ist ein Protokoll zur abhörsicheren Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. HTTPS ist schematisch identisch zu HTTP. Für die zusätzliche Verschlüsselung der Daten wird SSL / TLS verwendet. Der Standard-Port für HTTPS-Verbindungen ist 443.
Hyperchannel	Beim Hyperchannel haben mehrere Teilnehmer Zugriff auf das Übertragungsmedium. Ein Teilnehmer kann seine Informationen nur übertragen, wenn kein anderer Teilnehmer das Medium belegt. Ein Hyperchannel-Netzwerk dient hauptsächlich für Kurzstreckenbetrieb mit höchsten Datenraten.
IAE	IAE bezeichnet die standardisierte Steckdose (ISDN-Anschlusseinheit), an der ISDN-Endgeräte angeschlossen werden.
ICMP	Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.
IGMP	Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.
IKE	Das Internet-Key-Exchange-Protokoll (IKE) dient der automatischen Schlüsselverwaltung bei IPSec-Verbindungen. Der IKE-Prozess verläuft in zwei Phasen. Während Phase 1 authentifizieren sich die IKE-Teilnehmer gegenseitig und etablieren einen sicheren Kanal. In Phase 2 handeln die beiden IPSec-Teilnehmer die SAs aus. Es existieren zwei Versionen des IKE-Mechanismus.
Impulswahlverfahren	Das Impulswahlverfahren (IWW) ist ein Signalisierungsverfahren zur automatischen Telefonvermittlung. Tastatureingaben werden durch eine definierte Anzahl von Gleichstromimpulsen dargestellt. Siehe auch Mehrfrequenzwahlverfahren (MFV).
Infrastruktur-Netzwerk	In einem Infrastruktur-Netz bilden die einzelnen Endgeräte (Clients) über einen zentralen Knotenpunkt (Access Point) ein Wireless LAN. Dieser zentrale Access Point kann dabei auch ein Vermittler in weitere Netze sein.
Interne Telefonnummern	Die internen Telefonnummern werden für Gespräche innerhalb der Telefonanlage verwendet.
Internrufton	Der Internrufton dient als besondere Signalisierung in Telefonanlagen zur Unterscheidung von Intern- und Externanrufen.

IP	Das Internet Protocol (IP) ist ein Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es arbeitet auf der Vermittlungsschicht des OSI-Modells. Auf IP bauen die Protokolle TCP und UDP auf. Es existieren zwei Versionen Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6).
IP-Adresse	IP-Adressen werden zur Navigation in einem IP-Netzwerk verwendet, um Quelle und Ziel eindeutig zu bestimmen. IPv4-Adressen bestehen aus 32 Bits, IPv6-Adressen aus 128 Bits. Damit sind bei IPv4 232, also 4.294.967.296 Adressen darstellbar, bei IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen. Für IPv4 wird die Dezimaldarstellung (dotted decimal notation) verwendet, z. B. 192.168.0.250. Für IPv6 wird die Hexadezimaldarstellung verwendet, z. B. 2001:db8:85a3::8a2e:370:7344. Siehe auch Netzmaske.
IPCP	Das Internet Protocol Control Protocol (IPCP) dient, analog zu DHCP, zur Konfiguration eines Host mit IP-Adresse, Gateway und DNS-Server, falls eine PPP-Netzwerkverbindung verwendet wird. Mithilfe der Erweiterung Robust Header Compression over PPP kann der Header für eine schnellere Datenübertragung komprimiert werden. Analog wird in IPv6-Netzwerken die Funktionalität durch das Internet-Protocol-Version-6-Control-Protokoll (IPV6CP) bereitgestellt.
IPSec	IPSec (Internet Protocol Security) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. Die Protokollnummer für IPSec ist dabei vom verwendeten Protokoll abhängig. Der 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-BRI	Siehe BRI.
ISDN-Intern-/Extern	Alternative Bezeichnung für den S0-Bus.

ISDN-Login	Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.
ISDN-Nummer	Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.
ISDN-PRI	Siehe PRI.
ISDN-Router	Siehe Router.
ISP	Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.
ITU	Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.
IWV	Siehe Impulswahlverfahren.
Kanal	Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.
Kanalbündelung	Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.
Keepalive	Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.
Keepalive	Keepalive ist ein Mechanismus zur Aufrechterhaltung der Netzwerkverbindung und zur Überprüfung der Erreichbarkeit der Kommunikationspartner. Dazu werden in der Regel spezifische Pakete ins Netzwerk gesendet.
Kennzifferprozedur	Über die Telefontastatur kann man eine Sequenz (Kennzifferprozedur) eingeben (bestehend aus 0 - 9, *, # und R), um Funktionen der Telefonanlage aufzurufen.
Keypad	Das Keypad-Protokoll (Netz-Direkt) wird zum Aufruf und zur Steuerung von Leistungsmerkmalen, die von der Vermittlungsstelle bereitgestellt werden, verwendet.
Konferenzschaltung	Bei einer Konferenzschaltung können mehrere interne Gesprächsteilnehmer gleichzeitig miteinander telefonieren.
Konfiguration	Alle Einstellungen des Geräts werden als Konfiguration bezeichnet. Diese Konfiguration ist intern in MIB-Tabellen gespeichert. Diese Informationen können extern gesichert, von extern geladen oder ge-

löscht werden. Bearbeitet wird die Konfiguration über die HTTP(S)-Benutzeroberfläche, einen SNMP-Client oder angeschlossene Telefone.

Kurzwahl

Jeder Telefonnummer im Telefonbuch ist ein Kurzwahl-Index (000...999) zugeordnet. Dieser Kurzwahl-Index kann anstelle der langen Telefonnummer für die Wahl verwendet werden.

L2TP

Das Layer 2 Tunneling Protocol (L2TP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über verschiedene Protokolle zu transportieren. L2TP verwendet standardmäßig die Protokollnummer 1701. Die Architektur eines L2TP-Netzwerks besteht aus einem L2TP-Access-Concentrator (LAC), der auch fest in den Client integriert sein kann, und dem L2TP-Network-Server (LNS). Der LAC stellt die Verbindungen zum LNS her und verwaltet diese. Die Autorisierung wird über einen Network-Access-Server (NAS), der im LAC oder LNS implementiert sein kann, geregelt. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Die eigentlichen Nutzdaten werden unverschlüsselt ausgetauscht, während Kontrollnachrichten 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.

Lauthören

Beim Lauthören können im Raum anwesende Personen ein Telefongespräch mithören.

Layer

Ein Layer bezeichnet eine Schicht im OSI-Modell.

LCP

Das Link Control Protocol (LCP) wird in PPP-Verbindungen verwendet, um die 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 Kom-

	munikation zwischen einem Client und dem Directory-Server. LDAP wird für den Austausch und die Aktualisierung von Verzeichnissen, z. B. ein Telefonbuch, verwendet.
Lease Time	Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.
Leased Line	Siehe Standleitung.
LLC	Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.
LNS	Siehe L2TP.
Loopback	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
LTE	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
MAC-Adresse	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
Main Mode	Beim Aufbau einer IPSec-Verbindung wird der Main Mode zur Realisierung eines Phase-1-Austausches verwendet, indem ein sicherer Kanal eingerichtet wird. Siehe auch Aggressive Mode.
Makeln	Makeln erlaubt es, zwischen zwei Gesprächspartnern hin und her zu schalten, ohne dass der wartende Teilnehmer mithören kann.
Man-in-the-Middle Attack	Im Man-in-the-middle-Angriff befindet sich der Angreifer physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kann somit den Datenverkehr einsehen und sogar manipulieren.
MD5	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Media Gateway	Ein Media Gateway wandelt den Netzwerktyp von digitalen Sprach-, Audio- oder Bildinformationen um. Beispielsweise können die Signale eines ISDN-Netzwerks auf ein IP-Netzwerk umgesetzt werden.
Mehrfachrufnummer (MSN)	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
Mehrfrequenzwahl-	Das Mehrfrequenzwahlverfahren, auch als Tonwahlverfahren, MFV,

verfahren	MFC oder DTMF bezeichnet, ist ein Signalisierungsverfahren zur automatischen Telefonvermittlung. Tastatureingaben werden durch überlagerte, sinusförmige Signale dargestellt. Siehe auch Impulswahlverfahren (MFV).
Mehrgeräteanschluss	Beim Mehrgeräteanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von ISDN-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Anlagenanschluss.
Metrik	Die Metrik ist eine Maß für die Güte der Route. Die schnellste Route weist dabei die geringste Metrik (costs, »Kosten«) auf. Vereinfacht ist dies die Verbindung mit der kleinsten Anzahl an Knotenpunkten (Routern).
MFC	Siehe Mehrfrequenzwahlverfahren.
MFV	Siehe Mehrfrequenzwahlverfahren.
MIB	Die Management Information Base (MIB) beschreibt die Informationen, die über ein Netzwerk-Management-Protokoll (z. B. SNMP) abgefragt oder modifiziert werden können. Die MIB ist eine Datenbank, die alle Geräte und Funktionen im Netzwerk beschreibt.
MLP	Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.
Mobiler Teilnehmer	Falls der mobile Teilnehmer aktiviert ist, kann ein externes Telefon, z. B. ein Mobiltelefon, parallel gerufen (Parallelruf) werden. Ebenso können die Funktionen der Anlage, z. B. ein Rückruf, extern genutzt werden. Für diese Funktionen wird die Sterntaste des externen Telefons als R-Taste interpretiert.
Modem	Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.
MOH	Siehe Music On Hold.
MPDU	Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.
MPPC	Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.

MPPE	Microsoft Point-To-Point Encryption (MPPE) wird zur Verschlüsselung von Daten, die über PPP übertragen werden, eingesetzt. Es wurde von Microsoft und Cisco entwickelt und als RFC 3078 spezifiziert.
MS-CHAP	Das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) ist ein Authentisierungsverfahren. MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für PPTP-Verbindungen (VPN).
MSDU	Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.
MSN	Siehe Mehrfachrufnummer.
MSS	Die Maximum Segment Size (MSS) definiert die maximale Anzahl an Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Die MSS muss kleiner als die Maximum Transmission Unit (MTU) sein, um eine Fragmentierung der IP-Pakete zu vermeiden.
MSS Clamping	Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.
MTU	Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.
Multicast	Bei einem Multicast werden Datenpakete von einem Punkt an bestimmte Teilnehmer eines Netzes übertragen. In IPv4 wird dies über den Adress-Bereich 224.0.0.0 bis 239.255.255.255 und das Protokoll IGMP gesteuert, in IPv6 über ff00::/8-Adressen und ICMPv6.
Multilink	Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, ...) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.
Music On Hold	Der Begriff Music On Hold (MOH) steht für automatische Ansagen oder Wartemusik über die Telefonanlage.
MWI	Über den Message Waiting Indicator (MWI) wird das Vorhandensein einer neuen Nachricht signalisiert.
NAPT	Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.

NAT	Mithilfe von Network Address Translation (NAT) werden die Quell- und Ziel-IP-Adressen eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch PAT.
NBNS	NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.
Nebenstelle	Eine Nebenstelle bezeichnet bei Telefonanlagen das mit der Anlage verbundene Endgerät.
Netz-Direkt	Siehe Keypad.
Netzabschluss	Der Netzabschluss (Network Termination, NT) bezeichnet einen Anschluss bzw. eine Betriebsart. Am NT-Anschluss (Anschlussdose) wird einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt. Beim analogen Anschluss wird die Steckdose TAE genannt, beim ISDN-Basisanschluss NTBA und beim ISDN-Primärmultiplexanschluss NTPMGF. Im NT-Betrieb wird das Gateway am externen S0 der Telefonanlage angeschlossen und stellt für diese einen externen Amtsanschluss dar. Siehe auch TE.
Netzmaske	Die Netzmaske, auch Netzwerkmaske oder Subnetzmaske, definiert bei IPv4 in Verbindung mit der IP-Adresse das Netzwerk, indem sie die IP-Adresse in einen Netzwerk- und einen Geräteanteil aufteilt und somit bestimmt, welche Adressen geroutet werden müssen. Beispiel einer Netzmaske: 255.255.255.0. Bei IPv6 spricht man von der Präfixlänge.
Netzwerkadresse	Eine Netzadresse (Präfix) bezeichnet die Adresse des gesamten Netzwerks. Die Netzwerkmaske bzw. Präfixlänge unterteilt die IP-Adresse in die Netzadresse und Host-Adresse (Geräteadresse). Beispiel für eine Netzadresse: 192.168.0.250/24
Netzwerkroute	Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.
NT	Siehe Netzabschluss.
NTBA	Siehe Netzabschluss.
NTP	Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.
NTPMGF	Siehe Netzabschluss.
Nutzkanal	Siehe B-Kanal.

OAM	OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.
Offene Rückfrage	Bei der offenen Rückfrage wird ein Gespräch in einen Wartezustand versetzt und kann von jedem Teilnehmer wieder angenommen werden.
OSI-Modell	Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.
OSPF	OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.
PABX	Private Automatic Branch Exchange (PABX) ist eine andere Bezeichnung für eine Telefonanlage.
PAP	Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.
Parallelruf	Siehe Mobiler Teilnehmer.
Parken	Beim Parken wird eine Telefonverbindung gehalten, selbst wenn beim beteiligten Endgerät der Hörer aufgelegt oder die Kabelverbindung getrennt ist.
PAT	Mithilfe von Port and Address Translation (PAT) werden die Quell- und Ziel-IP-Adressen sowie die Quell- und Ziel-Ports eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch NAT.
PBX	Private Branch Exchange (PBX) ist eine andere Bezeichnung für eine Telefonanlage.
Peer	Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.
Phase-1/2	Siehe IKE.
Pick-Up	Bei Pick-Up werden Anrufe über Kennzifferprozeduren an einem internen Endgerät entgegengenommen, das sich nicht in der aktiven Rufverteilung befindet.
PIM	Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.

PIN	Mithilfe einer persönlichen Identifikationsnummer (PIN) kann man sich am Gerät authentisieren und dadurch Funktionen des Geräts nutzen.
Ping	Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist. Daneben wird die Zeitspanne zwischen dem Aussenden eines Datenpakets (ICMP(v6)-Echo-Request-Paket) und dem Empfangen eines daraufhin unmittelbar zurückgeschickten Antwortpakets gemessen. Dadurch kann die Qualität der Verbindung ermittelt werden.
PKCS	Die Public-Key Cryptography Standards (PKCS) beinhalten Standards für Public-Key-Kryptografie. Die PKCS sind konzipiert für binäre und ASCII-Daten und sind kompatibel mit dem X.509-Standard. Die veröffentlichten Standards sind PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, und #15. PKCS #10 beschreibt die Syntax für Zertifizierungsanfragen.
PKI	Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.
PMTU	Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.
Point-to-Multipoint	Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).
Point-to-Point	Siehe Anlagenanschluss und Durchwahl (VoIP).
Pool	Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.
POP3	Das Post Office Protocol Version 3 (POP3) ist ein Übertragungsprotokoll, um den E-Mail-Abruf von einem E-Mail-Server durch einen Client zu steuern.
Port	Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, ...) ein ankommendes Datenpaket weitergeleitet wird.
POTS	Plain Old Telephone System (POTS) bezeichnet das analoge Telefonnetz.
PPP	Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.

PPPoA	Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.
PPPoE	Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.
PPTP	Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. PPTP verwendet die Protokollnummer 1723. Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP-Access-Concentrator (PAC) und den PPTP-Network-Server (PNS). Der PAC ist üblicherweise in den Windows Client integriert. Er stellt die Verbindung zum PNS her und verwaltet diese. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.
Präfix	Siehe Netzwerkadresse.
Präfixdelegation	In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.
Präfixlänge	Siehe Netzmaske.
Preshared Key	Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.
PRI	Siehe Primärmultiplexanschluss.
Primärmultiplexanschluss	Der Primärmultiplexanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Primary Rate Interface (PRI) oder S2M-Anschluss. Ein Primärmultiplexanschluss bietet in Europa 30 und in den USA 23 Nutzkanäle (B-Kanäle) mit je 64 kbit/s, einen Steuerkanal (D-Kanal) mit 64 kbit/s und einen Synchronisationskanal mit 64 kbit/s in Europa und 8 kbit/s in den USA. Siehe auch Basisanschluss.
Proposal	Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.
Protokoll	Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP

Proxy	Ein Proxy ist eine Netzwerkkomponente. Der Proxy ist ein Vermittler. Er leitet eine Anfrage der Quelle mit seiner eigenen IP-Adresse an das Ziel weiter.
PVID	Der Port VLAN Identifier (PVID) ist die Standard-VLAN-ID des jeweiligen Ports. Ein Paket, das ohne VLAN-Tag diesen Port erreicht, wird mit dieser ID versehen.
Q-SIG	Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.
QoS	Quality of Service (QoS) beschreibt die Qualität (Güte) des Kommunikationsdienstes. Diese wird anhand von Bandbreite, Verzögerung, Paketverlusten und Jitter definiert. Um zeitkritische Datenpakete für VoIP oder Videostreaming möglichst schnell zu übertragen, werden alle Datenpakete bei QoS in Gruppen sortiert und entsprechend ihrer Priorität im Netzwerk schneller oder langsamer weitergeleitet.
Queue	In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen. Der RADIUS-Server authentifiziert den Client z. B. mittels der Überprüfung von Benutzernamen und Kennwort. Siehe auch TACACS+.
Raumüberwachung	Die Raumüberwachung ist ein Leistungsmerkmal. Die Geräusche eines Zimmers können mitgehört werden.
RE-ADSL2	Siehe G.992.5.
Real Time Jitter Control	Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.
Regelkette	In einer Regelkette sind unterschiedliche Filterregeln zusammengefasst. Eine Filterregel wählt einen Teil des Datenverkehrs aufgrund bestimmter Merkmale, z. B. der Quell-IP-Adresse, aus und wendet auf diese Teilmenge eine Aktion an, z. B. blockieren.
Registrar	Der SIP-Server (Registrar) muss eingesetzt werden, falls die Teilnehmer eines VoIP-Gesprächs keine statischen IP-Adressen verwenden. Der SIP-Server registriert die IP-Adressen der Clients und sendet diese Informationen an den SIP-Proxy, der die Anrufe vermittelt. Meistens sind SIP-Proxy und SIP-Registrar identisch.

Repeater	Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.
Reset	Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.
RFC	Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.
Rijndael	Siehe AES.
RIP	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
RJ45	RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.
Roaming	Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.
Router	Ein Router ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze auf der Vermittlungsschicht des OSI-Modells. Datenpakete werden anhand von IP-Adressen übertragen. Über Routing-Tabellen werden die besten Wege (Routen) durch das Netzwerk festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle, z. B. OSPF oder RIP, aus.
Router Advertisement	Router Advertisements sind Nachrichten, die der Router ins Netzwerk sendet. Diese verkünden die Anwesenheit des Routers im Netz. Ferner werden mithilfe von Router 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.
Rückfrage	Bei der Rückfrage wird das Telefongespräch mit dem ersten Gesprächspartner gehalten, während man ein zweites Gespräch führt.
Rückruf bei besetzt	Siehe automatischer Rückruf bei besetzt (CCBS).
Rückruf bei Nicht-melden	Siehe automatischer Rückruf bei Nichtmelden (CCNR).
Rufnummernband	Siehe Rufnummernblock beim Anlagenanschluss.
Rufnummernblock	Siehe Anlagenanschluss und Durchwahl (VoIP).
Rufumleitung	Rufumleitung (Call Deflection, CD) ist ein Leistungsmerkmal. Ein Anruf kann weitergeleitet werden, ohne ihn vorher angenommen zu haben.
Rufverteilung	Bei der Rufverteilung in der Telefonanlage werden eingehende Telefongespräche bestimmten Rufnummern oder Anwendungen (Fernzugang, ISDN-Login, ...) zugeordnet.
Ruhe vor dem Telefon	Siehe Anrufschutz.
S0-Bus	Der S0-Bus ist eine Schnittstelle beim ISDN-Basisanschluss und verbindet mehrere ISDN-Endgeräte mit dem NTBA. Der Bus wird über eine Vierdraht-Verkabelung realisiert. Siehe auch UP0.
S2M-Anschluss	Siehe Primärmultiplexanschluss.
SA	Eine sogenannte Sicherheitsverbindungen (Security Associations, SA) enthält Informationen über die Maßnahmen zur Sicherung der

Kommunikationsverbindung. Mindestens eine SA ist die Voraussetzung für den Aufbau einer gesicherten Verbindung. Eine SA enthält die IP-Adresse des Teilnehmers, das verwendete Authentifizierungsprotokoll, den verwendeten Verschlüsselungsalgorithmus, den Sicherheits-Parameter-Index (SPI), den Selektor und die Gültigkeitsdauer.

SAD

Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die SAD enthält Informationen über jede Sicherheitsverbindung. Also welche Verschlüsselungsalgorithmen, Schlüssel, Protokolle, Sitzungsnummern oder Gültigkeitszeiträumen verwendet werden sollen. Für eine ausgehende Verbindung zeigt ein Eintrag der SPD auf einen Eintrag der SAD. Dadurch kann die SPD festlegen, welcher SA für ein bestimmtes Paket verwendet wird. Bei einer 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.

Schaltkontakt

Über ein Telefon kann eine am Schaltkontakt angeschlossene Anlage, z. B. ein Türöffner, ein- und ausgeschaltet werden.

Scheduling

Unter Scheduling versteht man einen Aufgabenplan. Bestimmte Aktionen (z. B. Deaktivierung einer Schnittstelle) werden durch Ereignisse (z. B. Zeit oder Änderung einer MIB-Variablen) ausgelöst.

Serielle Schnittstelle

Die serielle Schnittstelle dient dem Datenaustausch zwischen Computern und Peripheriegeräten. Sie kann zur Konfiguration des Geräts oder zur Datenübertragung über eine IP-Infrastruktur verwendet werden (Serial over IP).

Server

Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden.

SFP

Small Form-factor Pluggable (SFP) ist eine Steckverbindung, die für extrem schnelles Ethernet entwickelt wurde.

SHA1

Secure-Hash-Algorithm Version 1 (SHA1) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.

SHDSL

Symmetrical High-bit-rate Digital Subscriber Line. Siehe DSL.

Shell

Die Shell ist eine Eingabeschnittstelle (z. B. Kommandozeile oder

grafische Benutzerschnittstelle) zwischen Computer und Benutzer.

Shorthold	Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.
SIF	Bei einer Stateful Inspection Firewall (SIF) wird die Weiterleitung eines Datenpakets nicht nur durch Quell- und Zieladressen oder Port bestimmt, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung.
SIP	Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das Protokoll wird für IP-Telefonie (VoIP) verwendet.
SIP-Provider	Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.
SMTP	Das Simple Mail Transfer Protocol (SMTP) wird zum Austausch von E-Mails eingesetzt.
SNMP	Mithilfe des Simple Network Management Protocol (SNMP) werden verschiedene Netzwerkkomponenten (z. B. Router, Server, usw.) von einem zentralen System aus konfiguriert, kontrolliert und überwacht. Die änderbaren Einstellungen der Netzwerkkomponenten sind dabei in einer Datenbank gespeichert – der Management Information Base (MIB). SNMP verwendet UDP. Die Netzwerkkomponente empfängt dabei Anfragen (Requests) auf Port 161, während das verwaltende System Bestätigungsmeldungen (TRAPs) auf Port 162 entgegennimmt.
SNTP	Das Simple Network Time Protocol (SNTP) wird zur Zeitübertragung und Synchronisation zwischen Server und Client eingesetzt.
Softkey	Als Softkey bezeichnet man eine Taste, deren Funktion von der zugehörigen Bildschirmanzeige bestimmt wird.
Spatial Streams	Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der 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. Da-

zu werden Faktoren wie Quell- und Zieladresse des Datenpakets verwendet.

- Splitter** Mithilfe einer Breitbandanschlusseinheit (BBAE), umgangssprachlich Splitter, werden Signale, die über eine Teilnehmeranschlußleitung eintreffen, in Daten- und Telefonleitungen aufgeteilt.
- SRTP** Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die mithilfe von AES verschlüsselte Variante des Real-Time Transport Protocol (RTP).
- SSH** Secure Shell (SSH) ist ein Netzwerkprotokoll mit dem man eine verschlüsselte Verbindung zur Shell eines Geräts herstellen kann.
- SSID** Der Service Set Identifier (SSID) definiert ein Funknetzwerk, das auf IEEE 802.11 basiert. Der SSID ist der Netzwerkname des Wireless LAN. Alle Access Points und Clients, die zum gleichen Netzwerk gehören, verwenden denselben SSID. Die SSID-Zeichenfolge kann bis zu 32 Zeichen lang sein und wird allen Paketen unverschlüsselt vorangestellt. Mithilfe der SSID ANY kontaktiert ein Client alle erreichbaren Access Points. Dem Anwender werden daraufhin alle verfügbaren WLANs angezeigt und er kann das passende Netz auswählen. Wenn ein Access Point für verschiedene Netze verwendet wird, erhält jedes Funknetzwerk eine eigene MSSID (Multi Service Set Identifier).
- SSL** Secure Sockets Layer (SSL) ist ein Protokoll zur Datenverschlüsselung. Seit Version 3.1 wird die neue Bezeichnung Transport Layer Security (TLS) verwendet. SSL wird hauptsächlich für HTTPS verwendet, um die Datenübertragung zwischen Web-Server und Web-Browser zu verschlüsseln.
- STAC** Mithilfe von STAC wird die übertragene Datenmenge verringert (Datenkompression).
- Standardroute** Die Standardroute (Default Route) wird verwendet, falls keine andere passende Route vorhanden ist.
- Standardrouter** Siehe Default Gateway.
- Standleitung** Eine Standleitung (Leased Line) ist eine permanente Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz.
- Statische IP-Adresse** Im Gegensatz zu einer dynamischen IP-Adresse wird die statische IP-Adresse fest vom Anwender zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-

Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.

STUN-Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Ein STUN-Server ermöglicht VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Netzwerk.
Subadressierung	Neben der ISDN-Telefonnummer kann eine Subadresse beim Verbindungsaufbau übertragen werden. Diese Subadresse überträgt eine beliebige Zusatzinformation. Diese kann genutzt werden, um z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt anzusprechen oder bestimmte Programme auf einem PC aufzurufen.
Subnetz	Ein Teilnetz eines IP-Netzes wird als Subnetz bezeichnet. Ein Teilnetz wird wie ein normales Netzwerk über IP-Adresse und (Sub-)Netzmaske (IPv4) bzw. Präfixlänge (IPv6) definiert. Beispiel: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 mögliche IP-Adressen) ist ein Subnetz von 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 mögliche IP-Adressen).
Switch	Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerksegmente miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells 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.
Systemtelefon	Ein Systemtelefon ist mit mehreren Funktions- und Sondertasten ausgestattet und kann die Leistungsmerkmale einer Telefonanlage nutzen.
T.38	T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.

TA	Siehe Terminaladapter.
TACACS+	Das Terminal Access Controller Access Control System Plus (TACACS+) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern. Der TACACS+-Server authentifiziert den Client mittels der Überprüfung von z. B. Benutzername und Kennwort. Im Gegensatz zum UDP-basierten RADIUS-Protokoll verwendet TACACS+ TCP auf Port 49 und überträgt die gesamte Kommunikation verschlüsselt.
TAE	Siehe Netzabschluss. Man unterscheidet zwischen F-codierten Steckverbindern für Telefone und N-codierten Steckverbindern für Faxgeräte, Modems und Anrufbeantworter.
TAPI	Telephony Applications Programming Interface (TAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch CAPI.
TCP	Beim Transmission Control Protocol (TCP) handelt es sich um ein verbindungsorientiertes Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungsorientierten Protokoll wird vor der Übertragung eine logische Verbindung aufgebaut und aufrechterhalten. Dies ermöglicht eine zuverlässige Übertragung der Daten. Allerdings werden ständig Kontrollinformationen neben dem eigentlichen Datenpaketen übertragen. Dies führt zu einem Anstieg des übertragenen Datenvolumens. Siehe auch UDP.
TCP-ACK-Paket	Ein ACK-Signal (Acknowledgement = Bestätigung) wird bei einer Datenübertragung verwendet, um den Erhalt oder die Verarbeitung von Daten oder Befehlen zu bestätigen. TCP verwendet ACK-Signale zur Kommunikation.
TE	Der Endgeräteanschluss (Terminal Equipment, TE) bezeichnet einen Anschluss bzw. eine Betriebsart. Der TE-Anschluss ist der Anschluss eines Endgeräts. Im TE-Betrieb wird das Gateway am internen S0 der Telefonanlage angeschlossen und stellt damit ein ISDN-Endgerät dar. Siehe auch NT.
TEI	Der Terminal Endpoint Identifier (TEI) ist gemäß ISDN-Protokoll DSS1 eine Kennung zur Identifizierung der Endgeräte.
Telefax	Siehe Fax.
Telefonnummer des Angerufenen anzeigen	Mithilfe von Connected Line Identification Presentation (COLP) wird die Telefonnummer des Angerufenen (B-Telefonnummer) zum An-

gen (COLP / COLR)	rufers übertragen. Mithilfe von Connected Line Identification Restriction (COLR) wird die Übertragung der Telefonnummer des Angerufenen zum Anrufer unterdrückt.
Telefonnummer des Anrufers anzeigen (CLIP / CLIR)	Mithilfe von Calling Line Identification Presentation (CLIP) wird die Telefonnummer des Anrufers (A-Telefonnummer) zum Angerufenen übertragen. CLIP off Hook übermittelt die Telefonnummer des anklopfenden Anrufers. Mithilfe von Calling Line Identification Restriction (CLIR) wird die Übertragung der Telefonnummer des Anrufers zum Angerufenen unterdrückt.
Telefonnummer unterdrücken	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR) und Telefonnummer des Angerufenen anzeigen (COLP / COLR).
Telnet	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
Terminaladapter	Mithilfe eines Terminaladapters (TA) können Endgeräte an eine Schnittstelle angeschlossen werden, an der sie nicht direkt betrieben werden können, z. B. analoge Endgeräte an einem ISDN-Anschluss.
TFE	Eine Türfreisprecheinrichtung (TFE) ist an Eingängen montiert und ein Teil eines Türsprechsystems, z. B. einer Telefonanlage.
TFTP	Das Trivial File Transfer Protocol (TFTP) regelt die Übertragung von Dateien. Im Vergleich zu FTP fehlen eine Möglichkeit zur Dateianzeige, eine Rechtevergabe und eine Benutzerauthentifizierung.
Tiger 192	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Time Service	Mithilfe des Time Protocol (time) wird Datum und Uhrzeit synchronisiert. Das Protokoll verwendet den Port 37 über TCP und UDP.
TK-Anlage	TK-Anlage ist eine andere Bezeichnung für eine Telefonanlage.
TLS	Siehe SSL.
Tonwahl	Siehe Mehrfrequenzwahlverfahren.
TOS	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
Traceroute	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpa-

kete bis zum abgefragten Ziel-Host vermittelt werden.

Trigger	Unter Trigger versteht man einen Auslöseimpuls.
Triple DES	Siehe DES.
Trunk	Ein Trunk sind gebündelte Anschlüsse bzw. Übertragungskanäle. Siehe auch Bündel.
TTL	Die Time to live (TTL) ist die konfigurierte Gültigkeitsdauer eines Datenpakets. Beim Internet Protocol (IP) legt die TTL fest, wie viele Hops ein Datenpaket passieren darf. Der Maximalwert beträgt 255 Hops. Mit jedem Hop wird die TTL um 1 reduziert. Falls ein Datenpaket nach Ablauf seiner TTL noch nicht sein Ziel erreicht hat, wird es verworfen.
Twofish	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128,192 oder 256 Bit.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) ist eine DSL-Variante. Sie wurde als ANSI T1.413 entwickelt und als G.992.2 standardisiert. U-ADSL erlaubt die parallele Nutzung verschiedener Kommunikationstechniken, z. B. ISDN und POTS, und benötigt keinen Splitter.
Überprüfung der Rückroute	Falls bei einer Schnittstelle "Überprüfung der Rückroute" (Back Route Verify) aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden.
UDP	Beim User Datagram Protocol (UDP) handelt es sich um ein verbindungsloses Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungslosen Protokoll ist keine Kontrolle für die Auslieferung des Pakets integriert. Die Kontrolle muss in der Anwendungsschicht erfolgen. Im Gegenzug ist UDP schneller als verbindungsorientierte Protokolle.
ULA	Unique Local Addresses (ULA) sind IPv6-Adressen, die nicht geroutet werden. Sie können in privaten Netzen (z. B. einem LAN) verwendet werden. ULAs beginnen mit dem Präfix fd.
UMTS	Das Universal Mobile Telecommunications System (UMTS), auch als 3G bezeichnet, ist ein Mobilfunkstandard mit einer spezifizierten max. Datenübertragungsrate von 384 kbit/s bzw. 21 Mbit/s in Verbindung mit HSPA+.

Unicast	Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertragen.
UP0	Der UP0-Anschluss ist eine Schnittstelle beim ISDN-Basisanschluss und verbindet genau ein ISDN-Endgerät mit dem NTBA. Der Anschluss wird über eine Zweidraht-Verkabelung realisiert und bietet eine höhere Reichweite als der S0-Bus.
UPnP	Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.
Upstream	Das Gateway leitet die Daten des eigenen Netzwerks weiter.
URL	Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: http://www.example.org/index.htm (Web-Seite im Internet)
UUS	Bei User to User Signalling (USS) können Textnachrichten mit anderen Teilnehmern ausgetauscht werden.
V.110	V.110 beschreibt ein Verfahren zur Anpassung von Bitströmen mit 0,6, 1,2, 2,4, 2,8, 7,2, 9,6, 12, 14,4, 19,2 und 38,4 kbit/s in den ISDN-Bitstrom von 64 kbit/s.
VDSL	Very High Speed Digital Subscriber Line. Siehe DSL.
VID	Siehe VLAN.
VLAN	Ein Netzwerk kann in eines oder mehrere logische Teilnetze – sogenannte Virtual-Local-Area-Networks (VLAN) – aufgespalten werden, indem die Netzwerkkomponenten das Datenpaket eines definierten Teilnetzes nicht mehr in andere Teilnetze weiterleiten. Jedem VLAN wird eine eindeutige Nummer zugeordnet. Diese Nummer wird VLAN ID (VID) genannt und den Datenpaketen im VLAN-Tag zugeordnet.
Voice Mail Box	Eine Voice Mail Box ist der persönliche Anrufbeantworter eines Benutzers in einem Voice Mail System.
Voice Mail System	Ein Voice Mail System ermöglicht das Speichern, Abrufen und Weiterleiten von Sprachmitteilungen ähnlich wie ein Anrufbeantworter, jedoch mit weitaus mehr Optionen.
VoIP	Voice over IP (VoIP), auch IP-Telefonie genannt, bezeichnet die Übertragung von Sprache über ein IP-Netzwerk. Der Auf- und Abbau der Telefonverbindung erfolgt dabei über Signalisierungsproto-

kolle, wie z. B. SIP.

VPN	Mithilfe eines virtuellen privaten Netzwerks (VPN) werden private Datenpakete durch ein öffentliches Netzwerk transportiert. Die Informationen werden dabei durch Einkapselung in neue Protokolle von den öffentlich zugänglichen Daten getrennt, um sie an den vorgesehenen Empfänger zu leiten. Man spricht in diesem Zusammenhang auch von einem Tunnel, der zwischen den privaten Netzen der beiden Verbindungsteilnehmer aufgebaut wird. VPN-Protokolle sind IP-Sec, PPTP, L2TP und GRE.
VSS	Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.
Wahlberechtigung	Siehe Amtsberechtigung.
Wahlkontrolle	Siehe Black / White List.
Wahlregeln	Mithilfe der Wahlregeln können Anrufe abhängig von der gewählten Rufnummer (Zone) über festgelegte Provider bzw. Bündel geleitet werden.
Wählverbindung	Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.
Wahlvorbereitung	Die Wahlvorbereitung beschreibt die Eingabe der Telefonnummer vor dem Einleiten des Gesprächs, z. B. durch Abheben des Hörers.
Walled Garden	Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.
WAN	Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausge dehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.
Wartemusik	Siehe Music On Hold.
WDS	Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.
Web-Server	Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.
Wechselsprechen	Wechselsprechen ist ein Leistungsmerkmal. Mithilfe der Wechselsprechfunktion wird ein Anruf automatisch angenommen und Laut hören eingeschaltet. Hebt der angerufene Teilnehmer den Hörer ab,

wird eine normale Sprechverbindung hergestellt.

WEP	Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.
WINS	Der Windows Internet Name Service (WINS) ist eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft. Wie DNS dient WINS der zentralen Namensauflösung. Siehe auch DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.
WMM	Wi-Fi Multimedia (WMM) priorisiert die Datenpakete unterschiedlicher Anwendungen und verbessert damit die Übertragung von Sprach-, Musik- und Videodaten in WLAN-Netzwerken. Dazu stellt WMM Quality-of-Service-Merkmale (QoS) für IEEE 802.11-basierte Netzwerke bereit.
WPA	Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.
WPA - Enterprise	WPA - Enterprise bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmer durch das Extensible Authentication Protocol (EAP). Nach erfolgreicher Authentisierung übermittelt der Server dem Client und dem Access Point einen gemeinsamen Schlüssel für die Datenübertragung im WLAN.
WPA - PSK	WPA - PSK bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmern über Preshared Keys. Dabei nutzen Access Point und Client die gleiche Zeichenfolge für die Schlüsselberechnung im WLAN. Diese Zeichenfolge muss von den Anwendern konfiguriert werden.
WPA 2	Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.
X.25	X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.
X.31	Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.
X.500	Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.
X.509	Der X.509-Standard beschreibt die Erstellung der Zertifikate für eine

Public-Key-Infrastruktur (PKI).

- X.75** X.75 ist eine standardisierte Protokollfamilie für ISDN-Netzwerke mit einer Übertragungsrate von 64 kbit/s.
- XAuth** Mithilfe von XAUTH (Extended Authentication) wird IKE um weitere Authentifizierungsmechanismen ergänzt. Nach einer erfolgreichen IKE-Phase-1-Authentifizierung kann der Benutzer noch einmal separat identifiziert werden. Die Identifizierung erfolgt über Benutzername und Passwort, PAP, CHAP oder Hardware-basierte Systeme.
- Zeitschlitz** Ein Zeitschlitz ist ein fest zugeordneter Zeitabschnitt innerhalb eines Übertragungsrahmens und entspricht meist einem Übertragungskanal.
- Zertifikat** Ein Zertifikat identifiziert eine Person, eine Institution, ein Gerät oder eine Anwendung. Ein Public-Key-Zertifikat ist ein digitales Zertifikat und stellt eine Verbindung zwischen der Identität und einem öffentlichen Schlüssel her. Zertifikate mit öffentlichem Schlüssel werden von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt. Nicht mehr vertrauenswürdige Zertifikate können über Zertifikatsperrlisten (Certificate Revocation List, CRL) deaktiviert werden.
- Zone** Unter einer Zone versteht man eine Rufnummer oder mehrere Rufnummern, die mit der gleichen Sequenz beginnen.

Index

- Aktiver Allgemeiner Präfix 156
- Benutzter Präfix/Länge 156
- Name 156
- Typ 156
- Von Schnittstelle 156
- Abfrage Intervall 204
- Address assignment 358
- Admin-Status 173
- Administrative FQDNs 362
- Administrativer Status 247 , 309 , 324 , 326 , 336
- Adressbereich 294
- Adresse/Präfix 294
- Adresse/Subnetz 294
- Adressen 316
- Adressmodus 97 , 235
- Adresstyp 294
- Ähnliches Zertifikat überschreiben 372
- Airtime Fairness 125
- Aktion 160 , 198 , 286 , 288 , 372 , 399
- Aktives Funkmodulprofil 122
- Aktualisierung aktivieren 344
- Aktualisierungsintervall 345
- Aktualisierungspfad 345
- Alle Multicast-Gruppen 207
- Allgemeiner Name 69
- Allgemeiner Präfix 101
- Analoge Schnittstelle auswählen 303
- Angerufene Adresse 309
- Angerufene Adresse 324 , 327
- Angerufene Leitung 327
- Ankommende Rufnummer 262
- Ankündigen 100
- Anrufende Adresse 324
- Anrufende Leitung 324
- Antwort 338
- Antwortintervall (Letztes Mitglied) 204
- Anzahl der Spatial Streams 125
- Anzahl erlaubter Verbindungen 255
- Anzahl Nachrichten 416
- APN 352
- ARP Processing 131
- Art der Einrichtung 101
- Art des Datenverkehrs 159
- ATM PVC 222
- ATM-Dienstkategorie 237
- ATM-Schnittstelle 233
- Ausgehende Rufnummer 262
- Ausgehende Schnittstelle 189
- Ausgehender Proxy 309
- Ausstehende Ende-
zu-Ende-Anforderungen 240
- Ausstehende Segment-Anforderungen 240
- Auswahl 295
- Auswahl des Client-Bands 134
- Auszuführende Aktion 389
- Authentifizierung 215 , 219 , 225 , 229
- Authentifizierungs-ID 303 , 309
- Authentifizierungsmethode 247 , 264
- Authentifizierungstyp 55
- Automatische Subnetzerstellung 101
- Autonomous Flag 103
- Autospeichermodus 70
- Autospeichermodus 372
- Bandbreite 125
- Bandbreitenbegrenzung Downstream 316
- Bandbreitenbegrenzung Upstream 316
- Basierend auf Ethernet-Schnittstelle 96
- Beacon Period 128
- Bedingung des Schnittstellenverkehrs 366
- Bedingung für Ereignisliste 372
- Befehlsmodus 372
- Befehlstyp 372
- Beinhalteter Standort (Parent) 316
- Benachrichtigungsdienst 416
- Benutzer 63 , 277
- Benutzer muss das Passwort ändern

- 63
- Benutzerdefiniert 69
- Benutzerdefinierte DHCP-Optionen 351
- Benutzerdefinierter Kanalplan 128
- Benutzername 210 , 217 , 222 , 227 , 309 , 344 , 363
- Berichtsmethode 200
- Berücksichtigen 169
- Beschreibung 60 , 65 , 73 , 122 , 125 , 148 , 159 , 173 , 179 , 183 , 189 , 194 , 198 , 210 , 217 , 222 , 227 , 233 , 247 , 254 , 264 , 272 , 277 , 292 , 293 , 294 , 295 , 296 , 298 , 303 , 309 , 316 , 319 , 324 , 327 , 329 , 336 , 353 , 366 , 372 , 395 , 399
- Beschreibung 151
- Betreff 416
- Betreibermodus 55
- Betriebsmodus 122 , 125
- Bevorzugte Gültigkeitsdauer 103
- Blockieren nach Verbindungsfehler für 215 , 219 , 225 , 229
- Blockzeit 269
- Burst-Größe 189
- Burst-Mode 125
- CA-Name 372
- CA-Zertifikat 67
- CA-Zertifikate 269
- CAPWAP-Verschlüsselung 122
- Client FQDN akzeptieren 362
- Client-Typ 236
- Code 296
- Codec-Reihenfolge 306 , 313
- Comfort Noise Generation (CNG) 307 , 315
- Continuity Check (CC) Ende-zu-Ende 242
- Continuity Check (CC) Segment 242
- COS-Filter (802.1p/Layer 2) 179 , 194 , 395
- CRL verwenden 372
- CSV-Dateiformat 372
- Dateikodierung 71 , 72
- Dateiname 372
- Dateiname auf Server 372
- Dateiname in Flash 372
- DH-Gruppe 264
- DHCP Broadcast Flag 104
- DHCP-Client 98
- DHCP-Client 213 , 224
- DHCP-Hostname 104 , 235
- DHCP-MAC-Adresse 104 , 235
- DHCP-Modus 105
- DHCP-Optionen 349
- DHCP-Server 98
- Dienst 160 , 173 , 179 , 194 , 286 , 288 , 395
- DNS-Aushandlung 215 , 219 , 225 , 229
- DNS-Domänen-Suchliste 359
- DNS-Hostname 338
- DNS-Propagation 105
- DNS-Server 231 , 278 , 347 , 359
- Drahtloser Modus 125
- Dropping-Algorithmus 191
- DSCP / Traffic Class Filter (Layer 3) 179 , 194 , 395
- DSCP-/TOS-Wert 148
- DSCP-Einstellungen für RTP-Daten 318
- DSCP/Traffic-Class-Filter setzen (Layer 3) 183
- DTIM Period 128
- DUID 362
- Durchsatz 139
- Durchsatz/Client 139
- Dynamische Black List 136
- E-Mail 69
- EAP-Vorabauthentifizierung 132
- Echounterdrückung 307 , 315
- Eigene IP-Adresse per ISDN/GSM übertragen 262
- Eintrag aktiv 55
- Empfänger 416
- Ende-zu-Ende-Sendeintervall 240
- Enkapsulierung 233

- Entfernte PPTP-IP-Adresse 219
- Entferntes IPv6-Netzwerk 252
- Enthaltene Zeichenfolge 416
- Ereignis 416
- Ereignisliste 366 , 372
- Ereignistyp 366
- Erfolgreiche Versuche 366 , 389
- Erlaubte Adressen 136
- Erreichbarkeitsprüfung 56 , 269 , 275
- Erzeugungsmethode 102
- Externe Adresse 329
- Externer Dateiname 71 , 72
- Facility 413
- Fehlgeschlagene Versuche 366 , 389
- Fehlversuche per Zeitraum 136
- Filter 183
- Fragmentation Threshold 128
- Frequenzband 125
- Gateway 349
- Gateway-Adresse 151
- Gateway-IP-Adresse 147
- GEO Zone Status 366
- Gerät 122
- Gewichtung 189
- Größe des Protokoll-Headers unterhalb
Layer 3 186
- Gruppen-ID 388
- Gruppenbeschreibung 55 , 169 , 170
- Gültigkeit 303 , 309
- Gültigkeitsdauer 103
- Hersteller auswählen 351 , 352
- Herstellerbeschreibung 351 , 352
- High-Priority-Klasse 183
- Hinzuzufügende/zu bearbeitende MIB/
SNMP-Variable 372
- Hostname 344
- IKE (Internet Key Exchange) 247
- Immer aktiv 210 , 217 , 222 , 227
- Indexvariablen 366 , 372
- Intervall 366 , 372 , 389 , 392
- Intra-cell Repeating 131
- IP-Adressbereich 231 , 278 , 347
- IP-Adresse 235 , 236 , 353 , 413
- IP-Adresse / Netzmaske 97
- IP-Adresse zur Nachverfolgung 171
- IP-Adressmodus 212 , 218 , 223 , 228
- IP-Komprimierung 275
- IP-Poolname 231 , 278 , 347 , 348
- IP-Version 295
- IP-Version 336
- IP-Version des Tunnelnetzwerks 247
- IP-Zuordnungspool 250
- IPv4 294
- IPv4 Proxy ARP 257
- IPv4-Adresse 338
- IPv4-Adressvergabe 250
- IPv4-Quelladresse/-netzmaske 179 ,
194 , 395
- IPv4-Zieladresse/-netzmaske 179 ,
194 , 395
- IPv6 98 , 213 , 224 , 294
- IPv6-Adresse 338
- IPv6-Adressen 98
- IPv6-Modus 98 , 213 , 224
- IPv6-Quelladresse/-länge 179 , 194 ,
395
- IPv6-Zieladresse/-länge 179 , 194 ,
395
- ISDN-Modus 319
- ISDN-Schnittstelle auswählen 303
- Kanal 122
- Kanalplan 128
- Kennung der statischen Schnittstelle
362
- Kennwort für geschütztes Zertifikat
372
- Klassen-ID 183 , 189
- Klassenplan 183
- Konfiguration verschlüsseln 372
- Konfiguration enthält Zertifikate/Schlüs-
sel 372
- Konfiguration speichern 60
- Konfigurationsmodus 250
- Kontrollmodus 186 , 244
- Land 69
- Layer 4-Protokoll 148
- LCP-Erreichbarkeitsprüfung 215 , 219
, 225 , 229

- LDAP-URL-Pfad 73
- Lease Time 349
- Lebensdauer 264 , 272
- Leitung 326
- Level 413
- Level Nr. 60
- Link-Präfix 101
- Lizenzschlüssel 46
- Lizenzseriennummer 46
- Lokale Zertifikatsbeschreibung 71 ,
72 , 372
- Lokale Adresse 329
- Lokale ID 247
- Lokale IP-Adresse 147 , 212 , 218 ,
223 , 228 , 250
- Lokale PPTP-IP-Adresse 219
- Lokale WLAN-SSID 372
- Lokaler Dateiname 372
- Lokaler ID-Typ 247 , 264
- Lokaler ID-Wert 264
- Lokales IPv6-Netzwerk 252
- Lokales Zertifikat 264
- Long Retry Limit 128
- Loopback Ende-zu-Ende 240
- Loopback-Segment 240
- MAC-Adresse 96 , 235 , 353
- Mail-Exchanger (MX) 345
- Max. Anzahl Clients - Hard Limit 134
- Max. Anzahl Clients - Soft Limit 134
- Max. Queue-Größe 191
- Max. Übertragungsrate 125
- Maximale Downstream-Bandbreite
316
- Maximale Upload-Geschwindigkeit
186 , 189 , 244
- Maximale Upstream-Bandbreite 316
- Maximale Antwortzeit 204
- Maximale Anzahl der erneuten Einwähl-
versuche 215 , 219 , 225 , 229
- Maximale Anzahl der IGMP-
Statusmeldungen 204
- Maximale Burst-Größe (MBS) 237
- Menüs 61
- Metrik 147 , 151 , 154 , 250
- MIB-Variablen 372
- Min. Queue-Größe 191
- Mitglieder 292 , 293 , 298 , 319
- MobiKE 257
- Modus 67 , 148 , 204 , 262 , 264 ,
277
- Modus des D-Kanals 262
- Monitored GEO Zone 366
- MTU 216
- Multicast-Gruppen-Adresse 207
- Nach Ausführung neu starten 372
- Nachrichtenkomprimierung 416
- Nachrichtentyp 413
- Name 122 , 277 , 358
- NAT-Eintrag erstellen 212 , 218 , 223
, 228
- NAT-Methode 159
- NAT-Traversal 269
- Netzmaske 235 , 236
- Netzwerkname (SSID) 131
- Neue Quell-IP-Adresse/Netzmaske
164
- Neue Ziel-IP-Adresse/Netzmaske 164
- Neuer Quell-Port 164
- Neuer Ziel-Port 164
- Neustart des Geräts nach 372
- OAM-Fluss-Level 240
- Öffentliche IPv4-Quelladresse 257
- Öffentliche Schnittstelle 257
- Öffentlicher Schnittstellenmodus 257
- On Link Flag 103
- Organisation 69
- Organisationseinheit 69
- Original Quell-Port/Bereich 160
- Original Ziel-IP-Adresse/Netzmaske
160
- Original Ziel-Port/Bereich 160
- Originale Quell-IP-Adresse/Netzmaske
160
- Ort 69
- Paketgröße 307 , 315
- Passwort 63 , 67 , 71 , 72 , 210 , 217
, 222 , 227 , 277 , 303 , 309 , 344 ,
363 , 372 , 399

- Peak Cell Rate (PCR) 237
- Peer-Adresse 247
- Peer-ID 247
- PFS-Gruppe verwenden 272
- Phase-1-Profil 255
- Phase-2-Profil 255
- PIN 352
- PMTU propagieren 275
- Pool-Verwendung 348
- Port 303, 345
- PPPoE-Ethernet-Schnittstelle 210
- PPPoE-Modus 210
- PPPoE-Schnittstelle für Mehrfachlink 210
- PPTP-Adressmodus 219
- PPTP-Ethernet-Schnittstelle 217
- Preshared Key 132, 247
- Primärer IPv4-DNS-Server 336
- Primärer IPv6-DNS-Server 336
- Priorisierungsalgorithmus 186
- Priorität 55, 189, 326, 336
- Priority Queueing 189
- Privaten Schlüssel generieren 67
- Proposals 264, 272
- Protokoll 154, 160, 173, 179, 194, 254, 296, 303, 309, 345, 372, 395, 413
- Provider 233, 344
- Providename 345
- Provisioning-Server 351
- Proxy ARP 104
- Quell-IP-Adresse 366, 372
- Quell-IP-Adresse 389, 392
- Quell-IP-Adresse/Netzmaske 148, 160, 173, 254
- Quell-Port 148, 254
- Quell-Port/Bereich 160, 173, 179, 194, 395
- Quelladresse/Länge 151
- Quelle 286, 288, 372
- Quellportbereich 296
- Quellschnittstelle 148, 173, 207
- Queues/Richtlinien 186
- RA-Signierungszertifikat 67
- RA-Verschlüsselungszertifikat 67
- RADIUS-Dialout 56
- RADIUS-Passwort 55
- RADIUS-Server 132
- RADIUS-Server Gruppen-ID 277
- Real Time Jitter Control 186
- Realm 309
- Regelkette 198, 200, 401
- Registrar 309
- Registrierung 303, 309
- Richtlinie 56
- Richtung 183, 329
- Richtung des Datenverkehrs 366
- Robustheit 204
- Rolle 277
- Route 154
- Route aktiv 151
- Routeneinträge 212, 218, 223, 228, 250
- Routenklasse 146
- Routenselektor 171
- Routentyp 146, 151
- Router Advertisement annehmen 98, 213, 224
- Router Advertisement übertragen 98
- Router-Gültigkeitsdauer 105
- Router-Präferenz 105
- RTS Threshold 128
- RTT-Modus (Realtime-Traffic-Modus) 189
- Rufnummer 312, 327
- Rx Shaping 137
- SCEP-Server-URL 372
- SCEP-URL 67
- Schlüsselgröße 372
- Schnittstelle 49, 50, 53, 146, 154, 159, 170, 186, 200, 204, 244, 336, 344, 348, 358, 372, 391, 401
- Schnittstellen 183, 316
- Schnittstellenaktion 391
- Schnittstellenmodus 96, 336
- Schnittstellenstatus 366
- Schnittstellenstatus festlegen 372

- Schnittstellentyp 303
- Schweregrad 416
- Segment-Sendeintervall 240
- Sekundärer IPv4-DNS-Server 336
- Sekundärer IPv6-DNS-Server 336
- Sende WOL-Paket über Schnittstelle 399
- Sendeleistung 122
- Server 345
- Server Timeout 56
- Server-IP-Adresse 55
- Server-URL 372
- Serveradresse 372
- Setze COS Wert (802.1p/Layer 2) 183
- Short Guard Interval 128
- Short Retry Limit 128
- Sicherheitsmodus 132
- Sicherheitsrichtlinie 97, 98, 212, 213, 218, 223, 224, 250, 252
- SIP-Endpunkt-IP-Adresse 303, 309
- SIP-Header-Feld(er) für Anruferadresse 312
- SNTP-Server 359
- Sortierreihenfolge 306, 313
- Special Handling Timer 173
- Sperrzeit für Black List 136
- Staat/Provinz 69
- Standard-Benutzerpasswort 55
- Standard-Ethernet für PPPoE-Schnittstellen 235
- Standardroute 212, 218, 223, 228, 250
- Standort 122
- Startmodus 255
- Startzeit 371
- Statische Adressen 102
- Status 366
- Status der Funktionstaste 366
- Status des Auslösers 372
- Status festlegen 372
- Stoppzeit 371
- Subjektnamen 372
- Subnetz-ID 101
- Sustained Cell Rate (SCR) 237
- TCP-ACK-Pakete priorisieren 215, 219, 225, 229, 236
- TCP-MSS-Clamping 104
- Teilnehmer / Benutzername 303
- Timeout bei Inaktivität 210, 217, 222, 227
- Timeout für Nachrichten 416
- Traffic Shaping 189
- Traffic Shaping 186
- Transformation der gerufenen Adresse 326
- Transformation der rufenden Adresse 327
- Transparente MAC-Adresse 50
- Trigger 391
- Trunk-Modus 309
- Tx Shaping 137
- Typ 179, 194, 233, 296, 316, 324, 395, 399
- Überbuchen zugelassen 189
- Überprüfung anhand einer Zertifikatsperlliste (CRL) 65
- Überprüfung der IPv4-Rückroute 257
- Übertragener Datenverkehr 366
- Übertragungsmodus 262
- Übertragungsschlüssel 132
- Überwachte Schnittstelle 366
- Überwachte Subsysteme 416
- Überwachte Variable 366
- Überwachte IP-Adresse 389
- Überwachte Schnittstelle 391
- Überwachtes Zertifikat 366
- UDP-Port 56
- UMTS/LTE-Schnittstelle 227
- Unveränderliche Parameter 175
- Vendor Option String 352
- Verbindungsstatus 179, 194, 395
- Verbleibende Gültigkeitsdauer 366
- Verbundene Clients 139
- Vergleichsbedingung 366
- Vergleichswert 366
- Vermeidung von Datenstau (RED) 191

- Verschlüsselungsmethode 186
- Versionsprüfung 372
- Versuche 372 , 392
- Verteilungsmodus 169
- Verteilungsrichtlinie 169 , 170
- Verteilungsverhältnis 170
- Vertrauenswürdigkeit des Zertifikats erzwingen 65
- Verwendeter Kanal 122
- Verwerfen ohne Rückmeldung 200
- Virtual Channel Connection (VCC) 237 , 240
- Virtual Channel Identifier (VCI) 233
- Virtual Path Connection (VPC) 240
- Virtual Path Identifier (VPI) 233
- VLAN 137 , 210
- VLAN Identifier 108
- VLAN-ID 96 , 137 , 210
- VLAN-Mitglieder 108
- VLAN-Name 108
- Wake-on-LAN-Filter 399
- Wake-On-LAN-Regelkette 399
- Wiederholungen 56
- Wiederkehrender Hintergrund-Scan 128
- Wildcard 345
- Wildcard-MAC-Adresse 50
- Wildcard-Modus 50
- WLAN-Modul auswählen 372
- WLC-SSID 372
- WMM 131
- WPA Cipher 132
- WPA-Modus 132
- WPA2 Cipher 132
- XAUTH-Profil 255
- Zeitbedingung 371
- Zeitstempel 413
- Zertifikat in Konfiguration schreiben 372
- Zertifikat ist ein CA-Zertifikat 65
- Zertifikatsanforderungsbeschreibung 67 , 372
- Ziel 286 , 288
- Ziel-IP-Adresse 366 , 372 , 392
- Ziel-IP-Adresse/Netzmaske 147 , 160 , 173 , 254
- Ziel-MAC-Adresse 399
- Ziel-Port/Bereich 160 , 173 , 179 , 194 , 395
- Zieladresse/Länge 151
- Zielport 148 , 254
- Zielportbereich 296
- Zielschnittstelle 207
- Zielschnittstelle 151
- Zugangs-Level 63
- Zugeordnete Leitung 329
- Zugewiesene Drahtlosnetzwerke (VSS) 122
- Zugriff 363
- Zugriffsfilter 198
- Zugriffskontrolle 136
- Zum SNMP Browser wechseln 60
- Zusammenfassend 69
- Zusätzlicher Filter des IPv4-Datenverkehrs 252 , 254
- 2,4/5-GHz-Übergang 431
- Abgewiesene Clients soft/hard 431
- ADSL-Logik 407
- Aktion 144 , 407 , 421 , 426
- Aktive Clients 431
- Aktuelle Ortszeit 41
- Aktueller Dateiname im Flash 407
- Als DHCP-Server 335
- Als IPCP-Server 335
- Alternative Schnittstelle, um DNS-Server zu erhalten 334
- Andere Inaktivität 291
- Angegriffener Access Point 142
- Anrufrkontrolle für lokale Nummern 320
- AP gefunden 138
- AP offline 138
- AP verwaltet 138
- Art des Angriffs 142
- Auf Client-Anfrage antworten 394
- Aushandlungsmodus 422
- Ausloggen 404
- Authentifizierung für PPP-Einwahl 59

- Authentifizierungsmethode 422
- Benachrichtigungsdienst 418
- Benutzer 403
- Benutzername 419
- Beschreibung 421 , 422 , 426 , 426 , 428
- BOSS 407
- Bridge-Link-Beschreibung 431 , 432
- Bytes 422
- Cache-Größe 334
- Cache-Treffer 342
- Cache-Trefferrate (%) 342
- Client-MAC-Adresse 430
- CPU-Last [%] 138
- CRLs senden 281
- CTS Frames als Antwort auf RTS empfangen 428
- Datei auswählen 407
- Dateiname 407
- Datenrate Mbit/s 429 , 430
- Datum 421
- Datum einstellen 41
- Dauer 424 , 425
- Details 421
- DHCP-Server 117
- Dienst 424 , 425
- DNS-Anfragen 342
- DNS-Domänen-Suchliste 360
- DNS-Server 361
- Domänenname 334
- Doppelte empfangene MSDUs 428
- Dritter Zeitserver 41
- Durchsatz 140
- Dynamische RADIUS-Authentifizierung 280
- E-Mail-Adresse 419
- Empfangene DNS-Pakete 342
- Entfernte IP-Adresse 403
- Entfernte ID 422
- Entfernte IP-Adresse 421 , 422
- Entfernte MAC 431 , 432
- Entfernte Netzwerke 421
- Entfernte Nummer 424 , 425
- Entfernter Port 422 , 427
- Erfolgreich beantwortete Anfragen 342
- Erfolgreich empfangene Multicast-MS-DUs 428
- Erfolgreich übertragene Multicast-MS-DUs 428
- Erreichbarkeitsprüfung 422
- Erster Zeitserver 41
- Erweiterte Route 153
- Faxkopfzeile 364
- Fehler 143 , 422 , 424
- Fehlerhafte Erhaltene Pakete 428
- Fertig 143
- Firewall auf Werkseinstellungen zurücksetzen 292
- Frame-Übertragungen ohne ACK 428
- Frames ohne Tag verwerfen 109
- Gateway 153
- Gesamt 424
- Größe der Zero Cookies 280
- HTTPS-TCP-Port 342
- IGMP-Status 206
- IKE (Phase-1) 424
- IKE (Phase-1) SAs 422
- Image bereits vorhanden. 143
- Importieren 71 , 72
- Initial Contact Message senden 280
- Interface selection 401
- IP-Adressbereich 117
- IP-Adresse 429 , 430
- IP-Adresse/Netzmaske 426
- IPSec (Phase-2) 424
- IPSec (Phase-2) SAs 422
- IPSec aktivieren 279
- IPSec über TCP 280
- IPSec-Debug-Level 279
- IPSec-Tunnel 423
- ISDN-Zeitserver 41
- Kanal 424
- Key Hash Payloads senden 281
- Klasse 403
- Konfigurationsschnittstelle 49
- Kontakt 36
- Kosten 424 , 425

- Kurzwahl 323
- Läuft ab 403
- LED-Modus 36
- Level 421
- Lokale Adresse 427
- Lokale ID 422
- Lokale IP-Adresse 422
- Lokaler Port 422 , 427
- Lokales Zertifikat 342
- Loopback aktiv 158
- Löschen 142 , 153
- MAC-Adresse 426 , 429 , 431 , 432
- MAC-Adresse des Rogue Clients 142
- Manuelle IP-Adresse des WLAN-Controller 36
- Maximale Anzahl der Accounting-Protokolleinträge 36
- Maximale Anzahl der IGMP-Statusmeldungen 206
- Maximale Anzahl der Syslog-Protokolleinträge 36
- Maximale E-Mails pro Minute 418
- Maximale Gruppen 206
- Maximale Quellen 206
- Maximale SMS pro Tag 420
- Maximale TTL für negative Cacheeinträge 334
- Maximale TTL für positive Cacheeinträge 334
- Maximales Nachrichtenlevel von Systemprotokolleinträgen 36
- Mbit/s 427
- Media Stream Termination 320
- Metrik 153
- Modus 155 , 206
- Modus / Bridge-Gruppe 49
- MSDUs, die nicht übertragen werden konnten 428
- MTU 422
- Multicast-Routing 203
- Nachricht 421
- Nachrichten 422
- Name der Quelldatei 407
- Name der Zieldatei 407
- NAT 426
- NAT aktiv 158
- NAT-Erkennung 422
- Negativer Cache 334
- Netzmaske 153
- Netzwerkname (SSID) 142
- Netzwerkname (SSID) 431
- Neuer Dateiname 407
- Nicht entschlüsselbare MPDUs erhalten 428
- Nicht geändert seit 426
- Nicht-Mitglieder verwerfen 109
- Nr. 155 , 421 , 426
- Pakete 422
- Passwort 419
- Passwörter und Schlüssel als Klartext anzeigen 39
- Ping-Befehl testweise an Adresse senden 404
- POP3-Server 419
- POP3-Timeout 419
- Port 432
- Portweiterleitungen 158
- Positiver Cache 334
- PPTP-Inaktivität 291
- PPTP-Passthrough 158
- Primärer DHCP-Server 353
- Protokoll 153
- Protokollformat 415
- PVID 109
- QoS-Queue 433
- Quelle 144 , 407
- Queued 433
- Rate 430 , 432
- Rauschen dBm 429 , 430 , 431 , 432
- Region 117
- Remote-Adresse 427
- Richtung 424 , 425
- Routentyp 153
- RTS Frames ohne CTS 428
- Rx-Bytes 426 , 426
- Rx-Fehler 426
- Rx-Pakete 426 , 426 , 427 , 429 , 430 , 431 , 432

- SAs mit dem Status der ISP-
 - Schnittstelle synchronisieren 280
- Schedule-Intervall 384
- Schnittstelle 109 , 117 , 153 , 155 ,
 - 394 , 424 , 425 , 433
- Schnittstelle ist UPnP-kontrolliert 394
- Schnittstellenbeschreibung 49
- Sekundärer DHCP-Server 353
- Senden 433
- Server aktivieren 364
- Server-Priorität 360
- Serverfehler 342
- Session Border Controller Modus 320
- Sicherheitsalgorithmus 421
- Signal 140
- Signal dBm 142 , 429
- Slave-AP-LED-Modus 117
- Slave-AP-Standort 117
- SMS-Gerät 420
- SMTP-Authentifizierung 419
- SMTP-Port 419
- SMTP-Server 419
- SNMP Read Community 39
- SNMP Write Community 39
- SNR dB 430
- SNTP-Server 361
- Sofort ausloggen 403
- Speicherverbrauch [%] 138
- SSID 142
- Stack 424
- Standard-Abwurfnebenstelle 320
- Standardeinstellungen wiederherstellen
 - 52
- Standardverhalten 316
- Standort 36
- Startzeit 425
- Statische Black List 142
- Status 421 , 423 , 424 , 426 , 427
- Status des Media Gateways 320
- Subsystem 421
- System als Zeitserver 41
- Systemadministrator-Passwort 39
- Systemadministrator-Passwort bestätigen
 - 39
- Systemlogik 407
- Systemname 36
- TCP-Inaktivität 291
- TCP-Port des CAPI-Servers 364
- Test-Ping-Modus 404
- Trace mode 401
- Traceroute-Adresse 405
- Traceroute-Modus 405
- Tx-Bytes 426 , 426
- Tx-Fehler 426
- Tx-Pakete 426 , 426 , 427 , 429 , 430
 - , 431 , 432
- Typ 426
- Überprüfung der Rückroute 155
- Übersicht 139
- Übertragene MPDUs 428
- UDP-Inaktivität 291
- Ungültige DNS-Pakete 342
- Unicast MPDUs erfolgreich erhalten
 - 428
- Unicast MSDUs erfolgreich übertragen
 - 428
- UPnP TCP Port 394
- UPnP-Status 394
- Uptime 429 , 430 , 431
- URL 144 , 407
- Verbundene Clients/VSS 138
- Verschlüsselt 424
- Verschlüsselung der Konfiguration
 - 407
- Verwaltungs-VID 109
- Verwerfen ohne Rückmeldung 158
- Verworfen 424 , 433
- VLAN aktivieren 109
- Vollständige IPSec-Konfiguration löschen
 - 279
- VSS-Beschreibung 431
- Wahlpause 320
- Weitergeleitet 424
- Weitergeleitete Anfragen 342
- Wert 428
- WINS-Server 334
- Wird ausgeführt 143
- WLAN Controller: VSS-Durchsatz 138

- Zeit 421
- Zeit bis zum Abschalten 38
- Zeit einstellen 41
- Zeitaktualisierungsintervall 41 , 44
- Zeitaktualisierungsrichtlinie 41
- Zeitzone 41
- Zero Cookies verwenden 280
- Zertifikate und Schlüssel einschließen 407
- Zertifikatsanforderung 66
- Zertifikatsanforderungs-Payloads senden 281
- Zertifikatsanforderungs-Payloads nicht beachten 281
- Zertifikatsketten senden 281
- Ziel-IP-Adresse 153
- Zu verwendende Schnittstelle 404
- Zuerst gesehen 142 , 432
- Zuletzt gesehen 142 , 431 , 431 , 432
- Zweiter Zeitserver 41
- Adressliste 293
- Aktionen 372
- Aktive Clients 139
- Aktive IPSec-Tunnel 34
- Aktive Sitzungen (SIF, RTP, etc...) 34
- Aktuelle Anrufe 424
- Allgemein 117 , 394
- Anrufrkontrolle 324
- Anrufliste 425
- Arbeitsspeichernutzung 34
- Auslöser 366
- Benachbarte APs 140
- Benachrichtigungseinstellungen 418
- Benachrichtigungsempfänger 416
- Benutzer 62 , 363
- Benutzer ausloggen 403
- Bridge-Links 431
- Cache 341
- CLID-Umwandlung 327
- Client-Verwaltung 140 , 430
- CPU-Nutzung 34
- CRLs 72
- Datum und Uhrzeit 40
- DHCP-Konfiguration 348
- DHCP-Relay-Einstellungen 353
- Dienstliste 296
- Dienstkategorien 237
- DNS-Server 336
- DNS-Test 404
- Domänenweiterleitung 339
- Drahtlosnetzwerke (VSS) 130 , 140
- Dynamische Hosts 341
- DynDNS-Aktualisierung 344
- DynDNS-Provider 345
- Firmware-Wartung 143
- Funkmodulprofile 124
- Globale DHCPv6-Optionen 360
- Globale Einstellungen 334
- Gruppen 295 , 298
- Hosts 388
- HTTP 52
- HTTPS 52
- HTTPS-Server 342
- Interner Speicher 34
- IP Pools 230 , 278
- IP-Pool-Konfiguration 347
- IP/MAC-Bindung 352
- IPSec-Peers 246
- IPSec-Statistiken 423
- IPSec-Tunnel 421
- IPv4-Filterregeln 285
- IPv4-Gruppen 292
- IPv4-Routing-Tabelle 153
- IPv4/IPv6-Filter 179
- IPv6-Routenkonfiguration 151
- IPv6-Routingtabelle 154
- ISDN Verwendung Intern 34
- ISDN-Login 52
- ISDN-Trunks 318
- Konfiguration eines Allgemeinen Präfixes 156
- Konfiguration von IPv4-Routen 145
- Konfiguration von zustandsbehafteten Clients 362
- Lastverteilungsgruppen 168
- NAT-Konfiguration 159
- NAT-Schnittstellen 158

- OAM-Regelung 239
- Optionen 59 , 154 , 206 , 279 , 290 ,
319 , 364 , 384 , 405 , 415
- Passwörter 38
- Phase-1-Profilen 264
- Phase-2-Profilen 271
- Ping 52
- Ping-Generator 392
- Ping-Test 404
- Portkonfiguration 109
- PPPoA 221
- PPPoE 210
- PPTP 217
- Profile 232
- QoS-Klassifizierung 182
- QoS-Schnittstellen/Richtlinien 185
- RADIUS 53
- Regelketten 198
- Regulierte Schnittstellen 243
- Rogue APs 141
- Rogue Clients 142
- Rufnummertransformation 329
- Schnittstellen 48 , 94 , 390 , 393 , 415
- Schnittstellenzuweisung 199 , 401
- SIP-Konten 308
- Slave Access Points 121 , 138
- SNMP 52
- Special Session Handling 172
- SSH 52
- Standorte 315
- Statische Hosts 338
- Statistik 341 , 425
- Syslog-Server 412
- System 36
- Systemlizenzen 44
- Systemmeldungen 421
- Systemneustart 411
- Teilnehmer 303
- Telnet 52
- Traceroute-Test 405
- UMTS/LTE 227
- Verwaltung 109
- VLANs 108
- VSS 429
- Wake-on-LAN-Filter 395
- WLAN Controller 138
- WOL-Regeln 399
- XAUTH-Profilen 276
- Zertifikatsliste 64
- Zertifikatsserver 73
- Zugriffsfiler 194
- Zugriffsprofile 60
- Zustandsbehaftete Clients 358
- Zustandsbehaftete Clients 362
- Adressen 293
- Allgemein 203
- Allgemeine IPv6-Präfixe 156
- ATM 231
- Benachrichtigungsdienst 416
- Benutzer ausloggen 403
- Bridges 432
- CAPI-Server 363
- Controller-Konfiguration 117
- DHCP-Server 346
- DHCPv6-Server 357
- Diagnose 404
- Dienste 295
- DNS 332
- DynDNS-Client 343
- Factory Reset 411
- Globale Einstellungen 36
- HTTPS 342
- IGMP 203
- Internes Protokoll 421
- IP-Accounting 414
- IP-Konfiguration 94
- IPSec 245 , 421
- ISDN/Modem 424
- Konfigurationszugriff 59
- Lastverteilung 168
- Media Gateway 323
- Monitoring 138
- NAT 157
- Neustart 410
- QoS 178 , 433
- Real Time Jitter Control 243
- Richtlinien 285
- Routen 145

- Scheduling 365
 - Schnittstellen 292 , 425
 - Schnittstellenmodus / Bridge-Gruppen 46
 - SIA 420
 - Slave-AP-Konfiguration 121
 - Software & Konfiguration 405
 - Systemprotokoll 412
 - Überwachung 388
 - Umgebungs-Monitoring 140
 - UPnP 393
 - VLAN 107
 - Wake-On-LAN 395
 - Wartung 143
 - Weiterleiten 207
 - Wizard 111
 - Zertifikate 64
 - Zugriffsregeln 193
 - Firewall 283
 - LAN 94
 - Monitoring 421
 - VoIP 303
 - Wartung 403
 - Wireless LAN Controller 111
 - DHCP-Client (Konfigurationsbeispiel) 354
 - DHCP-Relay-Server (Konfigurationsbeispiel) 354
 - DHCP-Server (Konfigurationsbeispiel) 354
 - NAT (Konfigurationsbeispiel) 165
 - SIF (Konfigurationsbeispiel) 298
- #
- #1#2, #3 70
- A**
- ACCESS_ACCEPT 53
 - ACCESS_REJECT 53
 - ACCESS_REQUEST 53
 - ACCOUNTING_START 53
 - ACCOUNTING_STOP 53
 - Administrativer Zugriff 51
- Adresse des Service-Centers 92
 - ADSL-Leitungsprofil 84
 - Aktuelle Geschwindigkeit / Aktueller Modus 75
 - Aktuelles Netzwerk 85 , 92
 - Anschlussart 35
 - APN (Access Point Name) 85
 - Assistent für Netzwerkeinstellung 20
 - Assistenten 32
 - Ausgewähltes PLMN 92
 - Authentifizierungsmethode 92
 - Automatische Konfiguration beim Start 77
- B**
- Bedienelemente 24
 - Benutzername 92
 - Beschreibung 35
 - Beschreibung - Verbindungsinformation - Link 35
 - Betriebsmodus (Aktiv) 372
 - Betriebsmodus (Inaktiv) 372
 - Bevorzugter Netzwerktyp 85
 - Bohrschablone 11
 - BOSS-Version 34
- C**
- Cell ID 92
- D**
- Datenrate Mbit/s 431 , 431 , 432 , 432
 - Dienst 81
 - Dienstmerkmal 81
 - Domäne 340
 - Downstream 83
 - DSCP-Einstellungen für SIP-Daten 322
 - DSL-Chipsatz 82
 - DSL-Konfiguration 82
 - DSL-Modem 82
 - DSL-Modus 83
 - DSP-Modul 35

E

Eingehender Diensttyp 85
 Ethernet-Ports 74
 Ethernet-Schnittstellenauswahl 75
 Externe Berichterstellung 412

F

Fallback-Nummer 85
 Fallback-Proxy-Schnittstelle 1 205
 Fallback-Proxy-Schnittstelle 2 205
 Feste IP-Adresse 92
 Flusskontrolle 75
 Funkmodul1 139
 Funkzellen Code 92

G

Gerät 92
 Grundeinstellungen bei Auslieferung
 8
 Grundkonfiguration 16

H

Herstellernamen anzeigen 36 , 36
 Home PLMN 92
 Host 340

I

ICC ID 92
 IGMP Proxy 205
 IGMP Snooping 131
 IMEI 92
 Interner ISDN-Anschluss 10
 Internet + Einwählen 209
 IP-Adresse 17
 IP-Adresse des NetManagers 36
 ISDN Anrufsignalisierung 323
 ISDN-Konfiguration 77
 ISDN-Konfigurationstyp 77
 ISDN-Port 81
 ISDN-Ports 77

K

Kommunikation mit dem NetManager
 36
 Konfiguration 23
 Konfigurationsbeispiel - DHCP-Client
 354
 Konfigurationsbeispiel - DHCP-Re-
 lay-Server 354
 Konfigurationsbeispiel - DHCP-Server
 354
 Konfigurationsbeispiel -
 Lastverteilung 176
 Konfigurationsbeispiel - NAT 165
 Konfigurationsbeispiel - Scheduling
 384
 Konfigurationsbeispiel - SIF 298
 Konfigurationsbeispiel - Zeitgesteuerte
 Aufgaben 384
 Konfigurationsdaten sammeln 17
 Konfigurationsoberfläche aufrufen 24
 Konfigurierte Geschwindigkeit / Konfigu-
 rierter Modus 75

L

Lastverteilung (Konfigurationsbeispiel
) 176
 Letzer Befehl 92
 Letzte Antwort 92
 Letzte gespeicherte Konfiguration 34
 Lokale Dienste 332

M

Max. Übertragungsrates 128
 Maximale Upstream-Bandbreite 83
 Mobilfunk-Anbieter 85
 Mobilnetzbetreiber 90
 Modem-Status 85
 Modemmodell 92
 MSN 81
 MSN-Erkennung 81
 MSN-Konfiguration 79
 Multicast 201

N

Name 93
 Netzmaske 17
 Netzwerk 145
 Netzwerk-Status 427
 Netzwerkeinstellung 20
 Netzwerkqualität 85 , 92
 Nr. 35

O

Öffentliche IPv6-Quelladresse 257
 Oper Status 92

P

Passwort 92
 PC einrichten 18
 Physikalische Verbindung 82
 Physikalische Schnittstellen 74
 Pin-Belegungen 12
 PLMN 93
 Port-STUN-Server 290
 Port-Verwendung 77
 Portkonfiguration 75
 Portname 77
 Primärer DNS-Server (IPv4/IPv6) 340
 Protokollierte Aktionen 290
 Proxy-Schnittstelle 205
 PUK 85

R

Registrar 35
 Remote Authentifizierung 53
 Reset 8
 Reset-Taster 11
 Roaming-Modus 90
 Rufnummer 92

S

Scheduling (Konfigurationsbeispiel)
 384

Schnittstelle 340
 Schnittstelle - Verbindungsinformation -
 Link 35
 Sekundärer DNS-Server (IPv4/IPv6)
 340
 Seriennummer 34
 Signal dBm (RSSI1, RSSI2, RSSI3)
 430 , 431 , 432
 SIM-Karte verwendet PIN 85
 SIP Port 322
 Softwareaktualisierung 21
 Status 33 , 35 , 93
 Status der IPv4-Firewall 290
 STUN Handler 290
 Support 9
 Switch-Port 75
 System-Voraussetzungen 16
 Systemdatum 34
 Systemsoftware 16
 Systemverwaltung 33

T

Terminierung 10
 Trace-Schnittstelle 401
 Transmit Shaping 83

U

UMTS/LTE 84
 UMTS/LTE-Status 85
 Upstream 83
 Uptime 34

V

Vollständige IPv4-Filterung 290
 Vorbereitungen 16
 VPN 245

W

WAN 209
 Wandmontage 11
 Weiterleiten 340
 Weiterleiten an 340

WEP-Schlüssel 1-4 132

WLAN 427

WLANx 427

X

X.31 TEI-Dienst 78

X.31 TEI-Wert 78

X.31 (X.25 im D-Kanal) 78

Z

Zeitgesteuerte Aufgaben
(Konfigurationsbeispiel) 384

Zugang über LAN 23

Zugangstyp 93