



# **Benutzerhandbuch be.IP 4isdn**

## **Betrieb als Fax Server**

Copyright© Version 10.2.10 RC (SVN 11184) 09/2021 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](http://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](http://www.bintec-elmeg.com). Wartemelodien des Systems: elmeg Song, Hold the line.

# Inhaltsverzeichnis

1	Einleitung . . . . .	1
2	Inbetriebnahme . . . . .	2
2.1	be.IP 4isdn . . . . .	2
2.1.1	Aufstellen und Anschließen . . . . .	2
2.1.2	Anschlüsse . . . . .	4
2.1.3	Anschlüsse (seitlich) . . . . .	4
2.1.4	Montagewinkel . . . . .	4
2.1.5	LEDs . . . . .	5
2.1.6	Lieferumfang . . . . .	7
2.1.7	Allgemeine Produktmerkmale . . . . .	7
2.2	Reset . . . . .	8
2.3	Support-Information . . . . .	9
3	Montage . . . . .	10
3.1	Anschluss von Geräten . . . . .	10
3.1.1	Interner ISDN-Anschluss . . . . .	10
3.2	Reset Taster . . . . .	10
3.3	Wandmontage . . . . .	10
3.4	Pin-Belegungen . . . . .	11
3.4.1	Ethernet-Schnittstellen . . . . .	11
3.4.2	ISDN-Schnittstelle . . . . .	12
3.4.3	VDSL-Schnittstelle . . . . .	13
3.4.4	Serielle Schnittstelle . . . . .	13
4	Grundkonfiguration . . . . .	15
4.1	Vorbereitungen . . . . .	15

4.1.1	Systemsoftware . . . . .	15
4.1.2	System-Voraussetzungen . . . . .	15
4.1.3	Daten sammeln . . . . .	16
4.1.4	PC einrichten . . . . .	17
4.2	Konfiguration des Systems. . . . .	18
4.2.1	Netzwerkeinstellung (LAN). . . . .	19
4.2.2	SIP-Provider eintragen . . . . .	19
4.3	Internetverbindung einrichten. . . . .	19
4.3.1	Internetverbindung über das interne VDSL-Modem . . . . .	19
4.3.2	Andere Internetverbindungen. . . . .	19
4.3.3	Konfiguration prüfen . . . . .	20
4.4	Benutzerzugang . . . . .	20
4.5	Softwareaktualisierung be.IP 4isdn . . . . .	21
5	<b>Zugang und Konfiguration . . . . .</b>	<b>23</b>
5.1	Zugang über LAN . . . . .	23
5.1.1	HTTP/HTTPS . . . . .	23
5.2	Konfiguration. . . . .	23
5.2.1	Konfigurationsoberfläche . . . . .	23
6	<b>Assistenten . . . . .</b>	<b>34</b>
7	<b>Systemverwaltung . . . . .</b>	<b>35</b>
7.1	Status. . . . .	35
7.2	Globale Einstellungen . . . . .	38
7.2.1	System . . . . .	38
7.2.2	Passwörter . . . . .	45
7.2.3	Datum und Uhrzeit . . . . .	47
7.2.4	Timer . . . . .	51

7.2.5	Systemlizenzen . . . . .	54
7.3	Kennziffern . . . . .	56
7.3.1	Änderbare Kennziffern . . . . .	56
7.4	Schnittstellenmodus / Bridge-Gruppen . . . . .	58
7.4.1	Schnittstellen . . . . .	60
7.5	Administrativer Zugriff . . . . .	63
7.5.1	Zugriff . . . . .	63
7.5.2	SSH . . . . .	64
7.5.3	SNMP . . . . .	68
7.6	Remote Authentifizierung . . . . .	69
7.6.1	RADIUS . . . . .	69
7.6.2	Optionen . . . . .	75
7.7	Zertifikate . . . . .	75
7.7.1	Zertifikatsliste . . . . .	76
7.7.2	CRLs . . . . .	83
7.7.3	Zertifikatsserver . . . . .	84
<b>8</b>	<b>Physikalische Schnittstellen . . . . .</b>	<b>86</b>
8.1	Ethernet-Ports . . . . .	86
8.1.1	Portkonfiguration . . . . .	87
8.2	ISDN-Ports (PBX) . . . . .	89
8.2.1	ISDN Intern . . . . .	89
8.2.2	ISDN-Konfiguration . . . . .	91
8.3	DSL-Modem . . . . .	91
8.3.1	DSL-Konfiguration . . . . .	91
<b>9</b>	<b>VoIP (PBX) . . . . .</b>	<b>94</b>
9.1	Einstellungen . . . . .	94
9.1.1	SIP-Provider . . . . .	94

9.1.2	Standorte . . . . .	106
9.1.3	Codec-Profile . . . . .	109
9.1.4	Optionen . . . . .	112
<b>10</b>	<b>Anrufkontrolle . . . . .</b>	<b>115</b>
10.1	Ausgehende Dienste . . . . .	115
10.1.1	Anrufweitschaltung (AWS) . . . . .	115
10.1.2	Wahlkontrolle . . . . .	117
<b>11</b>	<b>Anwendungen. . . . .</b>	<b>119</b>
11.1	Verbindungsdaten . . . . .	119
11.1.1	Gehend . . . . .	119
11.1.2	Kommend . . . . .	120
11.1.3	Allgemein . . . . .	121
11.2	Anrufliste . . . . .	122
11.2.1	Kommend . . . . .	122
11.2.2	Gehend . . . . .	123
11.2.3	Allgemein . . . . .	124
<b>12</b>	<b>LAN . . . . .</b>	<b>126</b>
12.1	IP-Konfiguration . . . . .	126
12.1.1	Schnittstellen . . . . .	126
12.2	VLAN . . . . .	140
12.2.1	VLANs . . . . .	140
12.2.2	Portkonfiguration . . . . .	141
12.2.3	Verwaltung . . . . .	142
<b>13</b>	<b>Wireless LAN Controller . . . . .</b>	<b>143</b>
13.1	Wizard . . . . .	144
13.1.1	Wireless LAN Controller Wizard . . . . .	145

13.1.2	Wireless LAN Controller VLAN Konfiguration . . . . .	151
13.2	Controller-Konfiguration . . . . .	152
13.2.1	Allgemein . . . . .	152
13.2.2	Autoprofil für Access Points . . . . .	155
13.3	Access-Point-Konfiguration . . . . .	156
13.3.1	Access Points . . . . .	156
13.3.2	Funkmodulprofile . . . . .	160
13.3.3	Drahtlosnetzwerke (VSS) . . . . .	166
13.4	Monitoring . . . . .	176
13.4.1	WLAN Controller . . . . .	176
13.4.2	Access Points . . . . .	177
13.4.3	Aktive Clients . . . . .	177
13.4.4	Drahtlosnetzwerke (VSS) . . . . .	178
13.4.5	Client-Verwaltung . . . . .	178
13.5	Umgebungs-Monitoring . . . . .	179
13.5.1	Eigene Access Points . . . . .	179
13.5.2	Benachbarte APs . . . . .	179
13.5.3	Rogue APs . . . . .	180
13.5.4	Rogue Clients . . . . .	180
13.6	Wartung . . . . .	181
13.6.1	Firmware-Wartung . . . . .	181
<b>14</b>	<b>Netzwerk . . . . .</b>	<b>184</b>
14.1	Routen . . . . .	184
14.1.1	Konfiguration von IPv4-Routen . . . . .	184
14.1.2	Konfiguration von IPv6-Routen . . . . .	190
14.1.3	IPv4-Routing-Tabelle . . . . .	192
14.1.4	IPv6-Routing-Tabelle . . . . .	193
14.1.5	Optionen . . . . .	193
14.2	Allgemeine IPv6-Präfixe . . . . .	194

14.2.1	Konfiguration eines Allgemeinen Präfixes . . . . .	195
14.3	NAT . . . . .	196
14.3.1	NAT-Schnittstellen . . . . .	196
14.3.2	NAT-Konfiguration . . . . .	198
14.3.3	NAT - Konfigurationsbeispiel . . . . .	204
14.4	Lastverteilung . . . . .	207
14.4.1	Lastverteilungsgruppen . . . . .	207
14.4.2	Special Session Handling . . . . .	211
14.4.3	Lastverteilung - Konfigurationsbeispiel. . . . .	214
14.5	QoS . . . . .	217
14.5.1	IPv4/IPv6-Filter . . . . .	217
14.5.2	QoS-Klassifizierung . . . . .	221
14.5.3	QoS-Schnittstellen/Richtlinien . . . . .	224
14.6	Zugriffsregeln . . . . .	231
14.6.1	Zugriffsfiler . . . . .	233
14.6.2	Regelketten . . . . .	237
14.6.3	Schnittstellenzuweisung . . . . .	238
<b>15</b>	<b>Multicast. . . . .</b>	<b>240</b>
15.1	Allgemein . . . . .	242
15.1.1	Allgemein . . . . .	242
15.2	IGMP . . . . .	242
15.2.1	IGMP . . . . .	242
15.2.2	Optionen . . . . .	245
15.3	Weiterleiten . . . . .	246
15.3.1	Weiterleiten . . . . .	246
<b>16</b>	<b>WAN. . . . .</b>	<b>248</b>
16.1	Internet + Einwählen . . . . .	248



16.1.1	PPPoE . . . . .	249
16.1.2	Dual Stack Lite (DS-Lite) . . . . .	258
16.1.3	PPTP . . . . .	259
16.1.4	PPPoA . . . . .	264
16.1.5	IP Pools . . . . .	272
16.2	ATM . . . . .	273
16.2.1	Profile . . . . .	274
16.2.2	Dienstkategorien . . . . .	278
16.2.3	OAM-Regelung . . . . .	280
16.3	Real Time Jitter Control . . . . .	284
16.3.1	Regulierte Schnittstellen . . . . .	285
<b>17</b>	<b>VPN . . . . .</b>	<b>286</b>
17.1	IPSec . . . . .	286
17.1.1	IPSec-Peers . . . . .	287
17.1.2	Phase-1-Profile . . . . .	305
17.1.3	Phase-2-Profile . . . . .	313
17.1.4	XAUTH-Profile . . . . .	318
17.1.5	IP Pools . . . . .	320
17.1.6	Optionen . . . . .	321
17.2	be.IP Secure Client . . . . .	324
17.3	LISP Light . . . . .	325
17.3.1	(ITR / ETR) Router . . . . .	327
17.3.2	Lokale / Entfernte Standorte . . . . .	330
17.3.3	EID Präfix Segregation (LISP Instanzen) . . . . .	331
17.4	L2TP . . . . .	333
17.4.1	Tunnelprofile . . . . .	334
17.4.2	Benutzer . . . . .	337
17.4.3	Optionen . . . . .	342

<b>18</b>	<b>Firewall . . . . .</b>	<b>343</b>
18.1	Richtlinien . . . . .	345
18.1.1	IPv4-Filterregeln . . . . .	345
18.1.2	IPv6-Filterregeln . . . . .	347
18.1.3	Optionen . . . . .	350
18.2	Schnittstellen . . . . .	352
18.2.1	IPv4-Gruppen . . . . .	352
18.2.2	IPv6-Gruppen . . . . .	353
18.3	Adressen . . . . .	353
18.3.1	Adressliste . . . . .	353
18.3.2	Gruppen . . . . .	355
18.4	Dienste . . . . .	355
18.4.1	Diensteliste . . . . .	356
18.4.2	Gruppen . . . . .	358
18.5	Konfiguration . . . . .	358
18.5.1	SIF - Konfigurationsbeispiel . . . . .	358
<b>19</b>	<b>Lokale Dienste . . . . .</b>	<b>363</b>
19.1	DNS . . . . .	363
19.1.1	Globale Einstellungen . . . . .	365
19.1.2	DNS-Server . . . . .	367
19.1.3	Statische Hosts . . . . .	369
19.1.4	Domänenweiterleitung . . . . .	371
19.1.5	Dynamische Hosts . . . . .	373
19.1.6	Cache . . . . .	373
19.1.7	Statistik . . . . .	373
19.2	HTTPS . . . . .	374
19.2.1	HTTPS-Server . . . . .	374

19.3	DynDNS-Client . . . . .	375
19.3.1	DynDNS-Aktualisierung . . . . .	375
19.3.2	DynDNS-Provider . . . . .	377
19.4	DHCP-Server . . . . .	379
19.4.1	IP-Pool-Konfiguration . . . . .	380
19.4.2	DHCP-Konfiguration . . . . .	380
19.4.3	IP/MAC-Bindung . . . . .	385
19.4.4	DHCP-Relay-Einstellungen . . . . .	386
19.4.5	DHCP - Konfigurationsbeispiel . . . . .	387
19.5	DHCPv6-Server . . . . .	389
19.5.1	DHCPv6-Server . . . . .	391
19.5.2	Globale DHCPv6-Optionen . . . . .	393
19.5.3	Zustandsbehaftete Clients . . . . .	394
19.5.4	Konfiguration von zustandsbehafteten Clients . . . . .	394
19.6	CAPI-Server . . . . .	395
19.6.1	Benutzer . . . . .	396
19.6.2	Optionen . . . . .	396
19.7	Scheduling . . . . .	397
19.7.1	Auslöser . . . . .	398
19.7.2	Aktionen . . . . .	405
19.7.3	Optionen . . . . .	416
19.7.4	Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling) . . . . .	417
19.8	Überwachung . . . . .	420
19.8.1	Hosts . . . . .	420
19.8.2	Schnittstellen . . . . .	423
19.8.3	Ping-Generator . . . . .	424
19.9	UPnP . . . . .	425
19.9.1	Schnittstellen . . . . .	426
19.9.2	Allgemein . . . . .	426
19.10	Hotspot-Gateway . . . . .	427

19.10.1	Hotspot-Gateway . . . . .	429
19.10.2	Optionen . . . . .	433
19.11	Wake-On-LAN . . . . .	433
19.11.1	Wake-on-LAN-Filter . . . . .	433
19.11.2	WOL-Regeln . . . . .	437
19.11.3	Schnittstellenzuweisung . . . . .	439
19.12	Trace . . . . .	439
19.12.1	Trace-Schnittstelle . . . . .	439
19.12.2	VoIP/SIP-Trace . . . . .	440
<b>20</b>	<b>Wartung . . . . .</b>	<b>441</b>
20.1	Benutzer ausloggen . . . . .	441
20.1.1	Benutzer ausloggen . . . . .	441
20.2	Diagnose . . . . .	442
20.2.1	Ping-Test . . . . .	442
20.2.2	DNS-Test . . . . .	442
20.2.3	Traceroute-Test . . . . .	443
20.3	Software &Konfiguration . . . . .	443
20.3.1	Optionen . . . . .	443
20.4	Neustart . . . . .	449
20.4.1	Systemneustart . . . . .	449
20.5	Factory Reset . . . . .	449
<b>21</b>	<b>Externe Berichterstellung. . . . .</b>	<b>450</b>
21.1	Systemprotokoll . . . . .	450
21.1.1	Syslog-Server . . . . .	450
21.2	IP-Accounting . . . . .	452
21.2.1	Schnittstellen . . . . .	453
21.2.2	Optionen . . . . .	453

21.3	Benachrichtigungsdienst . . . . .	454
21.3.1	Benachrichtigungsempfänger . . . . .	454
21.3.2	Benachrichtigungseinstellungen . . . . .	456
21.4	SNMP . . . . .	458
21.4.1	SNMP-Trap-Optionen . . . . .	459
21.4.2	SNMP-Trap-Hosts . . . . .	460
21.5	SIA . . . . .	460
21.5.1	SIA . . . . .	460
<b>22</b>	<b>Monitoring . . . . .</b>	<b>461</b>
22.1	Internes Protokoll . . . . .	461
22.1.1	Systemmeldungen . . . . .	461
22.2	IPSec . . . . .	461
22.2.1	IPSec-Tunnel . . . . .	461
22.2.2	IPSec-Statistiken . . . . .	463
22.3	Schnittstellen . . . . .	464
22.3.1	Statistik . . . . .	464
22.3.2	Netzwerk-Status . . . . .	466
22.4	Bridges . . . . .	466
22.4.1	br<x> . . . . .	466
22.5	Hotspot-Gateway . . . . .	466
22.5.1	Hotspot-Gateway . . . . .	466
22.6	QoS . . . . .	467
22.6.1	QoS . . . . .	467
<b>23</b>	<b>Benutzerzugang . . . . .</b>	<b>468</b>
23.1	Status . . . . .	468
23.2	Telefonbuch . . . . .	470

23.2.1	System-Telefonbuch . . . . .	470
23.2.2	Benutzertelefonbuch . . . . .	471
23.3	Verbindungsdaten . . . . .	471
23.3.1	Gehend . . . . .	471
23.3.2	Kommend . . . . .	472
23.4	Anrufliste . . . . .	473
23.4.1	Kommend . . . . .	473
23.4.2	Gehend . . . . .	473
23.5	Einstellungen . . . . .	474
23.5.1	Einstellungen von Features . . . . .	474
23.5.2	Allgemeine Einstellungen . . . . .	478
	Glossar . . . . .	481
	Index . . . . .	522

# 1 Einleitung



## Wichtig

Lesen Sie die Erläuterungen zum Einsatz Ihrer **be.IP 4isdn** sorgfältig durch. Funktionen, die im Handbuch nicht enthalten sind, werden nicht unterstützt!

Das Media Gateway **be.IP 4isdn** mit integriertem Business-Router bietet einen einfachen Einstieg in die IP-Technologie.

Das Gerät ist vor allem für die Migration bestehender ISDN-Telefonanlagen nach ALL-IP konzipiert. Migration bedeutet in diesem Zusammenhang, dass Sie Ihre ISDN-Telefonanlage zusammen mit allen angeschlossenen Endgeräten, wie zum Beispiel Telefonen und FAX-Gerät, mit der bestehenden Konfiguration unverändert weiterverwenden können. Da das Gateway über 4 ISDN-Anschlüsse verfügt, ist es für Standorte mit mehreren ISDN-Mehrgeräte- und Anlagenanschlüssen geeignet. Sollten diese vier Anschlüsse nicht ausreichen, können Sie zwei **be.IP 4isdn** koppeln. Mit dieser Einheit lassen sich ISDN-Telefonanlagen mit bis zu 8 ISDN-Anschlüssen und 16 gleichzeitig genutzten Sprachkanälen auf ALL-IP-Amtszugänge umstellen.

Wenn Sprachtranskodierung benötigt wird, ist das Media Gateway **be.IP 4isdn** ebenfalls erste Wahl. Auch ohne Verwendung von ISDN ist die Zahl der gleichzeitig verfügbaren Verbindungen durch den Einsatz zusätzlicher komprimierender DSPs deutlich höher als bei den anderen Geräten der be.IP-Serie.

Selbstverständlich unterstützt das Gerät die üblichen FAX-Szenarien am ISDN-Port mittels CAPI. Wenn in Ihrem Unternehmen ein Server-basiertes E-Mail-System zum Einsatz kommt, das über eine Third-Party-CAPI-Schnittstelle um FAX, Anrufbeantworter und Sprachnachrichten erweitert ist, so können Sie mit **be.IP 4isdn** im MGW-Modus die ISDN-Schnittstellen auch auf virtualisierten Serversystemen fernsteuern.

Third-Party-CAPI-Anwendungen direkt am ISDN-Amtsanschluss dagegen funktionieren in vielen Fällen unter ALL-IP nicht mehr. Bintec elmeg bietet hierfür auf der **be.IP 4isdn** im FAX-Modus die Möglichkeit, Ihre bestehenden Systeme ohne Änderung mittels CAPI direkt an SIP-Anschlüssen zu betreiben (ganz ohne ISDN). Mit der Lösung CAPI2SIP können Sie also auch Ihre CAPI-Anwendungen ins ALL-IP-Zeitalter mitnehmen.



## Hinweis

Der in der Konfigurationsoberfläche als "PBX"-Modus bezeichnete Betrieb entspricht bei **be.IP 4isdn** dem "Fax-Server"-Modus, da ein Betrieb als Telefonanlage nicht unterstützt wird.

## 2 Inbetriebnahme

### 2.1 be.IP 4isdn

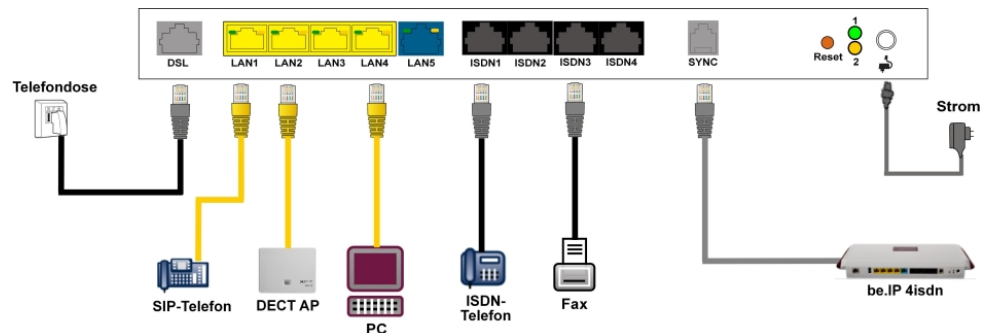
In diesem Kapitel erfahren Sie, wie Sie Ihr Gerät aufstellen, anschließen und in Betrieb nehmen.

Der Weg zu einer weiterführenden Konfiguration wird Ihnen anschließend Schritt für Schritt erläutert. 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.

#### 2.1.1 Aufstellen und Anschließen

Die **be.IP 4isdn** 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 Gerätes 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 4isdn** 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) **DSL**  
Verbinden Sie den Anschluss **DSL** über das graue Kabel an die TAE-Buchse der Telefendose an.
- (4) **ISDN-Endgeräte**  
Schließen Sie ein ISDN-Telefon an den internen ISDN-Anschluss der **be.IP 4isdn** an. Verwenden Sie dazu das dem Endgerät beigegefügte Kabel.
- (5) **SIP-Telefone**  
Schließen Sie Ihre SIP-Telefone an die 10/100/1000 Base-T Ethernet-Schnittstellen an. Einen letzten Schritt müssen Sie am PC ausführen.
- (6) **PC**  
Schließen Sie einen geeigneten PC über ein Ethernet-Kabel an eine der Ethernet-Schnittstellen der **be.IP 4isdn** an. Sollten Probleme bei der Verbindung zwischen PC und **be.IP 4isdn** auftreten, lesen Sie bitte die entsprechenden Kapitel zur Grundkonfiguration.
- (7) **SYNC**  
An den SYNC-Anschluss können Sie mit einem SYNC-Kabel eine zweite **be.IP 4isdn** anschließen. Damit stehen Ihnen weitere 4 ISDN-Anschlüsse zur Verfügung.

**Hinweis**

Die weiteren 4 ISDN-Anschlüsse sind nur im Modus Media Gateway verfügbar!

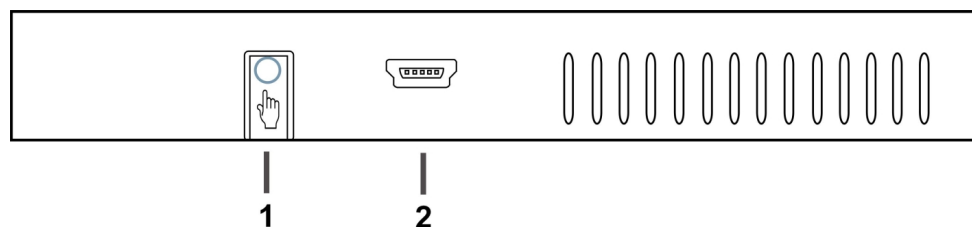
- (8) **VoIP**  
Für einen reinen IP-Anschluss ohne ISDN verwenden Sie die vom Provider bereitgestellte Anleitung.

## 2.1.2 Anschlüsse



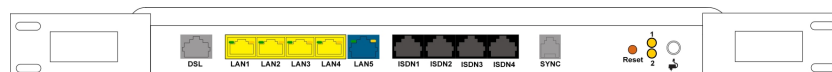
1	DSL-Schnittstelle Annex B/J
2	10/100/1000 Base-T Ethernet-Schnittstellen (LAN 1 - LAN4)
3	Ethernet-WAN-Schnittstelle (LAN5)
4	Schnittstelle für ISDN-Endgeräte (ISDN1 - ISDN4)
5	SYNC-Schnittstelle
6	Buchse für das Steckernetzteil

## 2.1.3 Anschlüsse (seitlich)



1	Funktionstaste
2	Console

## 2.1.4 Montagewinkel



Montieren Sie die Montagewinkel mit den im Set beiliegenden Schrauben am Gehäuse. Die Montagewinkel und die Schrauben sind als Zubehör erhältlich (Artikelnummer MN40285514).



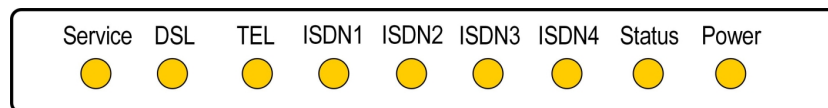
### Hinweis

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

## 2.1.5 LEDs

Anhand der LEDs können Sie den Status Ihres Geräts ablesen.

Die LEDs der **be.IP 4isdn** sind folgendermaßen angeordnet:



Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

### LED Statusanzeige

LED	Status	Information
Service	an	Automatische Wartung aktiv
	aus	Automatische Wartung inaktiv
DSL	an	Verbindung hergestellt
	langsam blinkend	Synchronisation läuft
	aus	Keine Synchronisation
	flackernd	Datentransfer
TEL	an	Telefonie am IP-Anschluss (Voice over IP) bereit
	aus	Telefonie nicht eingerichtet
ISDN1 bis ISDN 4	an	ISDN-Endgeräte angeschlossen
	aus	Ruhezustand oder außer Betrieb
Status	an	Nach dem Einschalten: Gerät wird gestartet
		während des Betriebs: Fehler
	langsam blinkend	Gerät ist aktiv
Power	an	Stromversorgung ist angeschlossen
	aus	Keine Stromversorgung

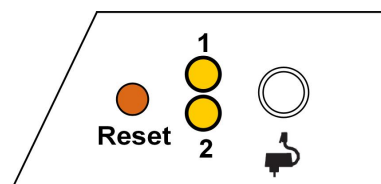
Die LEDs der Ethernet-Buchsen LAN 1-4 (LAN) und LAN 5 (WAN) zeigen folgende Statusinformationen an:

### 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 Gelb

## 2 Service Gelb

## 2.1.6 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Produktname	Kabelsätze/Sonstiges	Dokumentation
<b>be.IP 4isdn</b>	ein Ethernet LAN-Kabel (gelb)	Installationsposter
	ein Ethernet WAN-Kabel (blau)	Sicherheitshinweise
	ein VDSL-Kabel (grau)	
	ein Netzteil	
	19" Kit und Schrauben	

## 2.1.7 Allgemeine Produktmerkmale

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

### Allgemeine Produktmerkmale be.IP 4isdn

Eigenschaft	
<b>Maße und Gewicht:</b>	
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	20 (9 x Funktion, 1 x Service, 5x2 Ethernet)
Leistungsaufnahme Gerät	max. 30 W 12 V DC
Spannungsversorgung	12 V DC 2,5 A
<b>Umweltanforderungen:</b>	
Lagertemperatur	-25 °C bis +70 °C

<b>Eigenschaft</b>	
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	max. 85 %
Raumklassifizierung	Nur in trockenen Räumen betreiben
<b>Verfügbare Schnittstellen:</b>	
VDSL-Schnittstelle	Internes VDSL-Modem
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, auto-sensing, MDIX
DMZ-Schnittstelle (LAN5)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, auto-sensing, MDIX
ISDN-BRI-Schnittstellen (ISDN1 bis ISDN4)	4 interne ISDN-Schnittstellen, ISDN-Terminierung
SYNC-Schnittstelle	SYNC
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200 bis 115200 Baud
<b>Vorhandene Buchsen:</b>	
VDSL-Schnittstelle	1 x RJ45-Buchse (grau)
Ethernet-Schnittstellen LAN1 bis LAN4	4 x RJ45-Buchse mit integrierten LEDs
Ethernet-Schnittstelle LAN5 (WAN)	1 x RJ45-Buchse mit integrierten LEDs
BRI-Schnittstelle ISDN1 bis ISDN4	4 x RJ45-Buchse (schwarz)
SYNC-Schnittstelle	1 x RJ11-Buchse
Serielle Schnittstelle V.24	5-polige Mini-USB-Buchse
Hohlsteckerbuchse für Stromversorgung	

## 2.2 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.

## 2.3 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](http://www.bintec-elmeg.com).

## 3 Montage



### Warnung

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



### Achtung

Um einen störungsfreien Betrieb zu gewährleisten, sollte die **be.IP 4isdn** 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 10).

## 3.1 Anschluss von Geräten

### 3.1.1 Interner ISDN-Anschluss

Der interne ISDN-Anschluss der **be.IP 4isdn** 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.

### 3.2 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).

## 3.3 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 ~ Netzsteck-



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

- (2) Um eine gegenseitige Beeinträchtigung auszuschließen, montieren Sie das Gerät nicht in unmittelbarer Nähe von elektronischen Geräten wie z. B. HiFi-Geräten, Bürogeräten oder Mikrowellengeräten. Vermeiden Sie auch einen Aufstellort in der Nähe von Wärmequellen, z. B. Heizkörpern oder in feuchten Räumen.
- (3) Halten Sie die Abstände ein, die auf der Rückseite des Geräts eingeprägt sind.
- (4) Markieren Sie die Bohrlöcher an der Wand.
- (5) Überprüfen Sie die feste Auflage aller Befestigungspunkte der **be.IP 4isdn** 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 4isdn** 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 4isdn** mit dem externen xDSL-Anschluss. Sie können dazu so verfahren, 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.

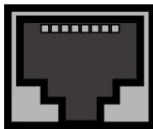
## 3.4 Pin-Belegungen

### 3.4.1 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 (LAN5) oder eines Servers.

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

1 ..... 8



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

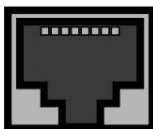
#### RJ45-Buchse für Ethernet-Anschluss

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 -

### 3.4.2 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

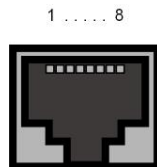
Pin	Funktion (NT)
1	Nicht genutzt
2	Nicht genutzt
3	Empfangen (+) 2a
4	Senden (+) 1a
5	Senden (-) 1b

Pin	Funktion (NT)
6	Empfangen (-) 2b
7	Nicht genutzt
8	Nicht genutzt

### 3.4.3 VDSL-Schnittstelle

Die **be.IP 4isdn** verfügt über eine VDSL-Schnittstelle. Die VDSL-Schnittstelle wird mittels eines RJ45-Steckers verbunden.

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



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

#### RJ45-Buchse für VDSL-Anschluss

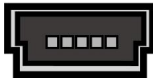
Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Nicht genutzt
4	Leitung 1a
5	Leitung 1b
6	Nicht genutzt
7	Nicht genutzt
8	Nicht genutzt

### 3.4.4 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

## 4 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.

### 4.1 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 17 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 4isdn** an, so dass zur Konfiguration ein eigenes Netz entsteht.

#### 4.1.1 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 4isdn](#) auf Seite 21.

#### 4.1.2 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

### 4.1.3 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>	

### 4.1.4 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.

## 4.2 Konfiguration des Systems



## 4.2.1 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.

## 4.2.2 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**.

## 4.3 Internetverbindung einrichten

Sie können mit Ihrem Gerät eine Internetverbindung aufbauen.

### 4.3.1 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.

### 4.3.2 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 **Internetzugang** in der Konfigurationsoberfläche.

### 4.3.3 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.

## 4.4 Benutzerzugang

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



#### Hinweis

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

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

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

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

## 4.5 Softwareaktualisierung be.IP 4isdn

Die Funktionsvielfalt der **be.IP 4isdn** wird permanent erweitert. Eine Softwareaktualisierung kann über das **GUI** vorgenommen werden.

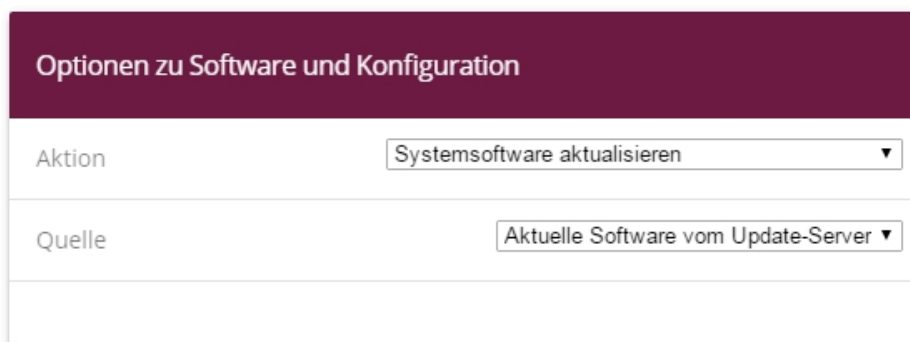
Voraussetzung für ein automatisches Update ist eine bestehende Internetverbindung.

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.

## 5 Zugang und Konfiguration

### 5.1 Zugang über LAN

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

#### 5.1.1 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`

### 5.2 Konfiguration

Die Konfiguration wird mit der HTML-Konfigurationsoberfläche durchgeführt.

#### 5.2.1 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.

Systeminformationen		Ressourceninformationen	
Uptime	1 Tag(e) 5 Stunde(n) 14 Minute(n)	CPU-Nutzung	0%
Systemdatum	Samstag, 11 Nov 2000, 02:47:44	Arbeitsspeichernutzung	45.9/127.9 MByte (35%)
Seriennummer	BE2CCA015030025	Interner Speicher	0.044/3.963 GByte (1%) 
BOSS-Version	V.10.1 Rev. 7 (Beta 19) IPv6, IPSec, PBX from 2016/03/15 00:00:00	Aktive Sitzungen (SIF, RTP, etc...)	3
Letzte gespeicherte Konfiguration	Freitag, 03 Nov 2000, 20:48:25	Aktive IPSec-Tunnel	0 / 1
Status Nachtbetrieb	Aus		

## Konfigurationsoberfläche Startseite

### 5.2.1.1 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.

### 5.2.1.2 Bedienelemente

#### Fenster der Konfigurationsoberfläche

Das Fenster der Konfigurationsoberfläche ist in drei Bereiche geteilt:

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

**Navigationsleiste** **Kopfleiste**

The screenshot shows the main configuration interface for be.IP 4isdn. On the left is a dark red navigation menu with various system management options. At the top is a header bar with the product name, logo, and user options. The main content area is divided into two columns: 'Systeminformationen' and 'Ressourceninformationen'.

**Systeminformationen**

Uptime	0 Tag(e) 0 Stunde(n) 0 Minute(n)
Systemdatum	Donnerstag, 01 Jan 2009, 01:00:41
Seriennummer	RNOCAAM16500007
BOSS-Version	V.10.1.21.10 IPSec, PBX from 2016/12/19 00:00:00
Letzte gespeicherte Konfiguration	Keine Boot-Konfiguration gespeichert
Status Nachtbetrieb	Aus

**Ressourceninformationen**

CPU-Nutzung	26%
Arbeitsspeichernutzung	41.9/127.9 MByte (32%)
Aktive Sitzungen (SIP, RTP, etc...)	3
Aktive IPSec-Tunnel	0 / 0
DSP-Kanäle	SoftCoder 0 / 4
	LANTIQ 0 / 5
	M 8 DSP V2 0 / 8

**Hauptkonfigurationsfenster**

## Kopfleiste

The header bar contains the following elements from left to right: a hamburger menu icon, the text 'be.IP 4isdn' and 'be\_ip\_4isdn', the bintec elmeg logo, the text 'bintec elmeg' and 'RTP Group Company', the text 'SPRACHE ANSICHT Standard', and a button labeled 'KONFIGURATION SPEICHERN' with a save icon. On the far right, there is an 'Ausloggen' button and a help icon.

## Konfigurationsoberfläche Kopfleiste

Menü	Funktion
	Öffnet die Navigationsleiste, über die Sie Zugriff auf die Menüs zur Konfiguration haben.
	<p><b>Ausloggen:</b> 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"> <li>• 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 erfolgt die Abmeldung vom Gerät.</li> <li>• Konfiguration speichern, dann verlassen: Ihre Änderungen werden gespeichert. Dabei wird die zuvor aktive Konfiguration ersetzt. Erst dann erfolgt die Abmeldung vom Gerät.</li> <li>• Ohne zu speichern verlassen: Ihre Änderungen sind zwar ak-</li> </ul>

Menü	Funktion
	<p>tiv, werden aber nicht gespeichert. Nach einem Neustart sind wieder die zuvor gültigen Einstellungen aktiv.</p>
	<p><b>Online-Hilfe:</b> 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; font-weight: bold;">SPRACHE</div> <div style="padding: 5px; text-align: center;">English</div> <div style="padding: 5px; text-align: center; background-color: #f0f0f0;">Deutsch</div>	<p><b>Sprache:</b> 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; font-weight: bold;">ANSICHT</div> <div style="padding: 5px; text-align: center;">Schnellstart</div> <div style="padding: 5px; text-align: center;">Benutzer</div> <div style="padding: 5px; text-align: center;">Experte</div> <div style="padding: 5px; text-align: center; background-color: #f0f0f0;">Vollzugriff</div>	<p><b>Ansicht:</b> 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 <b>Experte</b> und <b>Vollzugriff</b> fügen jeweils zusätzliche Menüs hinzu, die jedoch weitergehende Kenntnisse voraussetzen.</p>
<div style="background-color: #800040; color: white; padding: 5px; text-align: center; font-weight: bold;">  KONFIGURATION SPEICHERN         </div>	<p>Die Schaltfläche <b>Konfiguration speichern</b>.</p> <p>Wenn Sie Änderungen an der Konfiguration vorgenommen haben, können Sie diese auf zwei Arten speichern:</p> <ul style="list-style-type: none"> <li>• Konfiguration speichern - Ihre Änderungen werden in die aktuelle Startkonfiguration (die Konfiguration, mit der Ihr Gerät nach jedem Start aktiv wird) übernommen und gespeichert. Die zuvor aktive Konfiguration wird dabei ersetzt.</li> <li>• Konfiguration speichern und vorhergehende Boot-Konfiguration sichern: Ihre Änderungen werden wie oben gespeichert, aber die zuvor aktive Konfiguration wird so gesi-</li> </ul>



Menü	Funktion
	chert, so dass Sie ggf. später wieder darauf zurückgreifen können. Es kann immer nur eine Sicherungsdatei erzeugt werden.

### Navigationsleiste

Assistenten	▼
Systemverwaltung	▼
Physikalische Schnittstellen	▼
VoIP	▼
Endgeräte	▼
Anrufkontrolle	▼
Anwendungen	▼
LAN	▼
Wireless LAN Controller	▼
Netzwerk	▼
Multicast	▼
WAN	▼
VPN	▼
Firewall	▼
Lokale Dienste	▼
Wartung	▼
Externe Berichterstellung	▼
Monitoring	▼

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 an-

gezeigt. 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
<b>ÜBERNEHMEN</b>	Aktualisiert die Ansicht.
<b>ABBRECHEN</b>	Wenn Sie einen neu konfigurierten Listeneintrag nicht sichern wollen, machen Sie diesen und die evtl. getätigten Einstellungen durch <b>Abbrechen</b> rückgängig.
<b>OK</b>	Bestätigt die Einstellungen eines neuen Eintrags und die Parameteränderungen in einer Liste.
<b>LOS</b>	Startet die konfigurierte Aktion sofort.
<b>NEU</b>	Ruft das Untermenü zum Anlegen eines neuen Eintrags auf.
<b>HINZUFÜGEN</b>	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.

Symbol	Funktion
	Nachrichten werden gespeichert.
	Mit diesem Symbol gelangen Sie auf die Benutzeroberfläche eines <b>elmeg</b> 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 einer Verbindung.
	Kennzeichnet, dass der Datenverkehr verschlüsselt wird.
	Löst einen WLAN-Bandscan aus.
	Zeigt die nächste Seite einer Liste an.
	Zeigt die vorherige Seite einer Liste an.

### Listenoptionen

Menü	Funktion
Aktualisierungsintervall	Hier können Sie das Intervall einstellen, in dem die Ansicht aktualisiert werden soll.  Geben Sie dazu einen Zeitraum in Sekunden in das Eingabe-

Menü	Funktion
	feld ein und bestätigen Sie mit <b>ÜBERNEHMEN</b> .
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 <b>Ansicht x pro Seite</b> die gewünschte Zahl eingeben.</p> <p>Mit den Tasten <b>«</b> und <b>»</b> blättern Sie eine Seite vor bzw. eine Seite zurück.</p> <p>Sie können nach bestimmten Stichwörtern innerhalb der Konfigurationsparameter filtern, indem Sie bei <b>Filtern in x &lt;Option&gt; y</b> die gewünschte Filterregel auswählen und das Suchwort in das Eingabefeld eingeben. <b>LOS</b> 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>

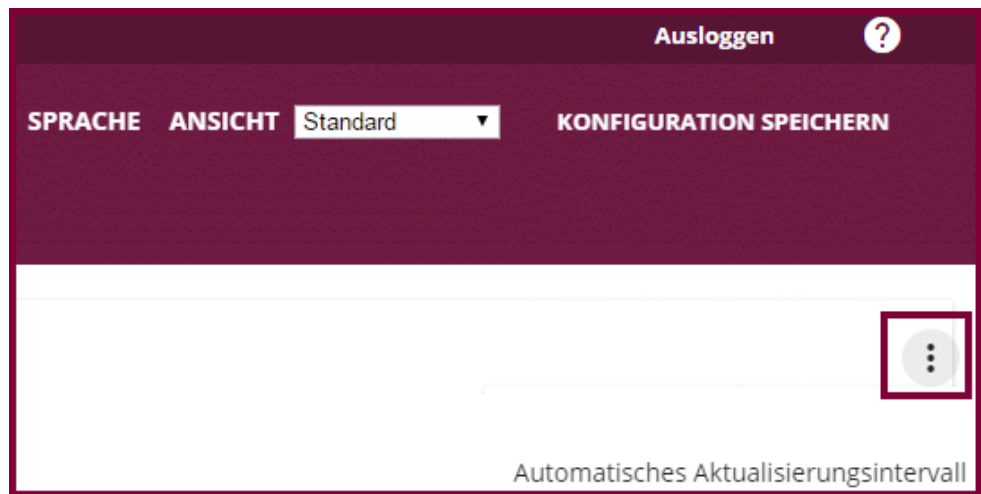
Automatisches Aktualisierungsintervall 60 Sekunden **ÜBERNEHMEN**

Konfiguration des Aktualisierungsintervalls

Ansicht 20 pro Seite **«** **»** Filtern in Keiner **▼** gleich **▼** **LOS**

Liste filtern

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



Automatische Aktualisierungsintervall öffnen

Klicken Sie auf **Automatisches Aktualisierungsintervall**.

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






Konfiguration des Aktualisierungsintervalls

### Struktur der Konfigurationsmenüs

Die Menüs enthalten folgende Grundstrukturen:

#### Menüstruktur


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

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

Für die Konfiguration stehen folgende Optionen zur Verfügung:

### Konfigurationselemente

Menü	Funktion
Eingabefelder	z. B. leeres Textfeld  Textfeld mit verdeckter Eingabe  Geben Sie entsprechende Daten ein.
Radiobuttons	z. B.  Wählen Sie die entsprechende Option aus.
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 <b>HINZUFÜGEN</b> . Ein neuer Listen-

Menü	Funktion
	eintrag wird angelegt. Geben Sie die entsprechenden Daten ein. Bleiben die Felder des Listeneintrags leer, wird dieser bei Bestätigen mit <b>OK</b> 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 eingeblendeten Hinweise in den Untermenüs! Diese geben Auskunft über eventuelle Fehlkonfigurationen.

### 5.2.1.3 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.

## 6 Assistenten

Das Menü **Assistenten** bietet Schritt-für-Schritt-Anleitungen für grundlegende Konfigurationsaufgaben.

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



## 7 Systemverwaltung

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

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

### 7.1 Status

Wenn Sie sich in 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

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
<b>Uptime</b>	Zeigt die Zeit an, die vergangen ist, seit das Gerät neu gestartet wurde.
<b>Systemdatum</b>	Zeigt das aktuelle Systemdatum und die Systemuhrzeit an.
<b>Seriennummer</b>	Zeigt die Geräte-Seriennummer an.
<b>BOSS-Version</b>	Zeigt die aktuell geladene Version der Systemsoftware an.
<b>Letzte gespeicherte Konfiguration</b>	Zeigt Tag, Datum und Uhrzeit der letzten Konfigurationsspeicherung (Boot-Konfiguration im Flash) an.
<b>Status Nachtbetrieb</b>	Zeigt an, ob sich Ihr Gerät im Normalbetrieb ( <i>Aus</i> ) oder im Nachtbetrieb ( <i>An</i> ) befindet.

#### Felder im Menü Ressourceninformationen

Feld	Wert
<b>CPU-Nutzung</b>	Zeigt die CPU-Auslastung in Prozent an.
<b>Arbeitsspeichernutzung</b>	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtspeicher in MByte an. Die Auslastung wird außerdem in Klammern in Prozent angezeigt.
<b>Aktive Sitzungen (SIF, RTP, etc... )</b>	Zeigt die Summe aller SIF, TDRS und IP-Lastverteilung Sessions an.
<b>Aktive IPSec-Tunnel</b>	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.
<b>DSP-Kanäle</b>	Zeigt die aktuell belegten DSP-Kanäle an.

**Felder im Menü SIP-Provider**

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

**Felder im Menü Physikalische Schnittstellen**

Feld	Wert
<b>Schnittstelle - Verbindungsinformation - Link</b>	<p>Hier sind alle physikalischen Schnittstellen aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle angeschlossen bzw. aktiv ist.</p> <p>Schnittstellendetails für Ethernet-Schnittstellen:</p> <ul style="list-style-type: none"> <li>• IP-Adresse</li> <li>• Netzmaske</li> <li>• Nicht konfiguriert</li> </ul> <p>Schnittstellendetails für ISDN-Schnittstellen:</p> <ul style="list-style-type: none"> <li>• Konfiguriert</li> <li>• Nicht konfiguriert</li> </ul> <p>Schnittstellendetails für xDSL-Schnittstellen:</p> <ul style="list-style-type: none"> <li>• Letzte Änderung</li> <li>• DSL Betriebsmodus</li> <li>• DSL-Geschwindigkeit (Empfangen und Senden)</li> <li>• Datenvolumen</li> </ul>

**Felder im Menü WAN-Schnittstellen**

Feld	Wert
<b>Beschreibung - Verbin-</b>	Hier sind alle WAN-Schnittstellen aufgelistet und deren wich-

Feld	Wert
<b>dungsinformation - Link</b>	tigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle aktiv ist.

## 7.2 Globale Einstellungen

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

### 7.2.1 System

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

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Grundeinstellungen

Feld	Wert
<b>Systemname</b>	Geben Sie den Systemnamen Ihres Geräts ein. Dieser wird auch als PPP-Host-Name benutzt.  Möglich ist eine Zeichenkette mit max. 255 Zeichen.  Als Standardwert ist der Gerätetyp voreingestellt.
<b>Standort</b>	Geben Sie an, wo sich Ihr Gerät befindet.
<b>Kontakt</b>	Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden.  Möglich ist eine Zeichenkette mit max. 255 Zeichen.  Nur für Kompaktsysteme: Der Standardwert ist <i>BINTECELMEG</i> .
<b>Maximale Anzahl der Syslog-Protokolleinträge</b>	Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen.  Mögliche Werte sind <i>0</i> bis <i>1000</i> .  Der Standardwert ist <i>50</i> . Sie können die gespeicherten Meldungen in <b>Monitoring-&gt;Internes Protokoll</b> anzeigen lassen.
<b>Maximales Nachricht-</b>	Wählen Sie die Priorität der Systemmeldungen aus, ab der pro-

Feld	Wert
<b>tenlevel von Systemprotokolleinträgen</b>	<p>tokolliert werden soll.</p> <p>Nur Systemmeldungen mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass bei der Priorität <i>Debug</i> sämtliche erzeugten Meldungen aufgezeichnet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Notfall</i>: Es werden nur Meldungen mit der Priorität Notfall aufgezeichnet.</li> <li>• <i>Alarm</i>: Es werden Meldungen mit der Priorität Notfall und Alarm aufgezeichnet.</li> <li>• <i>Kritisch</i>: Es werden Meldungen mit der Priorität Notfall, Alarm und Kritisch aufgezeichnet.</li> <li>• <i>Fehler</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch und Fehler aufgezeichnet.</li> <li>• <i>Warnung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler und Warnung aufgezeichnet.</li> <li>• <i>Benachrichtigung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung und Benachrichtigung aufgezeichnet.</li> <li>• <i>Information</i> (Standardwert): Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung, Benachrichtigung und Informationen aufgezeichnet.</li> <li>• <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.</li> </ul>
<b>Maximale Anzahl der Accounting-Protokolleinträge</b>	<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>
<b>Herstellernamen anzeigen</b>	<p>Hier könne 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 <i>00:a0:f9:37:12:c9</i> wird mit Herstelleranzeige zum Beispiel <i>BintecCo_37:12:c9</i> angezeigt.</p>

Feld	Wert
<b>Konfiguration der automatischen Speicherung</b>	<p>Hier können Sie festlegen, ob Änderungen der Konfiguration automatisch gespeichert werden sollen.</p> <p>Standardmäßig ist die Option aktiv.</p> <p>Eine genauere Beschreibung finden Sie unter dieser Tabelle.</p>

## Konfiguration der automatischen Speicherung

Nimmt man über das GUI eine Änderung an der Konfiguration vor und bestätigt diese auf der GUI-Seite (mit der entsprechenden Schaltfläche, also z. B. **OK**), so wird die Änderung wie bisher sofort aktiv. Zusätzlich wird die Änderung des Zustands der Konfiguration registriert. Im Syslog (Syslog-Level = *debug*) erscheint die Meldung *new config state: modified*. Sobald nach Erreichen dieses Zustands ein erneuter HTTP(S)-Verkehr zwischen dem Browser und dem GUI stattfindet, wird die Änderung des Zustands bestätigt und zur Speicherung freigegeben. Im Syslog erscheint die Meldung *new config state: confirmed*.

Sobald dieser Zustand erreicht ist und die Konfigurationssitzung über den Browser beendet wird, ohne dass die Konfiguration aktiv gespeichert wird, so nimmt das Gerät nach Ablauf der HTTP(S) Session eine automatische Speicherung vor. Im Syslog erscheint zunächst eine Meldung zur Beendigung der aktiven Session (z. B. *delete httpSessionStat entry admin at Fri Apr 21 11:04:34 2017 (keep alive timeout)*), danach erfolgt die Speicherung: *auto save on session termination*.

Sollte man sich durch einen Konfigurationsfehler selbst vom Zugriff auf das GUI gesperrt haben, findet die Bestätigung der Änderung (*new config state: confirmed*) nicht statt und sie wird nach Ablauf der Session nicht gespeichert. Durch einen Neustart des Geräts lässt sich die Änderung dann rückgängig machen.

## Übergabe auf besetzten Teilnehmer

In der Konfiguration kann festgelegt werden, ob die Weitergabe eines Gesprächs auf einen besetzten Teilnehmer möglich ist oder bei "Aus" der Anrufer den Besetzten hört und damit der Anruf beendet ist. Sonst wird der Anrufer gehalten und hört die Wartemusik. Legt der Zerteilnehmer den Hörer auf, hört der gehaltene Teilnehmer bei Auswahl *Mit Freiton* den Freiton, bei *Mit Wartemusik* weiterhin die Wartemusik, bis der Zerteilnehmer den Ruf entgegen nimmt. Der Zerteilnehmer wird gerufen und kann das gehaltene Gespräch übernehmen.

## Felder im Menü Systemeinstellungen

Feld	Wert
<b>Signalisierung der Übergabe</b>	<p>Stellen Sie ein, wie das Vermitteln auf einen internen Teilnehmer erfolgen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Mit Freiton</i> (Standardwert): Der Anrufer hört während er vermittelt wird eine Wartemusik des Systems und, nachdem er vermittelt wurde, den Freiton.</li> <li>• <i>Mit Wartemusik (Music On Hold, MoH)</i>: Der Anrufer hört, während er vermittelt wird, eine Wartemusik des Systems, bis der Zielteilnehmer den Ruf annimmt.</li> </ul>
<b>Übergabe auf besetzten Teilnehmer</b>	<p>Stellen Sie ein, ob das Vermitteln eines Anrufers auf einen besetzten Teilnehmer möglich ist.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Abwurf auf Rufnummer</b>	<p>Stellen Sie ein, auf welches Ziel kommende Anrufe z. B. bei Falschwahl abgeworfen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Kein Abwurf - Besetztton</i>: Der Anrufer hört standardmäßig den Besetztton und kann nicht auf ein Ziel abgeworfen werden.</li> <li>• <i>&lt;Rufnummer&gt;</i>: Der kommende Anruf wird standardmäßig an die ausgewählte Rufnummer geleitet.</li> </ul> <p>Standardwert ist die voreingestellte Internrufnummer <i>40 (Team global)</i>.</p>
<b>Externe Verbindungen zusammenschalten</b>	<p>Wählen Sie aus, ob beim Makeln mit zwei Externteilnehmern diese, nachdem Sie den Hörer aufgelegt haben, verbunden werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

## Ländereinstellungen

Ihr Unternehmen ist international ausgerichtet und hat Niederlassungen in mehreren Län-

dern. Trotz der abweichenden Netz-Realisierung in den einzelnen Ländern möchten Sie in jeder Niederlassung das gleiche System einsetzen. Durch die Einstellung der Ländervariante wird das System an die Besonderheiten des Netzes in dem gewünschten Land angepasst.

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

### Felder im Menü **Ländereinstellungen**

Feld	Wert
<b>Ländereinstellung</b>	<p>Wählen Sie das Land aus, in dem das System genutzt werden soll.</p> <p>Beachten Sie: Hiermit wird nicht die Sprache der Texte im Systemmenü der Systemtelefone umgestellt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Deutschland</i> (Standardwert)</li> <li>• <i>Nederland</i></li> <li>• <i>Great Britain</i></li> <li>• <i>België</i></li> <li>• <i>Italia</i></li> <li>• <i>Danmark</i></li> <li>• <i>España</i></li> <li>• <i>Sverige</i></li> <li>• <i>Norge</i></li> <li>• <i>France</i></li> <li>• <i>Portugal</i></li> <li>• <i>Österreich</i></li> <li>• <i>Schweiz</i></li> <li>• <i>Česko</i></li> <li>• <i>Slovenija</i></li> <li>• <i>Polska</i></li> <li>• <i>Magyarország</i></li> <li>• <i>Ellada</i></li> </ul>
<b>Internationaler Präfix /</b>	Geben Sie die Länderkennzahl ein.



Feld	Wert
<b>Länderkennzahl</b>	<p>Sie benötigen diesen Eintrag, wenn Sie z. B. unter <b>SIP-Provider</b> eine internationale Rufnummer automatisch generieren lassen möchten. Sie wählen wie gewohnt die nationale Vorwahl z. B. 05151 909999 und das System wählt dann automatisch +495151 909999. Tragen Sie die Länderkennzahl nicht ein, kann es zur Falschwahl kommen, das System wählt dann +5151 909999. Ohne den Eintrag <b>Internationale Rufnummer erzeugen</b> und <b>Internationaler Präfix / Länderkennzahl</b> muss bei SIP-Providern immer die vollständige Rufnummer mit Länderkennzahl gewählt werden.</p> <p>Beachten Sie: Nicht alle SIP-Provider unterstützen diese Einstellung.</p>
<b>Nationaler Präfix / Ortsnetzkennzahl</b>	<p>Tragen Sie den nationalen Präfix bzw. die Ortsnetzkennzahl für den Ort ein, an der Ihr System installiert ist. Diese Ortsnetzkennzahl wird beim Anlagenanschluss dringend benötigt, da sonst z. B. der automatische Rückruf nach extern nicht möglich ist.</p>

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

#### Felder im Menü **Abrechnungseinstellungen**

Feld	Wert
<b>Tarifeinheitenfaktor</b>	<p>Geben Sie den Faktor für die Verbindungskosten ein.</p> <p>Der Standardwert ist <i>0,00</i>.</p>
<b>Währung</b>	<p>Geben Sie hier den Namen der Währung, z. B. <i>EUR</i>, ein (max. dreistellig). Diese Eingabe ist nur ein Name, der in keiner Berechnung des Tarifeinheitenfaktors berücksichtigt wird. Sonderzeichen sind nicht erlaubt.</p>
<b>Gebühreninformationen (S0/Upn-Erweiterung)</b>	<p>Wählen Sie die Übertragungsmethode von Gebühreninformationen am internen S0-Bus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keypad</i>: Abhängig von Land und Provider werden die Gebühreninformationen so übertragen, dass sie direkt vom Endgerät angezeigt werden können.</li> <li>• <i>Funktional</i>: Die Gebühreninformationen werden binär kodiert übertragen und müssen von den Endgeräten erst deko-</li> </ul>

Feld	Wert
	<p>diert werden (EURO ISDN).</p> <ul style="list-style-type: none"> <li>• <i>Beide</i> (Standardwert): Beide Protokolle werden erkannt.</li> </ul>

#### Felder im Menü Tagmodus

Feld	Wert
<b>Globaler Abwurf</b>	<p>Wählen Sie die Anrufvariante im Tagmodus aus, die für das Gesamtsystem gelten soll, wenn kein spezieller Abwurf eingerichtet ist.</p> <p>Der Standardwert ist <i>Variante 1</i>.</p>

#### Nachtbetrieb

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

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

#### Felder im Menü Nachtbetrieb

Feld	Wert
<b>Team-Signalisierung</b>	<p>Wählen Sie die Anrufvariante für die Team-Signalisierung im Nachtbetrieb aus.</p> <p>Der Standardwert ist <i>Variante 1</i>.</p>
<b>TFE-Signalisierung</b>	<p>Wählen Sie die TFE-Anrufvariante für die TFE-Signalisierung im Nachtbetrieb aus.</p> <p>Der Standardwert ist <i>Variante 1</i>.</p>
<b>Abwurf auf Ansage</b>	<p>Wählen Sie die Anrufvariante für Abwurf auf Ansage im Nachtbetrieb aus.</p> <p>Der Standardwert ist <i>Variante 1</i>.</p>
<b>Individueller Teilnehmer Abwurf</b>	<p>Wählen Sie die Anrufvariante für Abwurf auf Durchwahl im Nachtbetrieb aus.</p> <p>Der Standardwert ist <i>Variante 1</i>.</p>

Feld	Wert
<b>Globaler Abwurf</b>	Wählen Sie die Anrufvariante für Allgemeinen Abwurf im Nachtbetrieb aus.  Der Standardwert ist <i>Variante 1</i> .
<b>Meldeeingang</b>	Wählen Sie die Anrufvariante für Alarm im Nachtbetrieb aus.  Der Standardwert ist <i>Variante 1</i> .

## 7.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.



### Hinweis

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

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

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

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

### Felder im Menü Systempasswort

Feld	Wert
<b>Systemadministrator-Kennwort</b>	Geben Sie das Passwort für den Benutzernamen <code>admin</code> an.  Das Standard-Passwort ist <code>admin</code> .  Dieses Passwort wird bei SNMPv3 auch für Authentifizierung (MD5) und Verschlüsselung (DES) verwendet.  Einige Geräte verfügen über ein individuell vergebenes Passwort. In diesem Fall finden Sie dies auf dem Typenschild Ihres Geräts.

Feld	Wert
<b>Systemadministrator-Kennwort bestätigen</b>	Bestätigen Sie das Passwort, indem Sie es erneut eingeben.

## PIN1 und PIN2

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

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

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

Folgende Leistungsmerkmale werden über die PIN2 geschützt:

- Fernzugang für Follow me, Raumüberwachung

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

Feld	Wert
<b>PIN1</b>	Geben Sie PIN1 ein.  Der Standardwert ist <i>none</i> .  Durch die 4-stellige PIN1 (Geheimzahl) schützen Sie die Einstellungen Ihres Systems durch die Konfiguration über ein Telefon.

### Felder im Menü Fernzugang Telefonie (sechsstellige PIN)

Feld	Wert
<b>Fernzugang (z. B. Follow me, Raumüberwachung)</b>	Wählen Sie aus, ob ein Fernzugang auf Ihr System gestattet werden soll.  Mit <i>Aktiviert</i> wird die Funktion aktiviert.  Standardmäßig ist die Funktion nicht aktiv.
<b>PIN2</b>	Nur wenn <b>Fernzugang (z. B. Follow me, Raumüberwachung)</b> aktiviert ist.

Feld	Wert
	<p>Geben Sie die <b>PIN2</b> ein.</p> <p>Der Standardwert ist <i>000000</i>.</p> <p>Durch die 6-stellige <b>PIN2</b> schützen Sie den Zugang von extern (Fernzugang).</p>

#### Felder im Menü **SNMP-Communities**

Feld	Wert
<b>SNMP Read Community</b>	<p>Geben Sie das Passwort für den Benutzernamen <code>read</code> ein.</p> <p>Das Standard-Passwort ist <i>admin</i>.</p>
<b>SNMP Write Community</b>	<p>Geben Sie das Passwort für den Benutzernamen <code>write</code> ein.</p> <p>Das Standard-Passwort ist <i>admin</i>.</p>

#### Feld im Menü **Globale Passwortoptionen**

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

### 7.2.3 Datum und Uhrzeit

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

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

## ISDN/Manuell

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

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

## Zeitserver

Sie können die Systemzeit auch automatisch über verschiedene Zeitserver beziehen. Um sicherzustellen, dass das Gerät die gewünschte aktuelle Zeit verwendet, sollten Sie einen oder mehrere Zeitserver konfigurieren.



### Hinweis

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

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

### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Zeitzone</b>	<p>Wählen Sie die Zeitzone aus, in der Ihr Gerät installiert ist.</p> <p>Möglich ist die Auswahl der Universal Time Coordinated (UTC) plus oder minus der Abweichung davon in Stunden oder ein vordefinierter Ort.</p> <p>Nur für Kompaktsysteme: Der Standardwert ist <i>Europe/Berlin</i>.</p>

Feld	Beschreibung
<b>Aktuelle Ortszeit</b>	Hier werden das aktuelle Datum und die aktuelle Systemzeit angezeigt. Der Eintrag kann nicht verändert werden.

#### Felder im Menü **Manuelle Zeiteinstellung**

Feld	Beschreibung
<b>Datum einstellen</b>	Wenn Sie auf das Eingabefeld für das Datum klicken, öffnet sich ein Standardkalender in Monatsansicht. Ein Klick auf das gewünschte Datum überträgt es in die Konfigurationsoberfläche.
<b>Zeit einstellen</b>	Geben Sie eine neue Uhrzeit ein.  Format: <ul style="list-style-type: none"> <li>• <b>Stunde:</b> hh</li> <li>• <b>Minute:</b> mm</li> </ul>

#### Felder im Menü **Automatische Zeiteinstellung (Zeitprotokoll)**

Feld	Beschreibung
<b>ISDN-Zeitserver</b>	Legen Sie fest, ob die Systemzeit über ISDN aktualisiert werden soll.  Falls ein Zeitserver konfiguriert ist, wird die Zeit nur solange über ISDN ermittelt, bis ein erfolgreiches Update von diesem Zeitserver empfangen wurde. Für den Zeitraum, in dem die Zeit über einen Zeitserver ermittelt wird, wird die Aktualisierung über ISDN außer Kraft gesetzt.  Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiviert.  Standardmäßig ist die Funktion aktiv.
<b>Erster Zeitserver</b>	Geben Sie den ersten Zeitserver an, entweder mit Domänennamen oder IP-Adresse.  Wählen Sie außerdem das Protokoll für die Abfrage des Zeitervers aus.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123.</li> </ul>

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



Feld	Beschreibung
<b>tervall</b>	<p>sche Zeitaktualisierung durchgeführt wird.</p> <p>Der Standardwert ist <i>1440</i>.</p>
<b>Zeitaktualisierungsrichtlinie</b>	<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"> <li>• <i>Normal</i> (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen.</li> <li>• <i>Aggressiv</i>: Zehn Minuten lang wird versucht, den Zeitserver zuerst nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen.</li> <li>• <i>Endlos</i>: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen.</li> </ul> <p>Bei der Verwendung von Zertifikaten für die Verschlüsselung des Datenverkehrs in einem VPN ist es von zentraler Bedeutung, dass auf dem Gerät die korrekte Zeit eingestellt ist. Um dies sicherzustellen, wählen Sie für <b>Zeitaktualisierungsrichtlinie</b> den Wert <i>Endlos</i>.</p>
<b>System als Zeitserver</b>	<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 aktiv. Zeitanfragen der Clients im LAN werden beantwortet.</p>

## 7.2.4 Timer

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

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

## Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Rufweiterleitung (CFNR)</b>	<p>Geben Sie die Zeit in Sekunden ein, nach der eine <b>Rufweiterleitung (CFNR)</b> ausgeführt wird.</p> <p>Möglich sind Werte von <i>1</i> bis <i>99</i>.</p> <p>Der Standardwert ist <i>15</i>.</p>
<b>Direktruf</b>	<p>Geben Sie die Zeit in Sekunden ein, nach der beim Abheben des Hörers die konfigurierte Rufnummer gewählt wird.</p> <p>Sie möchten ein Telefon einrichten, bei dem die Verbindung zu einer bestimmten Rufnummer auch ohne die Eingabe der Rufnummer aufgebaut wird (z. B. Notruftelefon). Sie befinden sich außer Haus. Es gibt jedoch jemanden zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Haben Sie für ein oder mehrere Telefone die Funktion "Direktruf" eingerichtet, braucht nur der Hörer des entsprechenden Telefons abgehoben zu werden. Nach einer in der Konfiguration eingestellten Zeit ohne weitere Eingaben wählt das System automatisch die festgelegte Direktrufnummer.</p> <p>Wählen Sie nach dem Abheben des Hörers nicht innerhalb der vorgegebenen Zeit, wird die automatische Wahl eingeleitet.</p> <p>Möglich sind Werte von <i>1</i> bis <i>30</i>.</p> <p>Der Standardwert ist <i>5</i>.</p>
<b>Externe TFE-Verbindung</b>	<p>Wird ein TFE-Gespräch von einem externen Telefon abgefragt, können Sie hier die Zeit in Sekunden einstellen, nach der dieses Gespräch zwangsgetrennt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Endlos</i></li> <li>• <i>60 Sekunden</i></li> <li>• <i>120 Sekunden</i></li> <li>• <i>180 Sekunden</i> (Standardwert)</li> <li>• <i>240 Sekunden</i></li> <li>• <i>300 Sekunden</i></li> </ul>

**Felder im Menü Erweiterte Einstellungen**

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

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

## 7.2.5 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](http://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](http://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 **Standard Lizenzen** (Standardlizenzen).

### 7.2.5.1 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
<b>Lizenzseriennummer</b>	Geben Sie die Lizenzseriennummer ein, die Sie beim Kauf der Lizenz erhalten haben.
<b>Lizenzschlüssel</b>	Geben Sie den Lizenzschlüssel ein, den Sie per E-Mail erhalten haben.



#### Hinweis


Wenn als Status *Nicht OK* angezeigt wird:

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

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

### Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

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

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

## 7.3 Kennziffern

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

### 7.3.1 Änderbare Kennziffern

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

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

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

## Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Amtskennziffer</b>	<p>Wählen Sie die Amtskennziffer aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keine</i></li> <li>• 0 (Standardwert)</li> <li>• 6</li> <li>• 7</li> <li>• 8</li> <li>• 9</li> </ul>
<b>Pick-Up Gruppe</b>	Geben Sie die neue Kennziffer für das Leistungsmerkmal <b>Pick-Up-Gruppe</b> ein.
<b>Pick-Up Gezielt</b>	Geben Sie die neue Kennziffer für das Leistungsmerkmal <b>Pick-Up Gezielt</b> ein.
<b>Vergabe von Projektnummern</b>	Geben Sie die neue Kennziffer für das Leistungsmerkmal <b>Vergabe von Projektnummern</b> ein.
<b>Kurzwahl</b>	Geben Sie die neue Kennziffer für das Leistungsmerkmal <b>Kurzwahl</b> ein.
<b>Manuelle Auswahl der Bündel</b>	<p>Legen Sie die neuen Kennziffern für das Leistungsmerkmal <b>Manuelle Auswahl der Bündel</b> an.</p> <p>Legen Sie dafür zunächst durch Klicken von <b>Hinzufügen</b> eine Bündelauswahl an, wählen Sie das Bündel aus und geben Sie die gewünschte Kennziffer für das Bündel ein.</p>
<b>Offene Rückfrage</b>	<p>Legen Sie die neuen Kennziffern für das Leistungsmerkmal <b>Offene Rückfrage</b> an.</p> <p>Legen Sie dafür zunächst durch Klicken von <b>Hinzufügen</b> ein Wartefeld, in dem der Anrufer gehalten werden soll, an und geben Sie die gewünschte Kennziffer für das Wartefeld ein. Sie können maximal 10 Einträge anlegen.</p>

## 7.4 Schnittstellenmodus / Bridge-Gruppen

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

### Routing versus Bridging

Mit Bridging werden gleichartige Netze verbunden. Im Gegensatz zum Routern arbeiten Bridges auf Schicht 2 (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)

## 7.4.1 Schnittstellen

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

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

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

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

### Felder im Menü Schnittstellen

Feld	Beschreibung
<b>Schnittstellenbeschreibung</b>	Zeigt den Namen der Schnittstelle an.
<b>Modus / Bridge-Gruppe</b>	Wählen Sie aus, ob Sie die Schnittstelle im <i>Routing-Modus</i> betreiben möchten oder ordnen Sie die Schnittstelle einer bestehenden ( <i>br0</i> , <i>br1</i> usw.) oder neuen Bridge-Gruppe ( <i>Neue Bridge-Gruppe</i> ) zu. Bei Auswahl von <i>Neue Bridge-Gruppe</i> wird nach Anklicken des <b>OK</b> -Buttons automatisch eine neue Bridge-Gruppe erzeugt.
<b>Konfigurationsschnittstelle</b>	Wählen Sie aus, über welche Schnittstelle die Konfiguration durchgeführt wird.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Eine auswählen</i> (Standardwert): Einstellung im Auslieferungszustand. Die richtige Konfigurationsschnittstelle muss aus den anderen Optionen ausgewählt werden.</li> <li>• <i>Nicht beachten</i>: Keine Schnittstelle wird als Konfigurationsschnittstelle definiert.</li> <li>• <i>&lt;Schnittstellename&gt;</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.</li> </ul>

### 7.4.1.1 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
<b>Schnittstelle</b>	Wählen Sie die Schnittstelle aus, deren Modus Sie verändern wollen.

#### Bearbeiten für Geräte der Wlxxxxn und RS-Serie

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

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
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, die gerade bearbeitet wird.

Feld	Wert
<b>Wildcard-Modus</b>	<p>Wählen Sie aus, welchen Wildcard-Modus Sie auf der Schnittstelle nutzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Es wird kein Wildcard-Modus verwendet.</li> <li>• <i>statisch</i>: Mit dieser Einstellung müssen Sie bei <b>Wildcard-MAC-Adresse</b> 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.</li> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Wildcard-MAC-Adresse</b>	<p>Nur für <b>Wildcard-Modus</b> = <i>statisch</i></p> <p>Geben Sie die MAC-Adresse eines Geräts eingeben, das über IP angebunden ist.</p>
<b>Transparente MAC-Adresse</b>	<p>Nur für <b>Wildcard-Modus</b> = <i>statisch, zuerst</i></p> <p>Wählen Sie aus, ob die <b>Wildcard-MAC-Adresse</b> 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>

Feld	Wert
	Standardmäßig ist die Funktion nicht aktiv.

## 7.5 Administrativer Zugriff

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

### 7.5.1 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. Wenn die Option aktiviert ist, wird sie nach ca. 30 Minuten automatisch wieder deaktiviert.

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

#### Felder im Menü Erweiterte Einstellungen

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

### 7.5.1.1 Hinzufügen

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

#### Felder im Menü Zugriff

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

### 7.5.2 SSH

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

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

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

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



#### Hinweis

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

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

#### Felder im Menü SSH-Parameter (Secure Shell)

Feld	Wert
<b>SSH-Dienst aktiv</b>	Wählen Sie aus, ob der SSH-Daemon aktiviert werden soll.  Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.

Feld	Wert
	Standardmäßig ist die Funktion aktiv.
<b>SSH-Port</b>	Hier können Sie den Port eingeben, über den die SSH-Verbindung aufgebaut werden soll.  Der Standardwert ist <i>22</i> .
<b>Maximale Anzahl gleichzeitiger Verbindungen</b>	Tragen Sie die maximale Anzahl gleichzeitig aktiver SSH-Verbindungen ein.  Der Standardwert ist <i>1</i> .

#### Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

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

#### Felder im Menü Schlüsselstatus

Feld	Wert
<b>RSA-Schlüsselstatus</b>	Zeigt den Status des RSA-Schlüssels an.

Feld	Wert
	<p>Wenn bisher kein RSA-Schlüssel generiert wurde, wird <i>Nicht generiert</i> und ein Link <i>Generieren</i> angezeigt. Wird der Link angeklickt, wird der Prozess für die Generierung angestoßen und die Ansicht aktualisiert. Nun wird der Status <i>Wird generiert</i> angezeigt. Wenn die Generierung erfolgreich abgeschlossen wurde, ändert sich der Status von <i>Wird generiert</i> auf <i>Generiert</i>. Sollte bei der Generierung ein Fehler aufgetreten sein, wird erneut <i>Nicht generiert</i> mit Link <i>Generieren</i> angezeigt. Sie können die Generierung wiederholen.</p> <p>Wird der Status <i>Unbekannt</i> angezeigt, ist die Generierung eines Schlüssels nicht möglich, z. B. wegen fehlendem Speicherplatz im FlashROM.</p>
<b>ECDSA-Schlüsselstatus</b>	<p>Zeigt den Status des ECDSA-Schlüssels an.</p> <p>Wenn bisher kein ECDSA-Schlüssel generiert wurde, wird <i>Nicht generiert</i> und ein Link <i>Generieren</i> angezeigt. Wird der Link angeklickt, wird der Prozess für die Generierung angestoßen und die Ansicht aktualisiert. Nun wird der Status <i>Wird generiert</i> angezeigt. Wenn die Generierung erfolgreich abgeschlossen wurde, ändert sich der Status von <i>Wird generiert</i> auf <i>Generiert</i>. Sollte bei der Generierung ein Fehler aufgetreten sein, wird erneut <i>Nicht generiert</i> mit Link <i>Generieren</i> angezeigt. Sie können die Generierung wiederholen.</p> <p>Wird der Status <i>Unbekannt</i> angezeigt, ist die Generierung eines Schlüssels nicht möglich, z. B. wegen fehlendem Speicherplatz im FlashROM.</p>
<b>ED25519-Schlüsselstatus</b>	<p>Zeigt den Status des ED25519-Schlüssels an.</p> <p>Wenn bisher kein ED25519-Schlüssel generiert wurde, wird <i>Nicht generiert</i> und ein Link <i>Generieren</i> angezeigt. Wird der Link angeklickt, wird der Prozess für die Generierung angestoßen und die Ansicht aktualisiert. Nun wird der Status <i>Wird generiert</i> angezeigt. Wenn die Generierung erfolgreich abgeschlossen wurde, ändert sich der Status von <i>Wird generiert</i> auf <i>Generiert</i>. Sollte bei der Generierung ein Fehler aufgetreten sein, wird erneut <i>Nicht generiert</i> mit Link <i>Generieren</i> angezeigt. Sie können die Generierung wiederholen.</p>



Feld	Wert
	Wird der Status <i>Unbekannt</i> angezeigt, ist die Generierung eines Schlüssels nicht möglich, z. B. wegen fehlendem Speicherplatz im FlashROM.

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Wert
<b>Toleranzzeit beim Login</b>	<p>Geben Sie die Zeit (in Sekunden) ein, die für den Verbindungsaufbau zur Verfügung steht. Wenn ein Client innerhalb dieser Zeit nicht erfolgreich authentifiziert werden kann, wird die Verbindung getrennt.</p> <p>Der Standardwert ist <i>600</i> Sekunden.</p>
<b>Komprimierung</b>	<p>Wählen Sie aus, ob Datenkompression verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>TCP-Keepalives</b>	<p>Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Protokollierungslevel</b>	<p>Wählen Sie den Syslog-Level für die vom SSH Daemon generierten Syslog-Messages aus.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> <li>• <i>Information</i> (Standardwert): Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet.</li> <li>• <i>Fatal</i>: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet.</li> <li>• <i>Fehler</i>: Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet.</li> <li>• <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.</li> </ul>

### 7.5.3 SNMP

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

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

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

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

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

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

#### Felder im Menü Grundeinstellungen

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

Feld	Wert
<b>SNMP multicast discovery</b>	<p>Aktivieren oder deaktivieren Sie die Funktion <b>SNMP multicast discovery</b>.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>



### Tipp

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

## 7.6 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

### 7.6.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

## RADIUS Pakete


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

### Pakettypen

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

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

### 7.6.1.1 Bearbeiten oder Neu

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

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

#### Felder im Menü Basisparameter

Feld	Wert
<b>Authentifizierungstyp</b>	<p>Wählen Sie aus, wofür der RADIUS-Server verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>PPP-Authentifizierung</i> (Standardwert, nur für PPP-Verbindungen): Der RADIUS-Server wird verwendet, um den Zugang zu einem Netzwerk zu regeln.</li> <li>• <i>Accounting</i> (nur für PPP-Verbindungen): Der RADIUS-Server wird zur Erfassung statistischer Verbindungsdaten verwendet.</li> <li>• <i>Login-Authentifizierung</i>: Der RADIUS-Server wird verwendet, um den Zugang zur SNMP Shell Ihres Geräts zu kontrollieren.</li> <li>• <i>IPSec-Authentifizierung</i>: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln.</li> <li>• <i>WLAN (802.1x)</i>: Der RADIUS-Server wird verwendet, um den Zugang zu einem Drahtlosnetzwerk zu regeln.</li> <li>• <i>XAUTH</i>: Der RADIUS-Server wird verwendet, um IPSec-Peers über XAuth zu authentisieren.</li> </ul>
<b>Betreibermodus</b>	<p>Nur für <b>Authentifizierungstyp</b> = <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"> <li>• <i>France Telecom</i>: Für Hotspot-Anwendungen der France</li> </ul>

Feld	Wert
	<p>Telecom.</p> <ul style="list-style-type: none"> <li>• <i>bintec HotSpot Server</i>: Für Hotspot-Anwendungen.</li> </ul>
<b>Server-IP-Adresse</b>	Geben Sie die IP-Adresse des RADIUS-Servers ein.
<b>RADIUS-Passwort</b>	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein.
<b>Standard-Benutzerpasswort</b>	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.
<b>Priorität</b>	<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 <b>Richtlinie</b> in den erweiterten Einstellungen.</p>
<b>Eintrag aktiv</b>	<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>
<b>Gruppenbeschreibung</b>	<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 <b>Priorität</b> und der <b>Richtlinie</b> abgefragt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Neu</i> (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein.</li> <li>• <i>Standardgruppe 0</i>: Wählen Sie diesen Eintrag für spezielle Anwendungen, wie z. B. Hotspot-Server-Konfiguration, aus.</li> <li>• <i>&lt;Gruppenname&gt;</i>: Wählen Sie aus der Liste eine schon defi-</li> </ul>

Feld	Wert
	nierte Gruppe aus.

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Wert
<b>Richtlinie</b>	<p>Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Verbindlich</i> (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert.</li> <li>• <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.</li> </ul>
<b>UDP-Port</b>	<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>
<b>Server Timeout</b>	<p>Geben Sie die maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden ein.</p> <p>Nach Ablauf dieser Zeit wird die Anfrage gemäß <b>Wiederholungen</b> 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>
<b>Erreichbarkeitsprüfung</b>	<p>Wählen Sie eine Überprüfung der Erreichbarkeit eines RADIUS-Servers im <b>Status</b> <i>Inaktiv</i>.</p> <p>Es wird regelmäßig (alle 20 Sekunden) ein Alive-Check durch-</p>

Feld	Wert
	<p>geführt, in dem ein ACCESS_REQUEST an die IP-Adresse des RADIUS-Servers gesendet wird. Bei erneuter Erreichbarkeit wird der <b>Status</b> wieder auf <i>aktiv</i> gesetzt. Wenn der RADIUS-Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit <i>inaktiv</i> ist.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Wiederholungen</b>	<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 <b>Status</b> auf <i>inaktiv</i> gesetzt. bei <b>Erreichbarkeitsprüfung</b> = <i>Aktiviert</i> versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird <b>Status</b> 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 <b>Status</b> auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf 0.</p>
<b>RADIUS-Dialout</b>	<p>Nur für <b>Authentifizierungstyp</b> = <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"> <li>• <i>Neulade-Intervall</i>: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein.</li> </ul> <p>Standardmäßig ist hier 0 eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>



## 7.6.2 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
<b>Authentifizierung für PPP-Einwahl</b>	<p>Standardmäßig wird folgende Reihenfolge bei der Authentifizierung 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"> <li>• <i>Inband</i>: Nur Inband-RADIUS-Anfragen (PAP, CHAP, MS-CHAP V1 &amp; V2) (d. h. PPP-Anfragen ohne Rufnummernidentifizierung) werden zum in <b>Server-IP-Adresse</b> definierten RADIUS-Server geschickt.</li> <li>• <i>Outband (CLID)</i>: Nur Outband-RADIUS-Anfragen (d. h. Anfragen zur Rufnummernidentifizierung) werden zum RADIUS-Server geschickt (CLID = Calling Line Identification).</li> </ul> <p>Standardmäßig ist <i>Inband</i> aktiviert, <i>Outband (CLID)</i> deaktiviert.</p>

## 7.7 Zertifikate

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

Für die Verschlüsselung benötigt der Sender den öffentlichen Schlüssel des Empfängers. Der Empfänger entschlüsselt die Daten mit seinem privaten Schlüssel. Um sicherzustellen,

dass der öffentliche Schlüssel der echte Schlüssel des Empfängers und keine Fälschung ist, wird ein Nachweis, ein sogenanntes digitales Zertifikat benötigt.

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

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

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


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

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

## 7.7.1 Zertifikatsliste

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

### 7.7.1.1 Bearbeiten

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

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
<b>Beschreibung</b>	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.
<b>Zertifikat ist ein CA-Zertifikat</b>	<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>
<b>Überprüfung anhand einer Zertifikatsperrliste (CRL)</b>	<p>Nur für <b>Zertifikat ist ein CA-Zertifikat = Wahr</b></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"> <li>• <i>Deaktiviert</i>: keine Überprüfung von CRLs.</li> <li>• <i>Immer</i>: CRLs werden grundsätzlich überprüft.</li> <li>• <i>Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist</i> (Standardwert): Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden.</li> <li>• <i>Einstellungen des übergeordneten Zertifikates benutzen</i>: Es werden die Einstellungen des übergeordneten Zertifikates verwendet, falls eines vorhanden ist. Falls nicht, wird genauso verfahren, wie unter "Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist" beschrieben.</li> </ul>
<b>Vertrauenswürdigkeit des Zertifikats erzwingen</b>	<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.

## 7.7.1.2 Zertifikatsanforderung

### Registration-Authority-Zertifikate im SCEP

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

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

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


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

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

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

#### Felder im Menü Zertifikatsanforderung

Feld	Beschreibung
<b>Zertifikatsanforderungsbeschreibung</b>	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
<b>Modus</b>	Wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen.  Zur Verfügung stehen:

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <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 <b>Details anzeigen</b> kopiert werden kann. Diese Datei muss der CA zugestellt und das erhaltene Zertifikat anschließend manuell auf Ihr Gerät importiert werden.</li> <li>• <i>SCEP</i>: Der Schlüssel wird mittels des Simple Certificate Enrollment Protocols bei einer CA beantragt.</li> </ul>
<b>Privaten Schlüssel generieren</b>	<p>Nur für <b>Modus</b> = <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>
<b>SCEP-URL</b>	<p>Nur für <b>Modus</b> = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B. <a href="http://scep.beispiel.com:8080/scep/scep.dll">http://scep.beispiel.com:8080/scep/scep.dll</a></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
<b>CA-Zertifikat</b>	<p>Nur für <b>Modus</b> = <i>SCEP</i></p> <p>Wählen Sie das CA-Zertifikat aus.</p> <ul style="list-style-type: none"> <li>• <i>-- Download --</i>: Geben Sie in <b>CA-Name</b> 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.</li> </ul>

Feld	Beschreibung
	<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 <b>Zertifikatsanforderung generieren</b> 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"> <li>• &lt;Name eines vorhandenen Zertifikats&gt;: Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, wählen Sie diese manuell aus.</li> </ul>
<b>RA-Signierungszertifikat</b>	<p>Nur für <b>Modus</b> = <i>SCEP</i></p> <p>Nur für <b>CA-Zertifikat</b> 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>
<b>RA-Verschlüsselungszertifikat</b>	<p>Nur für <b>Modus</b> = <i>SCEP</i></p> <p>Nur wenn <b>RA-Signierungszertifikat</b> nicht = <i>-- CA-Zertifikat verwenden --</i></p> <p>Wenn Sie ein eigenes Zertifikat zur Signierung der Kommunikation mit der RA verwenden, haben Sie hier die Möglichkeit, ein weiteres zur Verschlüsselung der Kommunikation auszuwählen.</p> <p>Der Standardwert ist <i>-- RA-Signierungszertifikat verwenden --</i>, d. h. es wird dasselbe Zertifikat wie zur Signierung verwendet.</p>
<b>Passwort</b>	<p>Nur für <b>Modus</b> = <i>SCEP</i></p> <p>Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.</p>

## Felder im Menü Subjektname

Feld	Beschreibung
<b>Benutzerdefiniert</b>	<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 <b>Zusammenfassend</b> ein Subjektname 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 <b>Allgemeiner Name, E-Mail, Organisationseinheit, Organisation, Ort, Staat/Provinz</b> und <b>Land</b> ein.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Zusammenfassend</b>	<p>Nur für <b>Benutzerdefiniert</b> = 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>
<b>Allgemeiner Name</b>	<p>Nur für <b>Benutzerdefiniert</b> = deaktiviert.</p> <p>Geben Sie den Namen laut CA ein.</p>
<b>E-Mail</b>	<p>Nur für <b>Benutzerdefiniert</b> = deaktiviert.</p> <p>Geben Sie die E-Mail-Adresse laut CA ein.</p>
<b>Organisationseinheit</b>	<p>Nur für <b>Benutzerdefiniert</b> = deaktiviert.</p> <p>Geben Sie die Organisationseinheit laut CA ein.</p>
<b>Organisation</b>	<p>Nur für <b>Benutzerdefiniert</b> = deaktiviert.</p> <p>Geben Sie die Organisation laut CA ein.</p>
<b>Ort</b>	<p>Nur für <b>Benutzerdefiniert</b> = deaktiviert.</p> <p>Geben Sie den Standort laut CA ein.</p>
<b>Staat/Provinz</b>	<p>Nur für <b>Benutzerdefiniert</b> = deaktiviert.</p>

Feld	Beschreibung
	Geben Sie den Staat/das Bundesland laut CA ein.
<b>Land</b>	Nur für <b>Benutzerdefiniert</b> = deaktiviert. Geben Sie das Land laut CA ein.

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

#### Felder im Menü **Subjekt-Alternativnamen**

Feld	Beschreibung
<b>#1, #2, #3</b>	<p>Definieren Sie zu jedem Eintrag den Typ des Namens und geben Sie zusätzliche Subjektnamen ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Es wird kein zusätzlicher Name eingegeben.</li> <li>• <i>IP</i>: Es wird eine IP-Adresse eingetragen.</li> <li>• <i>DNS</i>: Es wird ein DNS-Name eingetragen.</li> <li>• <i>E-Mail</i>: Es wird eine E-Mail-Adresse eingetragen.</li> <li>• <i>URI</i>: Es wird ein Uniform Resource Identifier eingetragen.</li> <li>• <i>DN</i>: Es wird ein Distinguished Name (DN) eingetragen.</li> <li>• <i>RID</i>: Es wird eine Registered Identity (RID) eingetragen.</li> </ul>

#### Feld im Menü **Optionen**

Feld	Beschreibung
<b>Autospeichermodus</b>	<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>



### 7.7.1.3 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
<b>Externer Dateiname</b>	Geben Sie den Dateipfad und -namen des Zertifikats ein, welches importiert werden soll oder wählen Sie die Datei mit <b>Durchsuchen...</b> über den Dateibrowser aus.
<b>Lokale Zertifikatsbeschreibung</b>	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
<b>Dateikodierung</b>	Wählen Sie die Art der Kodierung, so dass Ihr Gerät das Zertifikat dekodieren kann.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Auto</i> (Standardwert): Aktiviert die automatische Kodierererkennung. Falls der Zertifikat-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung.</li> <li>• <i>Base64</i></li> <li>• <i>Binär</i></li> </ul>
<b>Passwort</b>	Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort.  Tragen Sie das Passwort hier ein.

## 7.7.2 CRLs

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

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

automatisiert werden.

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

### 7.7.2.1 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
<b>Externer Dateiname</b>	Geben Sie den Dateipfad und -namen der CRL ein, welche importiert werden soll oder wählen Sie die Datei mit <b>Durchsuchen...</b> über den Dateibrowser aus.
<b>Lokale Zertifikatsbeschreibung</b>	Geben Sie eine eindeutige Bezeichnung für die CRL ein.
<b>Dateikodierung</b>	Wählen Sie die Art der Kodierung, so dass Ihr Gerät die CRL decodieren kann.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Auto</i> (Standardwert): Aktiviert die automatische Kodierererkennung. Falls der CRL-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung.</li> <li>• <i>Base64</i></li> <li>• <i>Binär</i></li> </ul>
<b>Passwort</b>	Geben Sie das zum Importieren zu verwendende Passwort ein.

### 7.7.3 Zertifikatsserver

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

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

Gerät abgefragt werden.

### 7.7.3.1 Neu

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

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

#### Felder im Menü Basisparameter

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

## 8 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.

### 8.1 Ethernet-Ports

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

Die Ethernet-Ports **ETH1** bis **ETH4** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle *en1-0* ist zugewiesen und mit **IP-Adresse** *192.168.0.251* 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.

### 8.1.1 Portkonfiguration

#### Portseparation

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

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

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

#### Felder im Menü Switch-Konfiguration

Feld	Beschreibung
<b>Switch-Port</b>	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
<b>Ethernet-Schnittstellenauswahl</b>	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 <b>1-4</b> die Schnittstelle <i>en1-0</i> , Switch Port <b>5</b> die Schnittstelle <i>en1-4</i> zugeordnet.

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

## 8.2 ISDN-Ports (PBX)

Die ISDN-Anschlüsse des Systems sind als interne ISDN-Anschlüsse zur Anschaltung verschiedener ISDN-Endgeräte (Systemtelefone, ISDN-Telefone, ...) vorgesehen.



### Hinweis

Ohne einen als Zubehör erhältlichen Adapter können beide ISDN-Anschlüsse Ihres Geräts nur als interne Anschlüsse (im NT-Modus) betrieben werden. Wenn Sie den entsprechenden Adapter angeschlossen haben, können Sie den entsprechenden Port in diesem Menü in den externen Betrieb (TE-Modus) schalten.

Beachten Sie, dass eine Umschaltung nur möglich ist, wenn Ihr Gerät im Jahr 2016 gefertigt worden ist. Sie erkennen das daran, dass auf dem Typenschild ein individuelles WLAN-Zugangspasswort aufgedruckt ist.

### 8.2.1 ISDN Intern

Im Menü **Physikalische Schnittstellen->ISDN-Ports->ISDN Intern** konfigurieren Sie die internen ISDN-Schnittstellen Ihres Systems. Die internen ISDN-Anschlüsse sind zur Anschaltung verschiedener ISDN-Endgeräte (Systemtelefone, ISDN-Telefone, ...) vorgesehen.

Zwei vordefinierte Einträge mit den Parametern **Name** = *S/U*, **Funktion** = *S0* und **Standard-MSN** = *30 (ISDN1 30)*

und *S/U*, **Funktion** = *S0* und **Standard-MSN** = *35 (ISDN2 35)*

werden angezeigt.

Interne ISDN-Anschlüsse sind immer Mehrgeräteanschlüsse.


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

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

#### Felder im Menü ISDN Intern

Feld	Beschreibung
<b>Name</b>	Zeigt die Bezeichnung der ISDN-Schnittstelle an.
<b>Funktion</b>	Zeigt die Funktion der ISDN-Schnittstelle an. Möglicher Wert: <ul style="list-style-type: none"> <li>• <i>S0</i>: Schnittstelle für ISDN-S0-Anschluss.</li> </ul>
<b>Standard-MSN</b>	Zeigt, ob für einen internen S0-Bus eine Standard-MSN zugewiesen ist.  Über eine Standard-MSN können Sie nicht konfigurierte S0-Endgeräte erreichen.  Als Standard-MSN können Sie interne Rufnummern wählen, die im Menü <b>Nummerierung-&gt;Benutzereinstellungen-&gt;Benutzer</b> konfiguriert sind und im Menü <b>Endgeräte</b> einem Endgerät zugeordnet sind.
<b>Status</b>	Zeigt den Status der Schnittstelle an.

#### 8.2.1.1 Bearbeiten

Wählen Sie die Schaltfläche , um einen Eintrag zu bearbeiten.

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

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Standard-MSN</b>	Wählen Sie die gewünschte Rufnummer. Sie können unter den Rufnummern wählen, die Sie im Menü <b>Nummerierung-&gt;Benutzereinstellungen-&gt;Benutzer-&gt;Rufnummern</b> konfiguriert haben.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Nicht konfiguriert</i></li> </ul>



Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>&lt;Rufnummer&gt;</i></li> </ul>

## 8.2.2 ISDN-Konfiguration

Ohne einen als Zubehör erhältlichen Adapter können beide ISDN-Anschlüsse Ihres Geräts nur als interne Anschlüsse (im NT-Modus) betrieben werden. Wenn Sie den entsprechenden Adapter angeschlossen haben, können Sie den entsprechenden Port in diesem Menü in den externen Betrieb (TE-Modus) schalten.

### SYNC-Anschluss Einstellungen



#### Hinweis

Diese Funktion steht nur für **be.IP 4isdn** zur Verfügung!

Hier können Sie über einen Schalter festlegen, ob Ihr Gerät als Taktgeber oder Taktnehmer arbeiten soll, wenn Sie zwei Geräte über den Sync-Anschluss verbinden, um die Anzahl der zur Verfügung stehenden ISDN-Ports zu erhöhen.

## 8.3 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.

### 8.3.1 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
<b>DSL-Chipsatz</b>	Zeigt die Kennung des eingebauten Chipsatzes an.
<b>Physikalische Verbindung</b>	<p>Zeigt den aktuellen DSL-Betriebsmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Unbekannt</i>: Der ADSL-Link ist nicht aktiv.</li> <li>• <i>ANSI T1.413</i>: ANSI T1.413</li> <li>• <i>ADSL1</i>: ADSL classic, G.DMT, ITU G.992.1</li> <li>• <i>G.lite G992.2</i>: Splitterless ADSL, ITU G.992.2</li> <li>• <i>ADSL2</i>: G.DMT.Bis, ITU G.992.3</li> <li>• <i>ADSL2 DELT</i>: ADSL2 Double Ended Line Test</li> <li>• <i>ADSL2 Plus</i>: ADSL2 Plus, ITU G.992.5</li> <li>• <i>ADSL2 Plus DELT</i>: ADSL2 Plus Double Ended Line Test</li> <li>• <i>READSL2</i>: Reach Extended ADSL2</li> <li>• <i>READSL2 DELT</i>: Reach Extended ADSL2 Double Ended Line Test.</li> <li>• <i>ADSL2 ITU-T G.992.3 Annex M</i></li> <li>• <i>ADSL2+ ITU-T G.992.5 Annex M</i></li> </ul>

#### Felder im Menü Aktuelle Leitungsgeschwindigkeit

Feld	Beschreibung
<b>Downstream</b>	<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>
<b>Upstream</b>	<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
<b>DSL-Modus</b>	<p>Wählen Sie den DSL-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Inaktiv</i>: Die ADSL-Schnittstelle ist nicht aktiv.</li> <li>• <i>ETSI T1.413</i>: ETSI T1.413</li> <li>• <i>ADSL1</i>: ADSL1 / G.DMT wird angewendet.</li> <li>• <i>Automatischer Modus (ADSL)</i> (Standardwert): Der ADSL-Modus wird dem der Gegenstelle automatisch ange-</li> </ul>

Feld	Beschreibung
	<p>passt.</p> <ul style="list-style-type: none"> <li>• <i>ADSL2</i>: ADSL2 / G.992.3 wird angewendet.</li> <li>• <i>ADSL2 Plus</i>: ADSL2 Plus / G.992.5 wird angewendet.</li> <li>• <i>VDSL</i>: VDSL2 (ITU-T G.993.2)</li> <li>• <i>VDSL/ADSL Multimodus</i> : Automatische Erkennung des DSL-Modus <i>ADSL1</i>, <i>ADSL2</i>, <i>ADSL2 Plus</i> oder <i>VDSL</i></li> </ul>
<b>Transmit Shaping</b>	<p>Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DSLAMs notwendig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (<i>Leitungsgeschwindigkeit</i>) (Standardwert): Die Datenrate in Senderichtung wird nicht reduziert.</li> <li>• <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.</li> <li>• <i>Benutzerdefiniert</i>: Die Datenrate wird reduziert auf den in <b>Maximale Upstream-Bandbreite</b> eingegebenen Wert.</li> </ul>
<b>Maximale Upstream-Bandbreite</b>	<p>Nur für <b>Transmit Shaping</b> = <i>Benutzerdefiniert</i></p> <p>Geben Sie die maximale Datenrate in Senderichtung in Bits pro Sekunde ein.</p>
<b>Rauschabstand</b>	<p>Der Signal-Rausch-Abstand (SNR) kann über den Schieberegler von 0 bis 5 dB geregelt werden. Ändern Sie den Wert nur bei DSLLeitungsproblemen.</p>

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>DSL-Leitungsprofil</b>	<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>

## 9 VoIP (PBX)

Voice over IP (VoIP) nutzt das Internet Protocol (IP) 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.

### 9.1 Einstellungen

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



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


- der Verfügbarkeit von freien Kanälen des Systems.
- der verfügbaren Bandbreite des DSL-Anschlusses.
- den konfigurierten, verfügbaren SIP-Providern.
- den eingetragenen SIP-out-Lizenzen.

#### 9.1.1 SIP-Provider


Als SIP-Provider bezeichnet man einen Internet Provider, der einen VoIP-Dienst anbietet und dafür das Session Initiation Protocol (SIP) nutzt. Wenn Sie sich bei einem SIP-Provider anmelden, können Sie über das Internet telefonieren.

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

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

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

### 9.1.1.1 Bearbeiten oder Neu

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

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

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Beschreibung</b>	Sie können eine Bezeichnung für den SIP-Provider eingeben. Möglich ist eine 20-stellige alphanumerische Zeichenfolge.
<b>Provider-Status</b>	Wählen Sie aus, ob dieser Provider-Eintrag aktiv sein soll ( <i>Aktiv</i> , Standardwert) oder nicht ( <i>Inaktiv</i> ).
<b>Anschlussart</b>	Wählen Sie aus, welche Art von VoIP-Rufnummer Sie konfigurieren möchten.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Einzelrufnummer</i> (Standardwert): Geben Sie einzelne VoIP-Rufnummern ein.</li> <li>• <i>Durchwahl</i>: Geben Sie eine Basisnummer in Verbindung mit einem Rufnummernblock an.</li> </ul>
<b>Authentifizierungs-ID</b>	Geben Sie die Authentifizierungs-ID Ihres Providers ein. Möglich ist eine 64-stellige alphanumerische Zeichenfolge.
<b>Passwort</b>	Sie können an dieser Stelle ein Passwort vergeben. Möglich ist eine 64-stellige alphanumerische Zeichenfolge.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein, den Sie von Ihrem Provider erhalten haben. Möglich ist eine 64-stellige alphanumerische Zeichenfolge.
<b>Domäne / Realm</b>	Tragen Sie einen weiteren Domänennamen oder eine weitere IP-Adresse des SIP-Proxy-Servers ein.  Wenn Sie keine Angaben machen, wird der Eintrag im Feld <b>Registrar</b> verwendet.  Beachten Sie: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dieser explizit vom Provider vorgegeben wird.

### Felder im Menü **Einstellungen für Gehende Rufnummer**

Feld	Beschreibung
<b>Gehende Rufnummer</b>	<p>Wählen Sie die gewünschte Signalisierung für Rufe nach außen aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (Standardwert)</li> <li>• <i>Globale Rufnummer für CLIP-No-Screening</i></li> <li>• <i>Individuelle Rufnummer für CLIP-No-Screening</i></li> <li>• <i>Feste DDI nach Extern</i> (Nur für <b>Anschlussart = Durchwahl</b>)</li> </ul>
<b>Globale Rufnummer für CLIP-No-Screening</b>	<p>Nur für <b>Gehende Rufnummer</b> <i>Globale Rufnummer für CLIP-No-Screening</i></p> <p>Geben Sie die Rufnummer ein, die bei allen Verbindungen nach extern beim Angerufenen angezeigt werden soll.</p> <p>Diese Rufnummer wird nicht überprüft.</p>
<b>Rufnummer des entfernten Gesprächspartners anzeigen</b>	<p>Nur für <b>Gehende Rufnummer</b> = <i>Globale Rufnummer für CLIP-No-Screening</i> und <i>Individuelle Rufnummer für CLIP-No-Screening</i></p> <p>Sie können die Rufnummer eines externen Gesprächspartners anzeigen lassen, sofern diese signalisiert wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Feste Rufnummer für ausgehende Gespräche anzeigen</b>	<p>Nur für <b>Gehende Rufnummer</b> = <i>Feste DDI nach Extern</i></p> <p>Geben Sie die Rufnummer ein, die bei allen Verbindungen nach extern beim Angerufenen angezeigt werden soll.</p>

### Felder im Menü **Registrar**

Feld	Beschreibung
<b>Registrar</b>	<p>Geben Sie den DNS-Namen oder die IP-Adresse des SIP-Servers an. Möglich ist eine 26-stellige alphanumerische Zeichenfolge.</p>

Feld	Beschreibung
<b>Port Registrar</b>	Geben Sie die Nummer des Ports ein, der für die Verbindung zum Server benutzt werden soll. Standardmäßig ist der Wert <i>5060</i> vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.
<b>Transportprotokoll</b>	<p>Wählen Sie das Transportprotokoll für die Verbindung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>UDP</i> (Standardwert)</li> <li>• <i>TCP</i></li> <li>• <i>TLS</i></li> <li>• <i>Automatisch</i> - Mit dieser Einstellung unterstützt Ihr Gerät eine automatische Aushandlung des Protokolls mit den Servern Ihres Anbieters. Damit diese Einstellung funktioniert, muss diese Aushandlung vom Anbieter ebenfalls unterstützt werden.</li> </ul>

#### Felder im Menü STUN

Feld	Beschreibung
<b>STUN-Server</b>	<p>Geben Sie den Namen oder die IP-Adresse des STUN-Servers ein.</p> <p>STUN = Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)</p> <p>Ein STUN-Server wird benötigt, um VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Internet zu ermöglichen. Hierbei wird die aktuelle öffentliche IP-Adresse des Anschlusses ermittelt und für eine genaue Adressierung von außen verwendet.</p> <p>Maximale Zeichenzahl: 32.</p>
<b>Port-STUN-Server</b>	<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 Timer

Feld	Beschreibung
<b>Registrierungstimer</b>	Geben Sie hier die Zeitdauer in Sekunden ein, vor deren Ablauf

Feld	Beschreibung
	sich der SIP-Client erneut registrieren muss, damit die Verbindung nicht automatisch getrennt wird.  Standardmäßig ist der Wert <i>600</i> vorgegeben.

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>Proxy</b>	Geben Sie den DNS-Namen oder die IP-Adresse des SIP-Servers an. Möglich ist eine 26-stellige alphanumerische Zeichenfolge.
<b>Port Proxy</b>	Geben Sie Nummer des Ports ein, der für die Verbindung zum Proxy benutzt werden soll. Standardmäßig ist der Wert <i>5060</i> vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.
<b>Transportprotokoll</b>	Wählen Sie das Transportprotokoll für die Verbindung aus.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>UDP</i> (Standardwert)</li> <li>• <i>TCP</i></li> <li>• <i>TLS</i></li> <li>• <i>Automatisch</i> - Mit dieser Einstellung unterstützt Ihr Gerät eine automatische Aushandlung des Protokolls mit den Servern Ihres Anbieters. Damit diese Einstellung funktioniert, muss diese Aushandlung vom Anbieter ebenfalls unterstützt werden.</li> </ul>

#### Felder im Menü **Weitere Einstellungen**

Feld	Beschreibung
<b>From Domain</b>	Geben Sie die „From Domain“ Ihres SIP-Providers ein. Diese wird nach dem @ als Absendeinformation im SIP-Header der SIP-Datenpakete verwendet.
<b>Anzahl der zulässigen gleichzeitigen Gespräche</b>	Wählen Sie die maximale Anzahl von Gesprächen aus, die gleichzeitig möglich sein sollten. Beachten Sie hier auch die Einstellungen des Bandbreitenmanagements.



Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>International</i> (Standardwert): Es sind unbegrenzt gleichzeitige Gespräche möglich.</li> <li>• 1</li> <li>• 2</li> <li>• 3</li> <li>• 4</li> <li>• 5</li> <li>• 10</li> </ul>
<b>Standort</b>	<p>Wählen Sie den Standort des SIP-Servers aus. Standorte werden im Menü <b>VoIP-&gt;Einstellungen-&gt;Standorte</b> definiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Alle Standorte</i> (Standardwert): Der Server wird an keinem definierten Standort betrieben.</li> <li>• <i>&lt;Standort-Name&gt;</i></li> </ul>
<b>Codec-Profil</b>	<p>Wählen Sie das Codec-Profil für diesen SIP-Server aus. Codec-Profile werden im Menü <b>VoIP-&gt;Einstellungen-&gt;Codec-Profil</b> definiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>System-Default</i> (Standardwert): Der Server wird mit einem im System vordefinierten Codec-Profil betrieben.</li> <li>• <i>&lt;Codec-Profil-Name&gt;</i></li> </ul>
<b>Wahlendeüberwachungstimer</b>	<p>Wählen Sie die Zeit (nach Wahl der letzten Ziffer einer Rufnummer) in Sekunden aus, nach der das System mit der Wahl nach extern beginnt. Standardwert ist 5.</p>
<b>Halten im System</b>	<p>Die netzwerkzentralen Funktionen Halten, Makeln, 3er Konferenz und Anklopfen können aktiviert werden, indem Sie die Schaltfläche Halten im System deaktivieren. In dieser Einstellung werden diese Leistungsmerkmale nicht mehr im PBX System sondern im öffentlichen Netzwerk ausgeführt. Voraussetzung für die Nutzung dieser Funktionen ist ein entsprechender Vertrag zwischen dem Provider und dem Kunden, der eine</p>

Feld	Beschreibung
	<p>Bandbreitenbegrenzung (Anzahl der gleichzeitig nutzbaren Sprachkanäle) vorsieht.</p> <p>Wenn ein SIP-Provider, z. B. die Deutsche Telekom, mehrere SIP-Accounts / Nummern über einen einzigen Zugang bereitstellt, sollte bei jedem SIP-Account die Option ausgeschaltet sein! Dies ist erforderlich, um die Bandbreitenreservierung über verschiedene Rufnummern über einen Netzwerkzugriff zu unterstützen.</p> <p>Wenn der externe Anruf gehalten wird, wird kein MoH von der TK-Anlage wiedergegeben, stattdessen stellt das öffentliche Netzwerk MoH oder eine Ansage an die entfernte gehaltene Partei bereit.</p>
<b>Anrufweitschaltung extern (SIP 302)</b>	<p>Wählen Sie aus, ob eine Anrufumleitung extern beim SIP-Provider durchgeführt wird. Der Anrufer wird mittels SIP-Status-Code 302 weitergeschaltet.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Internationale Rufnummer erzeugen</b>	<p>Wenn Sie diese Funktion aktivieren und unter <b>Globale Einstellungen</b> die <b>Ländereinstellung</b> (für Deutschland <sup>49</sup>) eingetragen haben, wird automatisch bei einer mit Vorwahl gewählten Rufnummer die 0049 vor der Rufnummer erzeugt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Nationale Rufnummer erzeugen</b>	<p>Wenn Sie diese Funktion einschalten und unter <b>Globale Einstellungen</b> den <b>Nationaler Präfix / Ortsnetzkenzahl</b> (für z. B. Hamburg <sup>40</sup>) eingetragen haben, wird automatisch die Vorwahl 040 vor der gewählten Rufnummer erzeugt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Nummernunterdrückung deaktivieren</b>	<p>Wenn Sie diese Funktion aktivieren, wird die Rufnummer immer mitgesendet unabhängig davon, ob Sie bei einem Teilnehmer <b>A-Rufnummer unterdrücken (CLIR)</b> ein- oder ausgeschaltet</p>

Feld	Beschreibung
	<p>haben.</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 nicht aktiv ist, haben Sie zusätzliche Wahlmöglichkeiten.</p> <p>Um sicherzustellen, dass Ihr System bei SIP-Verbindungen anonyme Anrufe weiterleiten kann, können Sie festlegen, in welchen Teil der SIP-Header-Informationen der String "Anonymus Call" abgelegt wird. Sie können diese Information mehrmals ablegen. Für die meisten Provider können Sie die Voreinstellung <i>Privacy ID = Aktiviert</i> belassen. Für den Provider 1 &amp; 1 müssen Sie zusätzlich <i>Privacy Header</i> aktivieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Anzeige</i></li> <li>• <i>Benutzer</i></li> <li>• <i>Domäne</i></li> <li>• <i>Privacy Header</i></li> <li>• <i>Privacy User</i></li> <li>• <i>Privacy ID</i></li> </ul>
<p><b>SIP-Header-Feld: FROM Display</b></p>	<p>Die Absender-ID wird im SIP Header im Feld "Display" übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Die Absender-ID wird nicht übertragen.</li> <li>• <i>Benutzername</i>: Der vom Benutzer konfigurierter Benutzername wird angezeigt.</li> <li>• <i>Anruferadresse</i>: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird angezeigt.</li> <li>• <i>Abrechnungsnummer</i>: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.</li> </ul>

Feld	Beschreibung
<b>SIP-Header-Feld: FROM User</b>	<p>Die Absender-ID wird im SIP Header im Feld "User" übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Benutzername</i> (Standardwert): Der vom Benutzer konfigurierter Benutzername wird angezeigt.</li> <li>• <i>Anruferadresse</i>: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird angezeigt.</li> <li>• <i>Abrechnungsnummer</i>: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.</li> </ul>
<b>SIP-Header-Feld: P-Preferred</b>	<p>Der SIP Header wird durch das sogenannte "p-preferred-identity" Feld erweitert, um dort die Absender-ID zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Die Absender-ID wird nicht übertragen.</li> <li>• <i>Benutzername</i>: Der vom Benutzer konfigurierter Benutzername wird angezeigt.</li> <li>• <i>Anruferadresse</i>: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird angezeigt.</li> <li>• <i>Abrechnungsnummer</i>: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.</li> </ul>
<b>SIP-Header-Feld: P-Asserted</b>	<p>Der SIP Header wird durch das sogenannte "p-asserted-identity" Feld erweitert, um dort die Absender-ID zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Die Absender-ID wird nicht übertragen.</li> <li>• <i>Benutzername</i>: Der vom Benutzer konfigurierter Benutzername wird angezeigt.</li> <li>• <i>Anruferadresse</i>: Die vom Benutzer konfigurierte Rufnummer, die dem Angerufenen angezeigt werden soll, wird ange-</li> </ul>

Feld	Beschreibung
	<p>zeigt.</p> <ul style="list-style-type: none"> <li>• <i>Abrechnungsnummer</i>: Die tatsächliche Rufnummer, von der aus der Ruf aufgebaut wird (z. B. zur Abrechnung des Rufs), wird angezeigt.</li> </ul>
<b>Ersetzen des internationalen Präfix durch "+"</b>	<p>Wählen Sie aus, ob bei internationalen Rufnummern der Präfix (z. B. 00) durch + ersetzt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Anmeldung eines Proxys erlauben</b>	<p>Wählen Sie aus, ob eine weitere TK-Anlage sich bei Ihrem System registrieren kann. Dadurch können mehrere TK-Systeme miteinander gekoppelt werden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>SIP-Bindungen nach Neustart löschen</b>	<p>Sollte z. B. nach der Registrierung bei einem Provider ein Reset des Systems erfolgen oder ein Netzausfall eintreten, kann je nach Provider eine weitere Registrierung nicht mehr möglich sein. Durch Einschalten dieses Leistungsmerkmals, wird eine erneute Registrierung nach Neustart ermöglicht.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Vorgeschaltetes Gerät mit NAT</b>	<p>Wenn Sie diese Funktion aktivieren, können Sie ein vorgeschaltetes Gerät mit NAT nutzen und trotzdem mit VoIP telefonieren. Ohne diese Funktion könnten Sie bei Nutzung eines vorgeschalteten Geräts mit NAT über VoIP nicht angerufen werden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Early-Media-Unterstützung</b>	<p>Wählen Sie aus, ob Sie den Austausch von Sprach- oder Audiodaten erlauben wollen, bevor ein Empfänger einen Anruf annimmt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
<b>Art der Registrierung</b>	<p>Wählen Sie, wie die Registrierung und Authentifizierung bei einem Provider ausgeführt wird bzw. ob sie entfallen kann. Im letzten Fall werden die relevanten Daten an eine bestimmte IP-Adresse geschickt, die den Verbindungspartnern bereits bekannt ist. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP.</p> <p>Ist eine Registrierung erforderlich kann sie auf zwei Weisen erfolgen:</p> <ul style="list-style-type: none"> <li>• <i>Einzeln</i>: Bei dieser Option wird jeweils eine MSN beim SIP-Provider registriert. Dieser stellt die Kontaktinformationen für Anrufer zur Verfügung.</li> <li>• <i>Bulk (BNC)</i>: Bei dieser Option wird ein SIP DDI (SIP Trunk) beim Provider registriert, d. h. es werden mehrere Rufnummern unter einer Adresse registriert.</li> </ul>
<b>T.38 FAX Unterstützung</b>	<p>Wählen Sie, ob Sie FAX-Dokumente per Voice over IP mit dem Standard T.38 übertragen wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Wenn die Funktion deaktiviert ist, werden Fax-Dokumente mit G.711 übertragen.</p>
<b>Ersetzen des Präfix der eingehenden Nummer</b>	Soll bei kommenden Anrufen die Rufnummer verändert im System weitergegeben werden, geben Sie in das erste Eingabefeld die Zahlenfolge der kommenden Rufnummer ein, die durch die im zweiten Eingabefeld eingetragene Zahlenfolge ersetzt werden soll.
<b>SIP Update senden</b>	Mit dieser Funktion können Sie sicherstellen, dass bei einem weitergeleiteten Anruf, die Nummer des neuen Gesprächspartners beim ursprünglichen Anrufer angezeigt wird.

**Hinweis**

Beachten Sie, dass diese Funktion nicht von allen Providern unterstützt wird.

Feld	Beschreibung
	Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion nicht aktiv.
<b>Anfrage-URI</b>	In einigen Anwendungsfällen (vor allem bei DDI-Verbindungen) muss die Zieladresse eines SIP-Rufs aus dem Request-URI des SIP Invites gelesen werden muss. Indem Sie diese Option aktivieren, wird die Adresse bevorzugt aus diesem Feld des Invites gelesen. Standardmäßig ist die Funktion nicht aktiv.
<b>Quell-IP-Adresse überprüfen</b>	Ihrem Gerät werden vom SIP-Provider als Antwort auf eine DNS-SRV-Anfrage die Adressen gültiger Registrierungsserver übermittelt. Wenn Sie diese Option aktivieren, wird bei jedem SIP Invite überprüft, ob er von einer der gültigen Adressen stammt. Ist das nicht der Fall, wird die Anfrage ignoriert. Standardmäßig ist die Funktion nicht aktiv.
<b>Überprüfung des TLS-Zertifikats</b>	Nur für DDI- / SIP-Trunk-Verbindungen. Wenn eine Verbindung über TLS (Transport Layer Security) verschlüsselt werden soll, wird das Serverzertifikat der Gegenstelle einer Gültigkeitsprüfung unterzogen, wenn diese Option aktiv ist. Standardmäßig ist die Funktion nicht aktiv.

#### Felder im Menü **Codec-Einstellungen**

Feld	Beschreibung
<b>Codec-Profil</b>	Wählen Sie das Codec-Profil für diesen SIP-Server aus. Codec-Profile werden im Menü <b>VoIP-&gt;Einstellungen-&gt;Codec-Profile</b> definiert.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>System-Default</i> (Standardwert): Der Server wird mit einem im System vordefinierten Codec-Profil betrieben.</li> <li>• <i>&lt;Codec-Profil-Name&gt;</i></li> </ul>
<b>Video</b>	Wählen Sie, ob Sie in Rufen von IP- zu IP-Telefonen die Übertragung von Videodaten unterstützen wollen. Nur, wenn beide Teilnehmer die Funktion unterstützen, kann sie zwischen ihnen ausgehandelt werden.
<b>SRTP</b>	Wählen Sie aus, ob Sie Rufe über diesen SIP-Provider zulassen wollen, die mittels SRTP (Secure Real-Time Transport Protocol) abgesichert sind.

Feld	Beschreibung
<b>MediaSec</b>	<p><i>MediaSec</i>: MediaSec handelt die Absicherung der RTP-Daten mit den SIP-Servern aus.</p> <p>Für eine reibungslose Unterstützung muss eine automatische Aushandlung des Transportprotokolls erfolgen. Bei fest eingestellten Transportprotokollen (UDP und TCP) kann es zu Problemen bei der Registrierung kommen. Darüber hinaus muss die Verwendung von SRTP erlaubt sein. Ihr VoIP-Anbieter muss MediaSec unterstützen.</p>

### 9.1.2 Standorte

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

Mit Hilfe der **Standorte** legen Sie fest, aus welchem IP-Adress-Bereich oder über welche LAN-Schnittstellen sich SIP-Clients registrieren dürfen. Ab Systemsoftware Release 10.1.5 Patch 5 gilt zusätzlich für VoIP-Provider: der Standort legt die WAN-Schnittstelle fest, über die sich ein SIP Account registrieren wird.

Zur Verwendung des Bandbreitenmanagements können einzelne Standorte eingerichtet werden. Ein Standort wird anhand seiner festen IP-Adresse bzw. DynDNS-Adresse oder mittels der Schnittstelle identifiziert, an der das Gerät angeschlossen ist. 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
<b>Standardverhalten</b>	<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"> <li>• <i>Registrierung nur in privaten Netzwerken</i> (Standardwert): Der VoIP-Teilnehmer wird nur registriert, wenn er sich innerhalb des privaten Netzwerks be-</li> </ul>



Feld	Beschreibung
	<p>findet.</p> <ul style="list-style-type: none"> <li>• <i>Nicht erlaubt</i>: Der VoIP-Teilnehmer wird nie registriert.</li> <li>• <i>Uneingeschränkte Registrierung</i>: Der VoIP-Teilnehmer wird immer registriert.</li> </ul>

### 9.1.2.1 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
<b>Beschreibung</b>	Geben Sie die Beschreibung des Eintrags ein.
<b>Beinhalteter Standort (Parent)</b>	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.
<b>Typ</b>	<p>Wählen Sie aus, ob der Standort mittels IP-Adressen/DNS-Namen oder Schnittstellen definiert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Adressen</i> (Standardwert): Der SIP-Standort wird über IP-Adressen bzw. DNS-Namen definiert.</li> <li>• <i>Schnittstellen</i>: Der SIP-Standort wird über die verfügbaren Schnittstellen definiert.</li> </ul>
<b>Adressen</b>	<p>Nur für <b>Typ</b> = <i>Adressen</i></p> <p>Geben Sie die IP-Adressen der Geräte an den SIP-Standorten ein.</p> <p>Klicken Sie auf <b>Hinzufügen</b> um neue Adressen zu konfigurieren.</p> <p>Geben Sie unter <b>IP-Adresse/DNS-Name</b> die gewünschte IP-Adresse bzw. den DNS-Namen ein.</p>

Feld	Beschreibung
	Geben Sie ebenfalls die erforderliche <b>Netzmaske</b> ein.
<b>Schnittstellen</b>	<p>Nur für <b>Typ</b> = <i>Schnittstellen</i></p> <p>Geben Sie die Schnittstellen an, an denen die Geräte eines SIP-Standorts angeschlossen sind.</p> <p>Klicken Sie auf <b>Hinzufügen</b>, um neue Schnittstelle auszuwählen.</p> <p>Wählen Sie unter <b>Schnittstelle</b> die gewünschte Schnittstelle aus.</p>
<b>Bandbreitenbegrenzung Upstream</b>	<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>
<b>Maximale Upstream-Bandbreite</b>	Geben Sie die maximale Datenrate in Senderichtung in kBits pro Sekunde ein.
<b>Bandbreitenbegrenzung Downstream</b>	<p>Legen Sie fest, ob die Downstream-Bandbreite begrenzt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Bandbreite reduziert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Maximale Downstream-Bandbreite</b>	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
<b>DSCP-Einstellungen für RTP-Daten</b>	<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"> <li>• <i>DSCP-Binärwert</i> (Standardwert): Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priori-</li> </ul>

Feld	Beschreibung
	<p>tät der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). Der vorkonfigurierte Wert ist <code>101110</code></p> <ul style="list-style-type: none"> <li>• <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</li> <li>• <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format).</li> <li>• <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111.</li> <li>• <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63.</li> <li>• <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.</li> </ul>

### 9.1.3 Codec-Profile


Als Codec bezeichnet man ein Verfahren, das analoge Daten wie zum Beispiel Audio- oder Videosignale digitalisiert, um sie zum Beispiel über das Internet übertragen zu können, oder im Gegenzug digitale Mediendaten dekodiert, um sie abspielen zu können.

Ein Codec-Profil ist eine Liste, die mehrere Codecs enthält und mit einem Namen versehen ist. Die Reihenfolge der möglichen Anwendung der Codecs ist durch die Codec-Reihenfolge festgelegt. Wenn der erste Codec in der Liste nicht verwendet werden kann, z. B. weil die Gegenstelle ihn nicht unterstützt, kommt der zweite Codec zum Einsatz usw.

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

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

#### 9.1.3.1 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->Codec-Profile->Neu** besteht aus folgenden Feldern:

## Felder im Menü Basisparameter

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie eine Beschreibung für den Eintrag ein.
<b>Codec-Reihenfolge</b>	<p>Wählen Sie die Reihenfolge der Codecs, wie sie vom System zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht, den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich.</li> <li>• <i>Qualität</i>: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich.</li> <li>• <i>Geringe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich.</li> <li>• <i>Hohe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.</li> </ul>
<b>G.711 uLaw</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>ISDN-Codec nach US-Kennlinie.</p> <p>G.711 uLaw erfasst den Frequenzbereich von 300 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,4. Dieser Audio-Codec verwendet das <math>\mu</math>law-Quantisierungsverfahren.</p>
<b>G.711 aLaw</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>ISDN-Codec nach EU-Kennlinie</p> <p>G.711 aLaw erfasst den Frequenzbereich von 300 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,4. Dieser Audio-Codec verwendet das alaw-Quantisierungsverfahren.</p>
<b>G.722</b>	Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i>

Feld	Beschreibung
	G.722 erfasst den Frequenzbereich von 50 Hz bis 7000 Hz mit einer Abtastrate von 16 kHz und erreicht bei einer Datenübertragungsrate von 64 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,5.
<b>G.729</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>G.729 erfasst den Frequenzbereich von 300 Hz bis 2400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 8 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,9.</p>
<b>G.726 (16 Kbit/s)</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>G.726 (16 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 16 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,7.</p>
<b>G.726 (24 Kbit/s)</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>G.726 (24 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 24 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,8.</p>
<b>G.726 (32 Kbit/s)</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>G.726 (32 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 32 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 3,9.</p>
<b>G.726 (40 Kbit/s)</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>G.726 (40 Kbit/s) erfasst den Frequenzbereich von 200 Hz bis 3400 Hz mit einer Abtastrate von 8 kHz und erreicht bei einer Datenübertragungsrate von 40 kbit/s einen MOS-Wert – ein Maß für die Sprachqualität – von 4,2.</p>
<b>DTMF</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>Wählen Sie aus, ob der Codec DTMF Outband verwendet werden soll. Zuerst wird versucht RFC 2833 zu verwenden. Wenn</p>

Feld	Beschreibung
	<p>die Gegenstelle diesen Standard nicht beherrscht, wird SIP Info verwendet.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>G.726 Codec-Einstellungen</b>	<p>Nur für <b>Codec-Reihenfolge</b> nicht <i>Standard</i></p> <p>Wählen Sie das Kodierverfahren für den G.726 Codec aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>I.366</i></li> <li>• <i>RFC3551 / X.420</i></li> </ul>

### 9.1.4 Optionen

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

Das Menü besteht aus folgenden Feldern:


#### Felder im Menü Grundeinstellungen

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

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>DSCP-Einstellungen für SIP-Daten</b>	Wählen Sie die Art des Dienstes für SIP-Daten aus (TOS, Type of Service).

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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>110000</i>.</li> <li>• <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</li> <li>• <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format).</li> <li>• <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111.</li> <li>• <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63.</li> <li>• <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.</li> </ul>
<p><b>SIP Port</b></p>	<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> <div data-bbox="541 1065 1315 1253" style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Hinweis</b></p> <p>Falls Sie den Port im laufenden Betrieb ändern, wird die Änderung erst nach dem nächsten Neustart der Anlage wirksam.</p> </div>
<p><b>Client Subscription Timer</b></p>	<p>Geben Sie einen Wert für die Zeitdauer in Sekunden ein, vor deren Ablauf der SIP-Client alle seine konfigurierten BLF-Tasten beim Gateway erneut anmelden muss, damit die Statusinformationen nicht verloren gehen.</p> <p>Standardmäßig ist der Wert <i>300</i> vorgegeben.</p> <p>Meist können Sie den voreingestellten Wert belassen. Bei vielen konfigurierten Tasten kann es empfehlenswert sein, den Wert zu erhöhen.</p>

**Felder im Menü SIP über TLS**

Feld	Beschreibung
<b>Lokales Zertifikat</b>	Für SIP über TLS können Sie ein Zertifikat wählen.  Standardmäßig ist das interne Zertifikat des Geräts voreingestellt.



## 10 Anrufkontrolle

In der Anrufkontrolle werden die Funktionen für externe Anrufe, externe Gespräche und die Wahlregeln für externe Gespräche festgelegt.

### 10.1 Ausgehende Dienste

Im Menü **Anrufkontrolle->Ausgehende Dienste** können Sie die Leistungsmerkmale **Anrufweitschaltung (AWS)** und **Wahlkontrolle** und konfigurieren.

#### 10.1.1 Anrufweitschaltung (AWS)

Im Menü **Anrufkontrolle->Ausgehende Dienste->Anrufweitschaltung (AWS)** konfigurieren Sie Anrufweitschaltungen von externen Anrufen für einen internen Teilnehmer.

Sie sind vorübergehend nicht in Ihrem Büro und möchten dennoch keinen Anruf verpassen. Mit einer Anrufweitschaltung zu einer anderen Rufnummer, z. B. zu Ihrem Handy, können Sie Ihre Anrufe auch annehmen, wenn Sie nicht am Platz sind. Sie können Anrufe für Ihre Rufnummer zu einer beliebigen Rufnummer weitschalten. Die Weitschaltung kann *Sofort*, *Bei Nichtmelden* oder *Bei Besetzt* erfolgen. Anrufweitschaltungen *Bei Nichtmelden* und *Bei Besetzt* können gleichzeitig bestehen. Sind Sie z. B. nicht in der Nähe Ihres Telefons, wird der Anruf nach einer kurzen Zeit zu einer anderen Rufnummer (z. B. zu Ihrem Handy) weitergeschaltet. Führen Sie bereits ein Telefongespräch an Ihrem Arbeitsplatz, erhalten weitere Anrufer möglicherweise "besetzt". Diese Anrufer können Sie mit einer Anrufweitschaltung bei besetzt z. B. zu einem Kollegen oder dem Sekretariat weitschalten.

Jeder interne Teilnehmer des Systems kann seine Anrufe zu einer anderen Rufnummer weitschalten. Die Anrufweitschaltung kann dabei zu internen Teilnehmer-Rufnummern, internen Team-Rufnummern oder externen Rufnummern erfolgen. Bei der Eingabe der Rufnummer, zu der die Anrufe weitergeschaltet werden sollen, prüft das System automatisch, ob es sich um eine interne oder um eine externe Rufnummer handelt.

Bei einem Team kann die Anrufweitschaltung für einen Teilnehmer im Team eingerichtet sein. Bei den anderen Teilnehmern im Team wird dieser Anruf weiterhin signalisiert. Die Anrufweitschaltung zu einem internen oder externen Teilnehmer wird dabei im System ausgeführt.

Die Anrufweitschaltung zu einer internen Rufnummer wird im System ausgeführt. Soll ein interner Anruf zu einer externen Rufnummer weitergeleitet werden, wird die Weiterleitung ebenfalls im System ausgeführt. Die Verbindung wird dabei über das Bündel aufgebaut, welches für den einrichtenden Teilnehmer freigegeben ist. Erfolgt die Anrufweitschaltung

über einen ISDN-Anschluss, bleibt ein B-Kanal belegt, bei einer Weiterschaltung von extern nach extern bleiben beide B-Kanäle belegt. Für die Anrufweiterschaltung eines externen Anrufes zu einer externen Rufnummer gibt es zwei Möglichkeiten:


- Anrufweiterschaltung in der Vermittlungsstelle: Die Anrufweiterschaltung wird in der Vermittlungsstelle ausgeführt, wenn bei einem externen Anruf nur ein interner Teilnehmer in der Anrufverteilung eingetragen ist. Für eine Anrufweiterschaltung in der Vermittlungsstelle müssen für die betreffenden ISDN-Anschlüsse beim Netzbetreiber die Leistungsmerkmale Call Deflection (Mehrgeräteanschluss) oder Partial Rerouting (Anlagenanschluss) aktiviert sein.
- Anrufweiterschaltung im System: Die Anrufweiterschaltung wird im System ausgeführt, wenn für die betreffenden ISDN-Anschlüsse die notwendigen Leistungsmerkmale für eine Anrufweiterschaltung in der Vermittlungsstelle nicht verfügbar sind. Werden bei einem externen Anruf mehrere Telefone (z. B. ein Team) gerufen, von denen einzelne eine Anrufweiterschaltung eingerichtet haben, wird die entsprechende Anrufweiterschaltung im System ausgeführt. Die externe Verbindung wird dabei über den B-Kanal eines Bündels aufgebaut, welches für den einrichtenden Teilnehmer freigegeben ist. Für die Dauer einer aktiven Anrufweiterschaltung bleibt dieser B-Kanal belegt.



#### Hinweis

Ist das System an das externe ISDN angeschlossen (sofern von Ihrem Gerät unterstützt), versucht das System bei Extern-zu-extern-Verbindungen grundsätzlich die Anrufweiterschaltung über die Vermittlungsstelle einzuleiten. Für Teams kann manuell in der Konfiguration festgelegt werden, ob die Anrufweiterschaltung über die Vermittlungsstelle oder das System erfolgen soll. Besitzt das System keine ISDN-Anschlüsse oder ist Call Deflection (Mehrgeräteanschluss) oder Partial Rerouting (Anlagenanschluss) nicht beim Netzbetreiber beauftragt, erfolgt die Anrufweiterschaltung nur im System.

#### 10.1.1.1 Bearbeiten oder Neu

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

Das Menü **Anrufkontrolle->Ausgehende Dienste->Anrufweiterschaltung (AWS) ->Neu** besteht aus folgenden Feldern:

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Interne Rufnummer</b>	Wählen Sie die interne Rufnummer aus, für die kommende An-

Feld	Beschreibung
	rufe weitergeschaltet werden sollen.
<b>Art der Anrufweiter-schaltung</b>	<p>Wählen Sie aus, wann kommende Anrufe auf die angegebene interne Rufnummer weitergeschaltet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Sofort</i></li> <li>• <i>Bei Besetzt</i></li> <li>• <i>Bei Nichtmelden</i> (Standardwert)</li> <li>• <i>Bei Besetzt / Bei Nichtmelden</i></li> </ul>
<b>Zielrufnummer "Bei Nichtmelden"</b>	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei Nichtmelden weitergeschaltet werden sollen.
<b>Zielrufnummer "Bei besetzt"</b>	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei besetzt weitergeschaltet werden sollen.
<b>Zielrufnummer "Sofort"</b>	Geben Sie die Rufnummer ein, auf die kommende Anrufe sofort weitergeschaltet werden sollen.

## 10.1.2 Wahlkontrolle

Im Menü **Anrufkontrolle->Ausgehende Dienste->Wahlkontrolle** sperren Sie bestimmte Rufnummern/Teilrufnummern oder Sie geben diese frei.

Sie möchten die Wahl bestimmter Rufnummern im System verhindern, z. B. die Rufnummern von teuren Mehrwertdiensten. Tragen Sie diese Rufnummern oder Teilrufnummern in die Liste der gesperrten Rufnummern der Wahlkontrolle ein. Alle Teilnehmer, die der Wahlkontrolle unterliegen, können diese Rufnummern nicht wählen. Sollten Sie bestimmte Rufnummern aus einem gesperrten Bereich dennoch benötigen, können Sie diese über die Liste der freigegebenen Rufnummern der Wahlkontrolle freigeben.

Mit der Liste der gesperrten Rufnummern können Sie bestimmte Rufnummern oder Vorwahlen sperren. Mit der Liste der freigegebenen Rufnummern können Sie gesperrte Rufnummern oder Vorwahlen freigeben. Ist eine Rufnummer, die als freigegebene Rufnummer eingetragen ist, länger als eine Rufnummer, die als gesperrte Rufnummer eingetragen ist, kann diese Rufnummer gewählt werden. Wenn Sie eine Rufnummer wählen, wird die Wahl nach der gesperrten Ziffer abgebrochen und Sie hören den Besetztton. In den Benutzereinstellungen können Sie jeden Benutzer einzeln der Wahlkontrolle zuordnen.

Beispiel: Gesperrte Rufnummer 01, alle externen Rufnummern die mit 01 beginnen sind

gesperrt. Freigegebene Rufnummer 012345, die Wahl kann erfolgen. Alle externen Rufnummern, die mit 012345 beginnen können gewählt werden. Sind zwei gleiche Rufnummern (gleiche Ziffernfolge und gleiche Anzahl von Ziffern, z. B. 01234 und 01234) sowohl in der Liste der freigegebenen Rufnummern als auch die der gesperrten Rufnummern eingetragen, wird die Wahl der Rufnummer verhindert.




### Hinweis

Über die Liste der freigegebenen Rufnummern werden Teilnehmer, die halbamtsberechtigt sind (die von extern angerufen werden können aber selbstständig nicht nach extern telefonieren können) oder nicht amtsberechtigt sind (keine externe Wahlberechtigung besitzen), zur externen Wahl der freigegebenen Rufnummer berechtigt.

Beachten Sie, dass die Ortsnetzkennzahl in der Konfigurierung eingetragen ist, sonst kann die gesperrte Rufnummer im Ortsnetz durch die Vorwahl der Ortsnetzkennzahl umgangen werden.

### 10.1.2.1 Bearbeiten oder Neu

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

Das Menü **Anrufkontrolle->Ausgehende Dienste->Wahlkontrolle->Neu** besteht aus folgenden Feldern:

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Gesperrte Rufnummer</b>	Geben Sie die Nummer ein, deren Wahl verhindert werden soll.
<b>Freigegebene Rufnummer</b>	Geben Sie die Nummer ein, deren Wahl explizit erlaubt sein soll.

## 11 Anwendungen

Unter **Anwendungen** werden interne Telefon-Leistungsmerkmale des Systems eingerichtet.

### 11.1 Verbindungsdaten

Im Menü **Anwendungen->Verbindungsdaten** konfigurieren Sie die Erfassung der kommenden und gehenden Verbindungen.

Die Erfassung der Verbindungsdatensätze verschafft Ihnen einen Überblick über das Telefonieverhalten in Ihrem Unternehmen.

Im Gerät können alle externen Gespräche in Form von Verbindungsdatensätzen gespeichert werden. In diesen Datensätzen finden Sie wichtige Informationen über die einzelnen Gespräche.

Sie müssen die Erfassung der Verbindungsdaten im Menü **Nummerierung->Benutzereinstellungen->Berechtigungsklassen->Anwendungen** aktivieren. Im Auslieferungszustand ist die Funktion deaktiviert.

#### 11.1.1 Gehend

Das Menü **Anwendungen->Verbindungsdaten->Gehend** enthält Informationen, die das Überwachen der gehenden Aktivitäten ermöglichen.

Das Menü besteht aus folgenden Feldern:

##### Felder im Menü Gehend

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Dauer</b>	Zeigt die Dauer der Verbindung an.
<b>Benutzer</b>	Zeigt den Benutzer an, der angerufen hat.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Angerufener Name</b>	Zeigt den Namen an, der angerufen hat.

Feld	Beschreibung
<b>Gewählte Rufnummer</b>	Zeigt die gewählte Rufnummer an.
<b>Projektnummer</b>	Zeigt ggf. die Projektnummer des Gesprächs an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung nach Extern geleitet wurde.
<b>Kosten</b>	Zeigt die Kosten der Verbindung an, jedoch nur, wenn der Provider die entsprechenden Informationen übermittelt.

### 11.1.2 Kommend

Im Menü **Anwendungen->Verbindungsdaten->Kommend** enthält Informationen, die das Überwachen der kommenden Aktivitäten ermöglichen.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Kommend

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Dauer</b>	Zeigt die Dauer der Verbindung an.
<b>Benutzer</b>	Zeigt den Benutzer an, der angerufen wurde.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Anrufername</b>	Zeigt den Namen des Anrufers an.
<b>Externe Rufnummer</b>	Zeigt die Rufnummer des Anrufers an.
<b>Projektnummer</b>	Zeigt ggf. die Projektnummer des Gesprächs an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.

### 11.1.3 Allgemein

Im Menü **Anwendungen**->**Verbindungsdaten**->**Allgemein** können Sie einrichten, wie die Verbindungsdaten im System gespeichert werden.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Benutzername für Webzugang</b>	Geben Sie einen Benutzernamen für den Verbindungsdaten-Administrator ein.
<b>Passwort für Webzugang</b>	Geben Sie ein Passwort für den Verbindungsdaten-Administrator ein.
<b>Gehende Verbindungen speichern</b>	Wählen Sie aus, welche gehenden Verbindungen gespeichert werden sollen.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Keine</i> (Standardwert)</li> <li>• <i>Alle</i></li> <li>• <i>Nur mit Projekt-Nummer</i></li> </ul>
<b>Kommende Verbindungen speichern</b>	Wählen Sie aus, welche kommenden Verbindungen gespeichert werden sollen.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Keine</i> (Standardwert)</li> <li>• <i>Alle</i></li> <li>• <i>Nur mit Projekt-Nummer</i></li> </ul>
<b>Rufnummernverkürzung</b>	Wählen Sie aus, ob die Rufnummer verkürzt gespeichert werden soll.  Soll aus Datenschutzgründen die Anzeige der Rufnummer nur unvollständig erfolgen, können Sie hier die Anzahl der Stellen, die nicht angezeigt werden sollen, festlegen. Sie können für <b>Gehende Verbindungen</b> und für <b>Kommende Verbindungen</b> getrennt die Anzahl der ausgeblendeten Ziffern eingeben. Das Ausblenden der Ziffern erfolgt von rechts nach links.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Nein</i> (Standardwert)</li> <li>• <i>Alle</i></li> <li>• <i>1</i> bis <i>9</i></li> </ul>
<b>Verbindungsdaten über Serial 2 ausgeben</b>	<p>Nur für modulare Telefonanlagen</p> <p>Wählen Sie, ob die Verbindungsdaten für jedes Gespräch über die serielle Schnittstelle (Serial 2) ausgegeben werden sollen. Sie können auf diese Weise eine externe Softwarelösung zur Gebührenerfassung (Hotel-Applikation) anbinden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

#### Felder im Menü Aktionen

Feld	Beschreibung
<b>Verbindungsdaten exportieren</b>	Wenn Sie den aktuellen Verbindungsdatenbestand in eine externe Datei speichern möchten, klicken Sie <b>Exportieren</b> und speichern die Datei unter dem gewünschten Speicherort und Dateinamen ab.
<b>Verbindungsdaten löschen</b>	Wenn Sie den aktuellen Verbindungsdatenbestand aus dem Systemspeicher entfernen möchten, klicken Sie <b>Löschen</b> .

## 11.2 Anrufliste

Im Menü **Anwendungen**->**Anrufliste** können Sie Details eingehender und ausgehender Rufe einsehen. Welche und wie viele Rufe jeweils erfasst werden, können Sie im Untermenü **Allgemein** festlegen.

### 11.2.1 Kommend

Im Menü **Anwendungen**->**Anrufliste**->**Kommend** enthält Informationen, die das Überwachen der kommenden Aktivitäten ermöglichen.

Das Menü besteht aus folgenden Feldern:



**Felder im Menü Kommand**

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Typ</b>	Zeigt den Typ der Verbindung an.
<b>Benutzer</b>	Zeigt den Benutzer an, der angerufen wurde.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Anrufernummer</b>	Zeigt die Nummer des Anrufers an.
<b>Anschlussrufnummer</b>	Zeigt die Nummer des Anschlusses an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.
<b>Löschen</b>	Für alle angezeigten Geräte können Sie die Schaltflächen <b>Alle auswählen</b> bzw. <b>Alle deaktivieren</b> nutzen.

**11.2.2 Gehend**

Das Menü **Anwendungen->Anrufliste->Gehend** enthält Informationen, die das Überwachen der gehenden Aktivitäten ermöglichen.

Das Menü besteht aus folgenden Feldern:

**Felder im Menü Gehend**

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Typ</b>	Zeigt den Typ der Verbindung an.
<b>Benutzer</b>	Zeigt den Benutzer an, der angerufen wurde.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.

Feld	Beschreibung
<b>Gewählte Rufnummer</b>	Zeigt die gewählte Nummer an.
<b>Anschlussrufnummer</b>	Zeigt die Nummer des Anschlusses an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.
<b>Löschen</b>	Für alle angezeigten Geräte können Sie die Schaltflächen <b>Alle auswählen</b> bzw. <b>Alle deaktivieren</b> nutzen.

### 11.2.3 Allgemein

Im Menü **Anwendungen**->**Anrufliste**->**Allgemein** können Sie einrichten, wie die Verbindungsdaten im System gespeichert werden.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Anrufe erfassen</b>	Wählen Sie aus, welche Arten von Anrufen erfasst werden sollen.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Keine</i></li> <li>• <i>Nur Ankommend</i> (Standardwert)</li> <li>• <i>Alle</i></li> </ul>
<b>Angenommene Anrufe erfassen</b>	Legen Sie fest, ob auch angenommene Rufe erfasst werden sollen. Dies kann die Anzahl der erfassten Rufe stark erhöhen und dazu führen, dass die Liste nur einen relativ kurzen Zeitraum abdecken kann, bis die maximale Anzahl an Rufen erschöpft ist und die ersten Rufe aus der Liste gelöscht werden
<b>Max. Anruferlisteneinträge für Systemrufe</b>	Legen sie die maximale Anzahl an Systemrufen fest, die in der Liste erfasst werden. Der Maximalwert ist <i>1000</i> . Hierzu gehören z. B. Rufumleitungen nach extern, Rufe, die von einer Ansage angenommen werden, Team-Rufe, wenn kein einzelner Benutzer annimmt, etc.
<b>Max. Anruferlisteneinträge für Benutzer</b>	Legen sie die maximale Anzahl an Benutzerrufen (Rufe, die von einem eingerichteten Benutzer aufgebaut oder angenommen werden) fest, die in der Liste erfasst werden. Der Maximalwert

Feld	Beschreibung
	ist 200.

## 12 LAN


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

### 12.1 IP-Konfiguration

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



#### 12.1.1 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

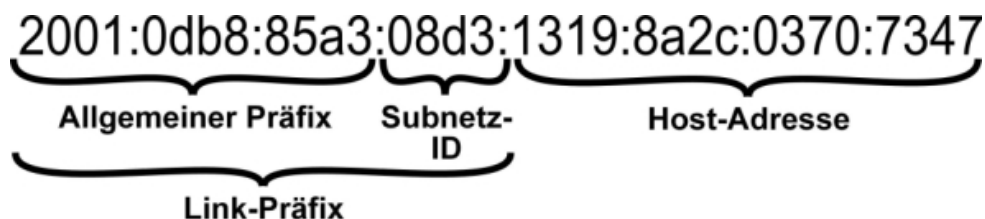
Falls Ihr Gerät an ein LAN angeschlossen ist, das aus zwei Teilnetzen besteht, sollten Sie für das zweite Teilnetz eine zweite **IP-Adresse / Netzmaske** eintragen.

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**.

### 12.1.1.1 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
<b>Basierend auf Ethernet-Schnittstelle</b>	<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>
<b>Schnittstellenmodus</b>	<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"> <li><i>Untagged</i> (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet.</li> <li><i>Tagged (VLAN)</i>: Diese Option gilt nur für Routing-Schnittstellen.</li> </ul> <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 <b>MAC-Adresse</b> ist in diesem Modus optional.</p>

Feld	Beschreibung
<b>VLAN-ID</b>	<p>Nur für <b>Schnittstellenmodus</b> = <i>Tagged</i> (VLAN)</p> <p>Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben.</p> <p>Mögliche Werte sind 1 (Standardwert) bis 4094.</p>
<b>MAC-Adresse</b>	<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 <b>Voreingestellte verwenden</b> 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 <b>Voreingestellte verwenden</b> aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet.</p> <p>Standardmäßig ist <b>Voreingestellte verwenden</b> aktiv.</p>

#### Felder im Menü Grundlegende IPv4-Parameter

Feld	Beschreibung
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> <li>• <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde.</li> </ul> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <a href="#">Firewall</a> auf Seite 343 konfigurieren.</p>
<b>Adressmodus</b>	<p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in <b>IP-Adresse / Netzmaske</b> zugewiesen.</li> <li>• <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.</li> </ul>
<b>DHCP Metrik</b>	<p>Es ist möglich, einer Schnittstelle, die per DHCP konfiguriert wird eine Metrik für die erhaltenen Routen zuzuweisen. Dies kann bei der Konfiguration von Backup-Verbindungen notwendig sein, um ein sauberes Umschalten zum Backup und wieder zurück zu gewährleisten.</p> <p>Der Standardwert ist <i>1</i>. Für eine Backup-Lösung sollte der Wert erhöht werden, damit die Backup-Route nicht eine zu hohe Priorität bekommt.</p>
<b>IP-Adresse / Netzmaske</b>	<p>Nur für <b>Adressmodus</b> = <i>Statisch</i></p> <p>Fügen Sie mit <b>Hinzufügen</b> einen neuen Adresseintrag hinzu und geben Sie die <b>IP-Adresse</b> und die entsprechende <b>Netzmaske</b> der virtuellen Schnittstelle ein.</p>

#### Felder im Menü Grundlegende IPv6-Parameter

Feld	Beschreibung
<b>IPv6</b>	<p>Wählen Sie aus, ob die gewählte 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>
<b>Sicherheitsrichtlinie</b>	<p>Hier nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> </ul>



Feld	Beschreibung
	<p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <ul style="list-style-type: none"> <li>• <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde.</li> </ul> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 343 konfigurieren.</p>
<b>IPv6-Modus</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Wählen Sie, ob die Schnittstelle im Host- oder im Router-Modus 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"> <li>• <i>Router (Router-Advertisement übermitteln)</i> (Standardwert): Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle gesendet werden sollen.</li> </ul> <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> <ul style="list-style-type: none"> <li>• <i>Host</i>: Die Schnittstelle wird im Host-Modus betrieben.</li> </ul>
<b>DHCP-Server</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i> und <b>IPv6-Modus</b> = <i>Router (Router-Advertisement übermitteln)</i></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</p>

Feld	Beschreibung
	<p>SLAAC erzeugen sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>IPv6-Adressen</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Sie können der gewählten Schnittstelle <b>IPv6-Adressen</b> zuordnen.</p> <p>Mit <b>Hinzufügen</b> können Sie einen oder mehrere Adresseinträge 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 (<b>IPv6-Modus</b> = <i>Host</i>, <b>Router Advertisement annehmen</b> <i>Aktiviert</i> und <b>DHCP-Client</b> <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 (<b>IPv6-Modus</b> = <i>Router (Router-Advertisement übermitteln)</i>, und <b>DHCP-Server</b> <i>Aktiviert</i>), so müssen Sie hier seine IPv6-Adressen konfigurieren.</p>
<b>Router Advertisement annehmen</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i> und <b>IPv6-Modus</b> = <i>Host</i></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>
<b>DHCP-Client</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i> und <b>IPv6-Modus</b> = <i>Host</i></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>

Feld	Beschreibung
	<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
<b>Ankündigen</b>	<p>Nur für <b>IPv6-Modus</b> = <i>Router</i> (<i>Router-Advertisement 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
<b>Art der Einrichtung</b>	<p>Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Von Allgemeinem Präfix</i> (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet.</li> <li>• <i>Statisch</i>: Sie können den Link-Präfix eingeben.</li> </ul>
<b>Allgemeiner Präfix</b>	<p>Nur für <b>Art der Einrichtung</b> = <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 <b>Netzwerk-&gt;Allgemeine IPv6-Präfixe-&gt;Konfiguration eines Allgemeinen Präfixes-&gt;Neu</b> angelegt sind.</p>
<b>Automatische Subnetzerstellung</b>	<p>Nur wenn <b>Art der Einrichtung</b> = <i>Von Allgemeinem Präfix</i> und wenn ein <b>Allgemeiner Präfix</b> gewählt ist.</p>

Feld	Beschreibung
	<p>Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID <i>0</i> verwendet, für das zweite Subnetz die Subnetz-ID <i>1</i>, usw.</p> <p>Mögliche Werte für die <b>Subnetz-ID</b> sind <i>0</i> bis <i>255</i>.</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> <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>
<b>Subnetz-ID</b>	<p>Nur wenn <b>Automatische Subnetzerstellung</b> 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 <i>0</i> bis <i>255</i>.</p> <p>Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.</p>
<b>Link-Präfix</b>	<p>Nur für <b>Art der Einrichtung</b> = <i>Statisch</i></p> <p>Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit <i>::</i> enden. Seine Länge ist mit <i>64</i> vorgegeben.</p>

#### Felder im Menü Host-Adresse


Feld	Beschreibung
<b>Erzeugungsmethode</b>	<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>

Feld	Beschreibung
	<p>EUI-64 setzt folgenden Prozess in Gang:</p> <ul style="list-style-type: none"> <li>• Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt.</li> <li>• In die entstandene Lücke wird <code>FFFF</code> eingefügt, um 64 Bit zu erhalten.</li> <li>• Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt.</li> <li>• Im ersten 8-Bit-Feld wird Bit 7 auf <code>1</code> gesetzt.</li> </ul>
<b>Statische Adressen</b>	<p>Sie können, unabhängig von der automatischen Erzeugung, die unter <b>Erzeugungsmethode</b> festgelegt ist, mit <b>Hinzufügen</b> den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit <code>64</code> vorgegeben. Beginnen Sie die Eingabe mit <code>: :</code></p>

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
<b>On Link Flag</b>	<p>Wählen Sie, ob das On-Link Flag (L-Flag) gesetzt werden soll.</p> <p>Dadurch fügt der Host das Präfix der Präfixliste hinzu.</p> <p>Mit Auswahl von <code>Wahr</code> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Autonomous Flag</b>	<p>Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll.</p> <p>Dadurch nutzt ein Host das Präfix und eine Schnittstellen-ID, um daraus seine Adresse abzuleiten.</p> <p>Mit Auswahl von <code>Wahr</code> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Bevorzugte Gültigkeitsdauer</b>	<p>Geben Sie eine Zeitspanne in Sekunden ein. Während dieser Zeit werden die Adressen, die mit Hilfe des Präfix per SLAAC</p>

Feld	Beschreibung
	<p>erzeugt wurden, bevorzugt verwendet.</p> <p>Der Standardwert ist <i>604800</i> Sekunden.</p>
<b>Gültigkeitsdauer</b>	<p>Geben Sie eine Zeitspanne in Sekunden an, für die das Präfix gültig ist.</p> <p>Der Standardwert ist <i>2592000</i> Sekunden.</p>
<div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;">  <p><b>Hinweis</b></p> <p>Der Wert für die Gültigkeitsdauer sollte niedriger sein als derjenige, der unter <b>Erweiterte IPv6-Einstellungen</b> für die Option <b>Router-Gültigkeitsdauer</b> konfiguriert ist.</p> </div>	

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


#### Felder im Menü **Erweiterte IPv4-Einstellungen**

Feld	Beschreibung
<b>DHCP-MAC-Adresse</b>	<p>Nur für <b>Adressmodus</b> = <i>DHCP</i></p> <p>Ist <b>Voreingestellte verwenden</b> 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 <b>Voreingestellte verwenden</b> 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>
<b>DHCP-Hostname</b>	<p>Nur für <b>Adressmodus</b> = <i>DHCP</i></p> <p>Geben Sie den Hostnamen ein, der vom Provider gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.</p>
<b>DHCP Broadcast Flag</b>	<p>Nur für <b>Adressmodus</b> = <i>DHCP</i></p>

Feld	Beschreibung
	<p>Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Standardroute erstellen</b>	<p>Nur für <b>Adressmodus</b> = <i>DHCP</i></p> <p>Wählen Sie aus, ob für diese Schnittstelle eine Standardroute festgelegt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Proxy ARP</b>	<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>
<b>TCP-MSS-Clamping</b>	<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
<b>Router-Gültigkeitsdauer</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i>, <b>IPv6-Modus</b> = <i>Router (Router-Advertisement übermitteln)</i> und <b>Router Advertisement übertragen</b> = <i>Aktiviert</i></p>

Feld	Beschreibung
	<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> <div data-bbox="539 483 1315 705" style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;">  <p><b>Hinweis</b></p> <p>Der Wert für die <b>Router-Gültigkeitsdauer</b> sollte höher sein als die kürzeste Link-Präfix-Gültigkeitsdauer, die im unter <b>Grundlegende IPv6-Parameter</b> für die Schnittstelle konfiguriert ist.</p> </div>
<p><b>Router-Präferenz</b></p>	<p>Nur für <b>IPv6 = Aktiviert</b>, <b>IPv6-Modus = Router (Router-Advertisement übermitteln)</b> und <b>Router Advertisement übertragen = Aktiviert</b></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"> <li>• <i>Hoch</i></li> <li>• <i>Mittel</i> (Standardwert)</li> <li>• <i>Niedrig</i></li> </ul>
<p><b>DHCP-Modus</b></p>	<p>Nur für <b>IPv6 = Aktiviert</b>, <b>IPv6-Modus = Router (Router-Advertisement übermitteln)</b> und <b>Router Advertisement übertragen = Aktiviert</b></p> <p>Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus.</p> <div data-bbox="539 1494 1315 1614" style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px;">  <p><b>Hinweis</b></p> <p>Der Router muss nicht als DHCP-Server eingerichtet sein.</p> </div>



Feld	Beschreibung
	<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>
<b>DNS-Propagation</b>	<p>Nur für <b>IPv6-Modus = Router</b> (<i>Router-Advertisement übermitteln</i>) und <b>Router Advertisement übertragen</b> <i>Aktiviert</i></p> <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"> <li>• <i>Aus</i>: Es wird keine DNS-Server-Adresse propagiert.</li> <li>• <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"> <li>• Globale Adressen</li> <li>• ULA (Unique Local Addresses)</li> <li>• Link-Lokale-Adressen</li> </ul> </li> <li>• <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.</li> </ul>

## 12.2 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**.

### 12.2.1 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.

#### 12.2.1.1 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
<b>VLAN Identifier</b>	Geben Sie die Ziffer ein, die das VLAN identifiziert. Im  -

Feld	Beschreibung
	Menü kann dieser Wert nicht mehr verändert werden. Mögliche Werte sind 1 (Standardwert) bis 4094
<b>VLAN-Name</b>	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> .
<b>VLAN-Mitglieder</b>	Wählen Sie die Ports aus, die zu diesem VLAN gehören sollen. Über die Schaltfläche <b>Hinzufügen</b> 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.

## 12.2.2 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
<b>Schnittstelle</b>	Zeigt den Port an, für den Sie die PVID definieren und Verarbeitungsregeln definieren.
<b>PVID</b>	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.
<b>Frames ohne Tag verwerfen</b>	Wenn die Option aktiviert ist, werden ungetaggte Frames verworfen. Ist die Option deaktiviert, werden ungetaggte Frames mit der in diesem Menü definierten PVID getaggt.
<b>Nicht-Mitglieder verwerfen</b>	Wenn die Option aktiviert ist, werden alle getaggten Frames verworfen, die mit einer VLAN-ID getaggt sind, in der der aus-

Feld	Beschreibung
	gewählte Port nicht Mitglied ist.

### 12.2.3 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:

#### Feld im Menü **Bridge-Gruppe br<ID> VLAN-Optionen**

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

## 13 Wireless LAN Controller

Mit dem Wireless LAN Controller können Sie eine WLAN-Infrastruktur aufbauen und verwalten. Die Vernetzung erfolgt dabei nach dem Master-Slave-Prinzip. Das System nutzt das CAPWAP-Protokoll (Control and Provisioning of Wireless Access Points Protocol) für die Kommunikation zwischen Master und Slaves. In größeren WLAN-Netzen übernimmt ein Gateway die Master-Funktion und verwaltet die Access Points (APs). In kleineren WLAN-Infrastrukturen mit bis zu sechs APs dient ein AP als Master. Der WLAN Controller kann ab Systemsoftwareversion 10.1.7 auch dazu verwendet werden, ein WLAN ausschließlich mit dem internen Funkmodul des Geräts zu realisieren.

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

Der WLAN Controller verfügt über einen Assistenten, der Sie bei der Konfiguration unterstützt. Sobald der Controller alle APs in seinem System "gefunden" hat, bekommen diese jeweils ein neues Passwort und eine neue Konfiguration. Sie werden über den WLAN Controller verwaltet und sind nicht mehr "von außen" manipulierbar; der Zugriff auf den jeweiligen AP ist gesperrt.

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

- APs erkennen und vernetzen

Sie können mit dem Assistenten fabrikneue Geräte automatisch erkennen und zu einem WLAN vernetzen.

- APs überwachen

Der WLAN Controller überwacht den Access-Point-Betrieb und die Client-Aktivitäten. Benachbarte APs außerhalb des eigenen WLANs werden ebenfalls erkannt und angezeigt. Bei Ausfall eines APs in Ihrem WLAN können Sie sich per E-Mail benachrichtigen lassen.

Unauthorisierte Verbindungsversuche zu einem AP von außen werden vom WLAN Controller verworfen.

Die Sicherung der Netzwerkschlüssel und Passwörter erfolgt nicht auf den APs selbst. Daher stellen APs, die an öffentlich zugänglichen Stellen installiert sind, im Falle eines Diebstahls kein Sicherheitsrisiko dar.

- APs verwalten

Software und Konfiguration lassen sich schnell und einfach ändern und an alle APs verteilen. Die Konfiguration ist zentral gespeichert und wird bei Bedarf (z. B. Stromausfall) automatisch erneut an alle APs übertragen. Updates der Systemsoftware erfolgen eben-

falls automatisiert.

Darüber hinaus werden unter anderem folgende Funktionen unterstützt:

- Automatische Kanalplanung für überlappungsfreie Frequenzvergabe
- VLAN und Multi-SSID
- IEEE 802.11 a/b/g/n/ac
- Optimiertes Roaming für Voice over WLAN (VoWLAN)
- Programm-gesteuerte Aktionen (z. B. WLAN ausschalten während der Nacht).

Sie können mit dem WLAN Controller zum Beispiel folgende Szenarien realisieren:

- Mehrere Standorte

Bei einem Unternehmen mit mehreren Standorten können Sie mit dem WLAN Controller alle Standorte mit WLAN ausstatten und untereinander vernetzen. Sie können für alle Mitarbeiter einen Zugang zum Intranet der Firma und zum Internet zur Verfügung stellen.

- Gäste-WLAN

Der WLAN Controller hilft Ihnen, einen WLAN-Zugang zu Ihrem lokalen Netzwerk anzulegen und ein Gäste-WLAN einzurichten. Die Nutzer des Gäste-WLANs sollen normalerweise zwar Zugang zum Internet haben aber keinen Zugriff auf das Intranet der Firma.



#### Hinweis

Wenn Sie mit dem WLAN Controller das interne WLAN-Funkmodul eines bintec-elmeg-Geräts konfigurieren und verwalten wollen, muss folgende Voraussetzung erfüllt sein:

Die WLAN-Schnittstelle muss sich in einer Bridge-Gruppe mit der Ethernet-Schnittstelle befinden, über die das Gerät an das LAN angeschlossen ist. Dieses ist nicht bei allen Produkten in der Standardkonfiguration der Fall. Überprüfen Sie ggf. zunächst die Einstellung der Schnittstellen.

## 13.1 Wizard

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



### Hinweis

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

## 13.1.1 Wireless LAN Controller Wizard

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

### 13.1.1.1 Grundeinstellungen

Der Wireless LAN Controller verwendet folgende Einstellungen:

#### Regulierungsbereich

Wählen Sie hier den Regulierungsbereich. Durch die Auswahl ergeben sich die Länder, die Sie im Anschluss für die Option **Region** auswählen können. Der Standardwert ist hier *ETSI* (European Telecommunications Standards Institute).

#### 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-Konfiguration->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.

### 13.1.1.2 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.

### 13.1.1.3 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.

#### 13.1.1.3.1 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.

#### IGMP Snooping

IGMP Snooping reduziert den Datenverkehr und damit die Netzlast. Mit Auswahl von *Aktiviert* ist die Funktion aktiv.

#### 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 eine Kombination von WPA, WPA 2 bzw. WPA 3 oder eine spezifische WPA-Version 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**

Bei der Verwendung von WPA-Enterprise können Sie 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.

**13.1.1.4 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 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.

## 13.1.2 Wireless LAN Controller VLAN Konfiguration

Um WLANs (VSS) voneinander zu trennen, können Sie bei der Konfiguration eines VSS die Funktion VLAN aktivieren und eine VLAN-ID vergeben. Damit die Trennung von anderen Schnittstellen wirksam ist, müssen Sie für dieses VLAN eine virtuelle Schnittstelle mit einer eigenen IP-Konfiguration anlegen und ggf. einen DHCP Pool erstellen, aus dem Clients innerhalb dieses VLANs mit IP-Adressen versorgt werden. Sie können diese Einstellungen wie bisher in den Menüs **LAN->IP-Konfiguration** bzw. **Lokale Dienste->DHCP Server** vornehmen oder das hier angebotene Menü nutzen. Einstellungen, die Sie hier vornehmen, werden automatisch in die anderen Menüs übernommen.

Sie sehen eine Übersicht der bisher angelegten VLANs mit ihren IDs und der jeweils zugeordneten IP- bzw. DHCP-Konfiguration. Um einen Eintrag zu bearbeiten, wählen Sie das Symbol  in der entsprechenden Zeile, um einen neuen Eintrag hinzuzufügen, klicken Sie auf **Neu**. Einen neuen Eintrag können Sie nur für ein VSS mit einer VLAN-ID erstellen, das noch keine VLAN-Konfiguration hat.

### 13.1.2.1 Bearbeiten oder Neu

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

Das Menü **Wireless LAN Controller->Wizard->Wireless LAN Controller VLAN Konfiguration->Neu** besteht aus folgenden Feldern:

#### Felder im Menü VSS VLAN Netzwerkkonfiguration

Feld	Beschreibung
<b>VLAN-ID</b>	Wählen Sie eine der existierenden VLAN-IDs aus dem Auswahlmenü. Es werden nur IDs angezeigt, für die noch keine Konfiguration vorliegt.
<b>IP-Adresse/Netzmaske</b>	Geben Sie hier die IP-Konfiguration der neuen Schnittstelle ein. Achten Sie darauf, dass diese noch nicht verwendet worden ist.
<b>DHCP-Server</b>	Um Clients, die sich mit diesem VLAN verbinden, eine IP-Konfiguration zuzuweisen, können Sie einen externen oder den internen DHCP-Server Ihres Geräts verwenden.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Extern oder statisch</i>: Verwenden Sie diese Option, wenn Sie in Ihrem Netzwerk bereits einen DHCP-Server be-</li> </ul>

Feld	Beschreibung
	<p>treiben oder die Clients, die sich mit den VLAN verbinden, eine statische IP-Konfiguration haben. Achten Sie darauf, dass ein externer DHCP-Server aus dem Netzwerk des VLAN erreichbar ist.</p> <ul style="list-style-type: none"> <li>• <i>Intern</i>: Verwenden Sie diese Option, wenn Sie Ihr Gerät als DHCP-Server für das VLAN einsetzen wollen.</li> </ul>
<b>IP-Adressbereich</b>	<p>Nur bei <b>DHCP-Server = Intern</b></p> <p>Geben Sie hier die erste und die letzte IP-Adresse ein, die Ihr Gerät innerhalb des VLAN vergeben soll. Achten Sie darauf, dass der Adressraum zur IP-Adresse der Schnittstelle dieses VLAN passt und sich nicht mit anderen IP-Adress-Pools überschneidet.</p> <p>Für die DHCP-Konfiguration wird automatisch Ihr Gerät als Gateway eingetragen, die Lease Time beträgt 120 Minuten. Wenn Sie diese Einstellungen anpassen wollen, gehen Sie in das Menü <b>Lokale Dienste-&gt;DHCP Server-&gt;DHCP-Konfiguration</b>.</p>


## 13.2 Controller-Konfiguration

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

### 13.2.1 Allgemein

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

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Status</b>	<p>Aktivieren Sie die Option <b>Status</b> um die Grundeinstellungen für den Wireless LAN Controller zu konfigurieren.</p> <p>Standarmäßig ist die Funktion nicht aktiv.</p>
<b>Die gesamte Konfiguration des WLAN Controllers löschen</b>	<p>Nur für <b>Status</b> = nicht aktiviert.</p> <p>Mithilfe des Symbols  können Sie eine Konfiguration löschen.</p>

Feld	Beschreibung
<b>Regulierungsbereich</b>	Wählen Sie hier den Regulierungsbereich. Durch die Auswahl ergeben sich die Länder, die Sie im Anschluss für die Option <b>Region</b> auswählen können. Der Standardwert ist hier <i>ETSI</i> (European Telecommunications Standards Institute).
<b>Region</b>	<p>Wählen Sie das Land, in welchem der Wireless LAN Controller betrieben werden soll.</p> <p>Mögliche Werte sind alle auf dem Wirelessmodul des Geräts vorkonfigurierten Länder.</p> <p>Der Bereich der verwendbaren Kanäle variiert je nach Länder-einstellung.</p> <p>Der Standardwert ist <i>Germany</i>.</p>
<b>Schnittstelle</b>	Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.
<b>DHCP-Server</b>	<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 <b>GUI</b> Menü dieses Geräts unter <b>Lokale Dienste-&gt;DHCP-Server-&gt;DHCP Pool-&gt;Neu-&gt;Erweiterte Einstellungen</b> im Feld <b>DHCP-Optionen</b> auf die Schaltfläche <b>Hinzufügen</b>. Wählen Sie als <b>Option</b> <i>CAPWAP Controller</i> und tragen Sie im Feld <b>Wert</b> 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 <b>Systemverwaltung -&gt;Globale Einstellungen-&gt;System</b> im Feld <b>Manuelle IP-Adresse des WLAN-Controller</b> eintragen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Intern</i>: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.</li> </ul>
<b>IP-Adressbereich</b>	<p>Nur für <b>DHCP-Server</b> = <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>
<b>Standort des verwalteten Access Points</b>	<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"> <li>• <i>Lokal (LAN)</i> (Standardwert)</li> <li>• <i>Entfernt (WAN)</i></li> </ul> <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>
<b>LED-Modus des verwalteten Access Points</b>	<p>Wählen Sie das Leuchtverhalten der Access Point-LEDs.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Status</i> (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde.</li> <li>• <i>Blinkend</i>: Die LEDs zeigen ihr Standardverhalten.</li> <li>• <i>Aus</i>: Alle LEDs sind deaktiviert.</li> </ul>



## 13.2.2 Autoprofil für Access Points

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.

### 13.2.2.1 Bearbeiten oder Neu

Das Menü **Wireless LAN Controller->Controller-Konfiguration->Access Point-Autoprofil->Neu** besteht aus folgenden Feldern:

#### Felder im Menü Access-Point-Filter

Feld	Beschreibung
<b>MAC-Adresse</b>	Geben Sie die MAC-Adresse eines Access Points ein, der bei seiner Integration in das Netzwerk automatisch konfiguriert werden soll.  Standardmäßig ist <b>Alle</b> aktiviert, so dass der Eintrag auf jeden neu hinzukommenden Access Point zutrifft.
<b>IP-Adresse/Netzmaske</b>	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
<b>Standort</b>	Geben Sie den Standort des APs an.
<b>Beschreibung</b>	Geben Sie eine eindeutige Beschreibung für den AP ein.

#### Felder im Menü Funkmodul 1 oder im Funkmodul 2

Feld	Beschreibung
<b>Betriebsmodus</b>	Wählen Sie aus, ob Access Points, denen das Autoprofil zugewiesen wird, das entsprechende Radiomodul aktivieren sollen.  Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion aktiv.
<b>Aktives Funkmodul-</b>	Nur für <b>Betriebsmodus</b> = <i>Aktiviert</i>



Feld	Beschreibung
<b>profil</b>	<p>Wählen Sie ein Funkmodulprofil aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• 2.4 GHz Radio Profile</li> <li>• 5 GHz Radio Profile</li> </ul>
<b>Zugewiesene Drahtlosnetzwerke (VSS)</b>	<p>Nur für <b>Betriebsmodus</b> = <i>Aktiviert</i></p> <p>Fügen Sie mit <b>Hinzufügen</b> ein Drahtlosnetzwerk hinzu.</p>


## 13.3 Access-Point-Konfiguration

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

### 13.3.1 Access Points

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

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

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


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


#### Mögliche Werte für Status


Status	Bedeutung
<b>Gefunden</b>	Der AP hat sich beim Wireless LAN Controller gemeldet. Der Controller hat die Systemparameter vom AP abgefragt.
<b>Initialisiere</b>	Der WLAN Controller und die APs "verständigen sich" über CAPWAP. Die Konfiguration wird an die APs übertragen und aktiviert.
<b>Managed</b>	Der AP ist auf den Status Managed gesetzt. Der Controller hat

Status	Bedeutung
	eine Konfiguration zum AP geschickt und diese aktiviert. Der AP wird vom Controller zentral verwaltet und kann nicht über das <b>GUI</b> konfiguriert werden.
<b>Keine Lizenz vorhanden</b>	Der WLAN Controller verfügt über keine freie Lizenz für diesen AP.
<b>Aus</b>	Der AP ist entweder administrativ deaktiviert oder ausgeschaltet bzw. ohne Stromversorgung o.ä.

### 13.3.1.1 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**->**Access Point-Konfiguration**->**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

Feld	Beschreibung
<b>Gerätetyp</b>	Hier werden Ihnen verschiedene relevante Informationen zu diesem Access Point angezeigt wie  ...der Typ des verwalteten Access Points.
<b>Seriennummer</b>	... die Seriennummer des verwalteten Gerätes.
<b>LAN-MAC-Adresse</b>	... die MAC-Adresse der LAN-Schnittstelle des verwalteten Geräts.
<b>Funkmodul 1 unterstützte Funktionen</b>	Informationen zu den vom Access Point unterstützten Funktionen: <ul style="list-style-type: none"> <li>• Frequenzbänder</li> <li>• Bandbreite</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• Drahtloser Modus</li> <li>• Spatial Streams</li> <li>• Data-Rate Trimming</li> <li>• WPA 3</li> </ul>

#### Felder im Menü Access-Point-Einstellungen

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

#### Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
<b>Betriebsmodus</b>	<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"> <li>• <i>Ein</i> (Standardwert): Das Funkmodul dient als Access Point in Ihrem Netzwerk.</li> <li>• <i>Aus</i>: Das Funkmodul ist nicht aktiv.</li> </ul>
<b>Aktives Funkmodulprofil</b>	Zeigt das aktuell gewählte Funkmodulprofil. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere

Feld	Beschreibung
	Funkmodulprofile angelegt sind.
<b>Kanal</b>	<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"> <li>• Für <b>Aktives Funkmodulprofil = 2,4 GHz Radio Profile</b> Mögliche Werte sind <i>1</i> bis <i>13</i> und <i>Auto</i> (Standardwert).</li> <li>• Für <b>Aktives Funkmodulprofil = 5 GHz Radio Profile</b> Mögliche Werte sind je nach Einstellung des Modulprofils <i>36</i>, <i>40</i>, <i>44</i>, <i>48</i> und <i>Auto</i> (Standardwert)</li> </ul>
<b>Verwendeter Kanal</b>	<p>Nur für Managed APs.</p> <p>Zeigt den aktuell benutzten Kanal.</p>
<b>Sendeleistung</b>	<p>Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen.</p> <p>Mögliche Werte:</p>


Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet.</li> <li>• 5 dBm</li> <li>• 8 dBm</li> <li>• 11 dBm</li> <li>• 14 dBm</li> <li>• 16 dBm</li> <li>• 17 dBm</li> </ul>
<b>Zugewiesene Drahtlosnetzwerke (VSS)</b>	Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

## 13.3.2 Funkmodulprofile

Im Menü **Wireless LAN Controller**->**Access Point-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**).

### 13.3.2.1 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 Controller**->**Access Point-Konfiguration** ->**Funkmodulprofile** ->**Neu** besteht aus folgenden Feldern:

#### Felder im Menü Funkmodulprofil-Konfiguration

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie eine beliebige Beschreibung des Funkmodulprofils ein.
<b>Betriebsmodus</b>	Legen Sie fest, in welchem Modus das Funkmodulprofil betrieben werden soll.  Mögliche Werte:

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Aus</i> (Standardwert): Das Funkmodulprofil ist nicht aktiv.</li> <li>• <i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk.</li> </ul>
<b>Frequenzband</b>	<p>Wählen Sie das Frequenzband des Funkmodulprofils aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>2,4 GHz In/Outdoor</i> (Standardwert): Ihr Gerät wird mit 2,4 GHz innerhalb oder außerhalb von Gebäuden betrieben.</li> <li>• <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz innerhalb von Gebäuden betrieben.</li> <li>• <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz außerhalb von Gebäuden betrieben.</li> <li>• <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz innerhalb oder außerhalb von Gebäuden betrieben.</li> <li>• <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.</li> </ul>

### Felder im Menü Performance-Einstellungen

Feld	Beschreibung
<b>Drahtloser Modus</b>	<p>Wählen Sie die Wireless-Technologie aus, die der Access-Point anwenden soll.</p> <p>Für das <b>Frequenzband</b> = <i>2,4 GHz In/Outdoor</i> stehen Ihnen alle Modi von <i>802.11b</i> bis zum aktuellen <i>802.11ax</i> (ohne <i>802.11ac</i>, das nur im 5-GHz-Modus sinnvoll ist) sowie Kombinationen davon zur Verfügung. Bedenken Sie, dass nicht alle Access Points und auch nicht alle Clients immer die neuesten Modi unterstützen.</p> <p>Für <b>Frequenzband</b> = <i>5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor</i> oder <i>5,8 GHz Outdoor</i> stehen Ihnen alle Modi von <i>802.11a</i> bis zum aktuellen <i>802.11ax</i> (ohne <i>802.11b</i> und <i>g</i>, die für 5-GHz nicht spezifiziert sind) sowie Kombinationen davon zur Verfügung. Bedenken Sie, dass nicht alle Access Points und auch nicht alle Clients immer die neuesten</p>

Feld	Beschreibung
	Modi unterstützen.
<b>Bandbreite</b>	<p>Nur für <b>Frequenzband</b> = 5 GHz und nicht <b>Drahtloser Modus 802.11a</b>.</p> <p>Wählen Sie aus, wie viele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• 20 MHz: Ein Kanal mit 20 MHz Bandbreite wird verwendet.</li> <li>• 40 MHz: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Haupt-Kanal und der andere als Erweiterungs-Kanal.</li> <li>• 80 MHz: Vier Kanäle mit je 20 MHz Bandbreite werden verwendet. Somit steht eine Bandbreite von 80 MHz zur Verfügung.</li> </ul>
<b>Anzahl der Spatial Streams</b>	<p>Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen.</p> <p>Mögliche Werte: 1 bis 4. Die verfügbaren Optionen hängen von der Kombination des Frequenzbands und des Drahtlosen Modus ebenso ab wie vom Access-Point-Modell.</p>
<b>Airtime Fairness</b>	<p>Diese Funktion ist nicht für alle Geräte verfügbar.</p> <p>Mit der <b>Airtime Fairness</b> -Funktion wird gewährleistet, dass Senderressourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.</p>
<b>Wiederkehrender Hintergrund-Scan</b>	<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</p>




Feld	Beschreibung
	<p>Sie die Funktion <b>Wiederkehrender Hintergrund-Scan</b> aktivieren. Diese Suche erfolgt ohne eine Beeinträchtigung der Funktion als Access Point.</p> <p>Aktivieren oder deaktivieren Sie die Funktion <b>Wiederkehrender Hintergrund-Scan</b>.</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
<p><b>Kanalplan</b></p>	<p>Wählen Sie den gewünschten Kanalplan aus.</p> <p>Der sogenannte 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 mindestens 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"> <li>• <i>Alle</i>: Alle Kanäle können bei der Kanalwahl gewählt werden.</li> <li>• <i>World Mode</i> (für <b>Frequenzband</b> = 2,4 GHz, Standardwert): Die automatische Kanalauswahl verwendet nur die überlappungsfreien Kanäle 1, 6, 11.</li> <li>• <i>ETSI-Modus</i> (für <b>Frequenzband</b> = 2,4 GHz): Die automatische Kanalauswahl verwendet nur die überlappungsfreien Kanäle 1, 5, 9, 13.</li> <li>• <i>Keine Wetterradarkanäle</i> (für <b>Frequenzband</b> = 5 GHz, Standardwert): Die Wetterradarkanäle sind von der Kanalwahl ausgeschlossen.</li> </ul> <p>Mögliche Werte:</p> <p>36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140.</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Indoors No DFS/TPC</i> (für <b>Frequenzband = 5 GHz</b>): Diese Kanäle können innerhalb von Gebäuden verwendet werden. DFS (Dynamic Frequency Selection) und TPC (Transmitter Power Control) kommen dabei nicht zum Einsatz.</li> </ul> <p>Mögliche Werte:</p> <p><i>36, 40, 44, 48.</i></p> <ul style="list-style-type: none"> <li>• <i>Keine Outdoor-Kanäle</i> (für <b>Frequenzband = 5 GHz</b>): In diesem Kanalplan sind die nur für Indoor-Anwendungen freigegebenen Kanäle 36 bis 64 zusammengefasst. Mit diesem Kanalplan können insbesondere 5GHz-WLAN-fähige Multimedia-Geräte wie Smart TVs optimal in das WLAN-Netz eingebunden werden, die häufig die 5GHz-Outdoor-Kanäle (ab Kanal 100) nicht unterstützen.</li> <li>• <i>Benutzerdefiniert</i>: Wählen Sie die gewünschten Kanäle selbst aus.</li> </ul>
<b>Benutzerdefinierter Kanalplan</b>	<p>Nur für <b>Kanalplan = Benutzerdefiniert</b></p> <p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <p>Mit <b>Hinzufügen</b> 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>
<b>Bei Störung Kanal wechseln</b>	<p>Aktivieren Sie diese Option, wenn der Access Point den Funkkanal ändern soll, sobald die Verbindung durch Störungen beeinträchtigt wird.</p>
<b>Short Guard Interval</b>	<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>
<b>Max. Übertragungsrate</b>	<p>Wählen Sie die Übertragungsgeschwindigkeit aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Auto</i> (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt.</li> <li>• <i>&lt;Wert&gt;</i>: Je nach Einstellung für <b>Frequenzband</b>, <b>Bandbreite</b>,</li> </ul>

Feld	Beschreibung
	<p><b>Anzahl der Spatial Streams</b> und <b>Drahtloser Modus</b> stehen verschiedene feste Werte in MBit/s zur Auswahl.</p>
<b>Beacon Period</b>	<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>
<b>DTIM Period</b>	<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>
<b>RTS Threshold</b>	<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>
<b>Short Retry Limit</b>	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Frames ein, dessen Länge kürzer oder gleich dem in <b>RTS Threshold</b> 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>
<b>Long Retry Limit</b>	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, dessen Länge größer ist als der in <b>RTS Threshold</b> definierte Wert. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen.</p>

Feld	Beschreibung
	<p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 4.</p>
<b>Fragmentation Thresh- hold</b>	<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>


### 13.3.3 Drahtlosnetzwerke (VSS)

Im Menü **Wireless LAN Controller**->**Access Point-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.

#### 13.3.3.1 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**->**Access Point-Konfiguration** ->**Drahtlosnetzwerke (VSS)**->**Neu** besteht aus folgenden Feldern:


#### Felder im Menü Service Set Parameter

Feld	Beschreibung
<b>Netzwerkname (SSID)</b>	<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 <b>Netzwerkname (SSID)</b> übertragen werden soll.</p>


Feld	Beschreibung
	<p>Mit Auswahl von <i>Sichtbar</i> wird der Netzwerkname sichtbar übertragen.</p> <p>Standardmäßig ist er sichtbar.</p>
<b>Intra-cell Repeating</b>	<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> <p>Die Nutzer des Gäste-WLANs sollen normalerweise zwar Zugang zum Internet haben aber keinen Zugriff auf das Intranet der Firma. Um das zu verhindern, muss die Option deaktiviert sein.</p>
<b>U-APSD</b>	<p>Wählen Sie aus, ob der Stromsparmodus Unscheduled Automatic Power Save Delivery (U-APSD) aktiviert werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>IGMP Snooping</b>	<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
<b>Sicherheitsmodus</b>	<p>Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>OWE-Transition</i></li> </ul>

Feld	Beschreibung
	<p>Die Einstellung <i>OWE-Transition</i> erfordert keine Eingabe eines <b>Preshared Key</b> und ist für offene Gästenetze geeignet. Es bietet sich für Netze an, die von WPA3-fähigen Clients, aber auch von älteren, nicht WPA3-fähigen, Clients genutzt werden sollen. Bei Clients, die <b>WPA3</b> unterstützen, erfolgt die Datenübertragung zwischen Access Point und Client verschlüsselt. Bei Clients, die kein <b>WPA3</b> unterstützen, erfolgt die Datenübertragung unverschlüsselt.</p> <ul style="list-style-type: none"> <li>• <i>OWE</i></li> </ul>
	<div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px;">  <p><b>Hinweis</b></p> <p>OWE funktioniert nur mit Endgeräten, die WPA3 und OWE unterstützen.</p> </div>
	<p>Die Einstellung <i>OWE</i> erfordert keine Eingabe eines <b>Preshared Key</b> und ist für offene Gästenetze geeignet. Die Datenübertragung zwischen Access Point und Client ist dennoch verschlüsselt.</p> <ul style="list-style-type: none"> <li>• <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung</li> <li>• <i>WEP 40</i>: WEP 40 Bit</li> <li>• <i>WEP 104</i>: WEP 104 Bit</li> <li>• <i>WPA-PSK</i>: WPA Preshared Key</li> <li>• <i>WPA-Enterprise</i>: 802.11x</li> </ul>
<b>Übertragungsschlüssel</b>	<p>Nur für <b>Sicherheitsmodus</b> = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in <b>WEP-Schlüssel</b> konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Der Standardwert ist <i>Schlüssel 1</i>.</p>
<b>WEP-Schlüssel 1-4</b>	<p>Nur für <b>Sicherheitsmodus</b> = <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 Zei-</p>

Feld	Beschreibung
	chen.
<b>WPA-Modus</b>	<p>Für <b>Sicherheitsmodus</b> = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>WPA</i>: WLAN Clients, die <b>WPA</b> unterstützen, können sich verbinden.</li> <li>• <i>WPA2</i>: WLAN Clients, die <b>WPA2</b> unterstützen, können sich verbinden.</li> <li>• <i>WPA3</i>: Nur WLAN Clients, die <b>WPA3</b> unterstützen, können sich verbinden.</li> <li>• <i>WPA</i> und <i>WPA2</i>: WLAN Clients, die <b>WPA1</b> oder <b>WPA2</b> unterstützen, können sich verbinden.</li> <li>• <i>WPA2</i> und <i>WPA3</i> (Standardwert): WLAN Clients, die <b>WPA2</b> oder <b>WPA3</b> unterstützen, können sich verbinden.</li> </ul>
<b>WPA Cipher</b>	<p>Für <b>Sicherheitsmodus</b> = <i>WPA-PSK</i> oder <i>WPA-Enterprise</i> und für <b>WPA-Modus</b> = <i>WPA</i> oder <i>WPA</i> und <i>WPA2</i> .</p> <p>Wählen Sie aus, welche Verschlüsselung Sie anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>AES</i>: AES wird angewendet.</li> <li>• <i>TKIP</i>: TKIP wird angewendet</li> <li>• <i>AES</i> und <i>TKIP</i> (Standardwert): AES oder TKIP werden angewendet.</li> </ul>
<b>WPA2 Cipher</b>	<p>Für <b>Sicherheitsmodus</b> = <i>WPA-PSK</i> oder <i>WPA-Enterprise</i> und für <b>WPA-Modus</b> = <i>WPA2</i> oder <i>WPA</i> und <i>WPA2</i></p> <p>Wählen Sie aus, welche Verschlüsselung Sie anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>AES</i>: AES wird angewendet.</li> <li>• <i>AES</i> und <i>TKIP</i> (Standardwert): AES oder TKIP werden angewendet.</li> </ul>
<b>WPA2/3 Cipher</b>	Für <b>Sicherheitsmodus</b> = <i>WPA-PSK</i> oder


Feld	Beschreibung
	<p>und für <b>WPA-Modus</b> = <i>WPA2</i> und <i>WPA3</i> wird lediglich eine Verschlüsselung mit AES unterstützt. Weitere Einstellungen sind nicht erforderlich.</p>
<p><b>WPA3 Cipher</b></p>	<p>Für <b>Sicherheitsmodus</b> = <i>WPA-PSK</i> oder <i>WPA-Enterprise</i> und für <b>WPA-Modus</b> = <i>WPA3</i> wird eine Verschlüsselung mit AES in folgenden Varianten unterstützt:</p> <ul style="list-style-type: none"> <li>• AES</li> <li>• AES-GCMP</li> <li>• AES-256</li> <li>• AES-GCMP-256.</li> </ul>
<p><b>Preshared Key</b></p>	<p>Nur für <b>Sicherheitsmodus</b> = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.</p> <div data-bbox="541 843 1315 1031" style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> <b>Hinweis</b></p> <p>Ändern Sie unbedingt den Standard Preshared Key! Solange der Schlüssel nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p> </div>
<p><b>RADIUS-Server</b></p>	<p>Nur für <b>Sicherheitsmodus</b> = <i>WPA-Enterprise</i> Sie können den Zugang zu einem Drahtlosnetzwerk über einen RADIUS-Server regeln.</p> <p>Mit <b>Hinzufügen</b> können Sie neue Einträge anlegen. Geben Sie die IP-Adresse und das Passwort des RADIUS-Servers ein.</p>
<p><b>EAP-Vorabauthentifizierung</b></p>	<p>Nur für <b>Sicherheitsmodus</b> = <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>



Feld	Beschreibung
	<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
<b>Max. Anzahl Clients - Hard Limit</b>	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p> <p>Mögliche Werte sind ganze Zahlen von <i>1</i> bis <i>254</i>.</p> <p>Der Standardwert ist <i>32</i>.</p>
<b>Max. Anzahl Clients - Soft Limit</b>	<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 <b>Max. Anzahl Clients - Hard Limit</b> werden Anfragen strikt abgelehnt.</p> <p>Der Wert der <b>Max. Anzahl Clients - Soft Limit</b> muss gleich oder kleiner sein als der <b>Max. Anzahl Clients - Hard Limit</b>.</p> <p>Der Standardwert ist <i>28</i>.</p> <p>Sie können diese Funktion deaktivieren, indem Sie <b>Max. Anzahl Clients - Soft Limit</b> und <b>Max. Anzahl Clients - Hard Limit</b> auf den gleichen Wert einstellen.</p>
<b>Auswahl des Client-Bands</b>	<p>Wählen Sie aus, ob das 5-GHz-Band bevorzugt verwendet werden soll.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Deaktiviert, optimiert für Fast Roaming</i>: das 5-GHz-Band wird nicht bevorzugt verwendet, Fast Roaming kommt zum Einsatz.</li> <li>• <i>5-GHz-Band bevorzugt</i>: Das 5-GHz-Band soll - wenn möglich - bevorzugt verwendet werden.</li> </ul> <div data-bbox="539 491 1319 679" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> <b>Hinweis</b></p> <p>Wenn Sie die Einstellung <i>5GHz-Band bevorzugt</i> verwenden, müssen Sie in beiden Client-Bändern denselben Netzwerknamen (SSID) konfigurieren.</p> </div> <ul style="list-style-type: none"> <li>• <i>AP Steering (Access Point Steering)</i>: Beim Access Point Steering wird ein WLAN Client ggf. nicht nur in ein anderes Frequenzband, sondern auch an einen anderen Access Point verwiesen. Voraussetzung hierfür ist die Aktivierung von 802.11k/v.</li> </ul>
<b>Schneller BSS-Übergang (802.11r)</b>	802.11r ermöglicht auch bei stark verschlüsselten WLAN-Netzen eine unterbrechungsfreie Verbindung, wenn der WLAN-Client von einem zum einen anderen Access Point wechselt.
<b>Verwaltung der Funkressourcen (802.11k) und Netzwerkunterstütztes Roaming (802.11v)</b>	802.11k/v tauscht Informationen zwischen WLAN Clients und WLAN Access Points aus und steuert auf Basis dieser Informationen die Lastverteilung zwischen mehreren Access Points effizienter. Diese beiden Optionen werden in der Regel zusammen aktiviert, lassen sich aber auch getrennt voneinander konfigurieren. Dabei regelt 802.11v den Austausch der Informationen über die aktuelle Netzwerktopologie, während 802.11k das intelligente Client Roaming auf Basis der Topologiedaten regelt.

#### Felder im Menü MAC-Filter

Feld	Beschreibung
<b>Zugriffskontrolle</b>	<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>

Feld	Beschreibung
<b>Erlaubte Adressen</b>	Legen Sie Einträge mit <b>Hinzufügen</b> an und geben Sie die MAC-Adressen der Clients ( <b>MAC-Adresse</b> ) ein, die zugelassen werden sollen.
<b>Dynamische Black List</b>	<p>Mithilfe der Funktion <b>Dynamische Black List</b> 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 <b>Wireless LAN Controller-&gt;Monitoring-&gt;Rogue Clients</b> erfolgen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiviert.</p>
<b>Fehlversuche per Zeitraum</b>	<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 wird.</p> <p>Standardwerte sind <i>10</i> Fehlversuche in <i>60</i> Sekunden.</p>
<b>Sperrzeit für Black List</b>	<p>Geben Sie die Zeit ein, für die ein Eintrag in der dynamischen Black List gelten soll.</p> <p>Der Standardwert ist <i>500</i> Sekunden.</p>

**Felder im Menü VLAN**

Feld	Beschreibung
<b>VLAN</b>	<p>Wählen Sie aus, ob für dieses Drahtlosnetzwerk VLAN-Segmentierung verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
VLAN-ID	<p>Geben Sie den Zahlenwert ein, der das VLAN identifiziert.</p> <p>Mögliche Werte sind 2 bis 4094.</p> <p>VLAN ID 1 ist nicht möglich, da sie bereits verwendet wird.</p>

#### Felder im Menü Bandbreitenbeschränkung für jeden WLAN-Client

Feld	Beschreibung
Rx Shaping	<p>Wählen Sie die Begrenzung der Bandbreite in Empfangsrichtung.</p> <p>Mögliche Werte sind</p> <ul style="list-style-type: none"> <li>Keine Begrenzung (Standardwert)</li> <li>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.</li> </ul>
Tx Shaping	<p>Wählen Sie die Begrenzung der Bandbreite in Senderichtung.</p> <p>Mögliche Werte sind</p> <ul style="list-style-type: none"> <li>Keine Begrenzung (Standardwert)</li> <li>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.</li> </ul>

#### Felder im Menü Data-Rate Trimming

Feld	Beschreibung
Geschwindigkeitsprofil im 2,4-GHz-Band	<p>Mit Data-Rate Trimming können Sie bei Bedarf die WLAN-Leistung verbessern. Sie können niedrige Datenübertragungsraten blockieren und damit erzwingen, dass ausschließlich höhere Datenraten verwendet werden. Clients, die mit niedrigeren Übertragungsgeschwindigkeiten andere Clients behindern, werden vom Access Point abgemeldet.</p> <p>Wählen Sie das Profil mit den Geschwindigkeiten aus, das für die Clients freigegeben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>Alle (Min. 1 MBit/s) - Alle Clients, die eine Übertragungsgeschwindigkeit von 1 MBit/s aufrecht erhalten können, können sich am Access Point anmelden.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Min. 6 MBit/s (keine 802.11b-Geräte)</i>- s.o. für Clients mit 6 Mbit/s Mindestgeschwindigkeit; Clients, die nach dem veralteten Standard 802.11b arbeiten, werden nicht zugelassen.</li> <li>• <i>Min. 12 MBit/s (keine 802.11b-Geräte)</i>- s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit</li> <li>• <i>Min. 24 MBit/s (keine 802.11b-Geräte)</i>- s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit</li> </ul>
<b>Geschwindigkeitsprofil im 5-GHz-Band</b>	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Alle (Min. 6 MBit/s)</i> - Alle Clients, die eine Übertragungsgeschwindigkeit von 6 MBit/s aufrecht erhalten können, können sich am Access Point anmelden.</li> <li>• <i>Ab 12 MBit/s</i> - s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit</li> <li>• <i>Ab 24 MBit/s</i> - s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit</li> </ul>

#### Felder im Menü Unteren RSSI-Schwellwert verwalten

Feld	Beschreibung
<b>RSSI-Schwellwert</b>	<p>Mithilfe des Parameters RSSI Schwellwert können Sie einen Grenzwert für den Signalpegel definieren. Wenn ein Access Point „sieht“, dass einer seiner Clients länger als unter der Toleranzzeit angegeben diesen Signalpegel unterschreitet, stellt er die Kommunikation zu ihm ein. Der Client wird dadurch gezwungen, sich einen neuen Access Point zu suchen, d. h. zu prüfen, welcher Access Point das beste Signal liefert und sich mit ihm zu verbinden.</p> <p>Geben Sie den unteren RSSI-Schwellwert in dBm an. Wenn dieser Wert länger als unter der Toleranzzeit angegeben unterschritten wird, so stellt der Access Point die Kommunikation zum betroffenen Client ein.</p> <p>Der Standardwert ist <math>-110</math> dBm.</p>
<b>Toleranzzeit</b>	<p>Geben Sie die Zeit in Sekunden ein, während der die Datenübertragungsrate unter den RSSI-Schwellwert sinken darf, ohne dass der Client mit Konsequenzen rechnen muss.</p>

Feld	Beschreibung
	Der Standardwert ist 5 Sekunden.

## 13.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.



### Hinweis

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

### 13.4.1 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
<b>AP gefunden</b>	Zeigt die Anzahl der gefundenen Access Points an.
<b>AP offline</b>	Zeigt die Anzahl der Access Points an, die nicht mit dem Wireless LAN Controller verbunden sind.
<b>AP verwaltet</b>	Zeigt die Anzahl der verwalteten Access Points an.
<b>Access Points, die mit der aktuell installierten Lizenz verwaltet werden können</b>	bintec-elmeg-Geräte verfügen ab Werk über eine freie Lizenz zur Verwaltung von Access Points. Der Anzahl der verwaltbaren Access Points ist dabei von Gerätetyp zu Gerätetyp unterschiedlich.
<b>Maximal Anzahl an Access Points, die von diesem Gerät mit einer vollen Lizenz verwaltet werden können</b>	Aufgrund unterschiedlicher Hardwareausstattung können bintec-elmeg-Geräte eine bestimmte Anzahl von Access Points verwalten.
<b>WLAN Controller: VSS-Durchsatz</b>	Zeigt den empfangenen und den gesendeten Datenverkehr in Bytes pro Sekunde zeitabhängig an.
<b>CPU-Last [%]</b>	Zeigt die CPU-Auslastung in Prozent zeitabhängig an.
<b>Speicherverbrauch [%]</b>	Zeigt den Speicherverbrauch in Prozent zeitabhängig an.
<b>Verbundene Clients/</b>	Zeigt die Anzahl der verbundenen Clients pro Drahtlosnetzwerk

Status	Bedeutung
VSS	(VSS) zeitabhängig an.

## 13.4.2 Access Points

Im Menü **Wireless LAN Controller->Monitoring->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 **Access Points**.

### 13.4.2.1 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
<b>Durchsatz</b>	Zeigt den empfangenen und den gesendeten Datenverkehr pro Funkmodul zeitabhängig an.
<b>Verbundene Clients</b>	Zeigt die Anzahl der angeschlossenen Clients pro Funkmodul zeitabhängig an.

### 13.4.2.2 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
<b>Durchsatz/Client</b>	Zeigt den empfangenen und den gesendeten Datenverkehr pro Client zeitabhängig an.

## 13.4.3 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 Access Points, 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.
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.

### 13.4.4 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 Access Points, VSS, MAC-Adresse (VSS), Kanal, Status**).

### 13.4.5 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.



## 13.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Access Points und Clients.

### 13.5.1 Eigene Access Points

Dieses Menü zeigt Informationen über die vom Controller verwalteten Access Points an, wie sie sich gegenseitig "sehen". Dies liefert nützliche Informationen über das von den verwalteten Access Points gebildete Netzwerk und hilft Ihnen bei der Identifizierung potenzieller WLAN-Probleme.

Das Menü enthält Informationen wie den Namen des Access Points, den Kanal, auf dem er arbeitet, seine Signalstärke und wann er von welchem Access Point und auf welchem Kanal zuletzt gesehen wurde.

### 13.5.2 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.

### 13.5.3 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.

### 13.5.4 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->Access Point-Konfiguration ->Drahtlosnetzwerke (VSS)**. Sie können ebenfalls Einträge zur statischen Blacklist hinzufügen.

#### Mögliche Werte für Rogue Clients

Status	Bedeutung
<b>MAC-Adresse des Rogue Clients</b>	Zeigt die MAC-Adresse des Clients an, der sich auf der Blacklist befindet.
<b>Netzwerkname (SSID)</b>	Zeigt die beteiligten SSID an.
<b>Angegriffener Access</b>	Zeigt den betroffenen AP an.

Status	Bedeutung
<b>Point</b>	
<b>Signal dBm</b>	Zeigt die Signalstärke des Clients während des Zugriffsversuchs an.
<b>Art des Angriffs</b>	Hier wird die Art des möglichen Angriffs angezeigt, z. B. eine fehlerhafte Authentifizierung.
<b>Zuerst gesehen</b>	Zeigt die Zeit des ersten registrierten Zugriffsversuchs an.
<b>Zuletzt gesehen</b>	Zeigt die Zeit des letzten registrierten Zugriffsversuchs an.
<b>Statische Black List</b>	Sie können einen Rogue Client als nicht vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte <b>Statische Black List</b> aktivieren. Die Sperrung des Clients endet dann nicht automatisch, sondern muss von Ihnen manuell wieder aufgehoben werden.
<b>Löschen</b>	Mithilfe des  -Symbols können Sie Einträge löschen.

#### 13.5.4.1 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
<b>MAC-Adresse des Rogue Clients</b>	Geben Sie die MAC-Adresse des Clients ein, der der statischen Blacklist hinzugefügt werden soll.
<b>Netzwerkname (SSID)</b>	Wählen Sie das Drahtlosnetzwerk aus, von dem der Rogue Client ausgeschlossen werden soll.

## 13.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

### 13.6.1 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
<b>Image bereits vorhanden.</b>	Das Software Image ist bereits vorhanden, es ist kein Update nötig.
<b>Fehler</b>	Es ist ein Fehler aufgetreten..
<b>Wird ausgeführt</b>	Das Update wird gerade ausgeführt.
<b>Fertig</b>	Das Update ist beendet.

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

#### Felder im Menü Firmware-Wartung

Feld	Beschreibung
<b>Aktion</b>	<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"> <li>• <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware initiieren.</li> <li>• <i>Konfiguration mit Statusinformationen sichern</i>: Sie können eine Konfiguration sichern, welche Statusinformationen der APs enthält.</li> </ul>
<b>Quelle</b>	<p>Wählen Sie die Quelle für die Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>HTTP-Server</i> (Standardwert): Die Datei ist bzw. wird auf dem entfernten Server gespeichert, der in der <b>URL</b> angegeben wird.</li> <li>• <i>Aktuelle Software vom Update-Server</i>: Die Datei liegt auf dem offiziellen Update-Server. (Nur für <b>Aktion</b> =</li> </ul>

Feld	Beschreibung
	<p><i>Systemsoftware aktualisieren)</i></p> <ul style="list-style-type: none"><li>• <i>TFTP-Server</i>: Die Datei ist bzw. wird auf dem TFTP-Server gespeichert, der in der <b>URL</b> angegeben wird.</li></ul>
<b>URL</b>	<p>Nur für <b>Quelle</b> = <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>

## 14 Netzwerk

### 14.1 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.

#### 14.1.1 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,

##### 14.1.1.1 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
<b>Routentyp</b>	<p>Wählen Sie die Art der Route aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standardroute über Schnittstelle</i>: Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist.</li> <li>• <i>Standardroute über Gateway</i>: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist.</li> <li>• <i>Host-Route über Schnittstelle</i>: Route zu einem einzelnen Host über eine spezifische Schnittstelle.</li> <li>• <i>Host-Route via Gateway</i>: Route zu einem einzelnen Host über ein spezifisches Gateway.</li> <li>• <i>Netzwerkroute via Schnittstelle</i> (Standardwert): Route zu einem Netzwerk über eine spezifische Schnittstelle.</li> <li>• <i>Netzwerkroute via Gateway</i>: Route zu einem Netzwerk über ein spezifisches Gateway.</li> </ul> <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"> <li>• <i>Vorlage für Standardroute per DHCP</i>: Die Information, welches Gateway verwendet werden soll, wird per DHCP empfangen und in die Route übernommen.</li> <li>• <i>Vorlage für Host-Route per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Host ergänzt.</li> <li>• <i>Vorlage für Netzwerkroute per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Info-</li> </ul>

Feld	Beschreibung
	<p>mationen zu einem bestimmten Netzwerk ergänzt.</p> <div data-bbox="541 278 1319 568" style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;"> <p> <b>Hinweis</b></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>
<b>Schnittstelle</b>	Wählen Sie die Schnittstelle aus, welche für diese Route verwendet werden soll.
<b>Routenklasse</b>	<p>Wählen Sie die Art der <b>Routenklasse</b> aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (Standardwert): Definiert eine Route mit den Standardparametern.</li> <li>• <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.</li> </ul>

#### Felder im Menü Routenparameter

Feld	Beschreibung
<b>Lokale IP-Adresse</b>	<p>Nur für <b>Routentyp</b> = <i>Standardroute über Schnittstelle, Host-Route über Schnittstelle</i> <b>oder</b> <i>Netzwerkroute via Schnittstelle</i></p> <p>Geben Sie die eigene IP-Adresse des Routers auf der ausgewählten Schnittstelle ein.</p>
<b>Ziel-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Routentyp</b> <i>Host-Route über Schnittstelle</i> <b>oder</b> <i>Netzwerkroute via Schnittstelle</i></p> <p>Geben Sie die IP-Adresse des Ziel-Hosts bzw. Zielnetzes ein.</p>



Feld	Beschreibung
	<p>Bei <b>Routentyp</b> = <i>Netzwerkroute via Schnittstelle</i></p> <p>Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.</p>
<b>Gateway-IP-Adresse</b>	<p>Nur für <b>Routentyp</b> = <i>Standardroute über Gateway, Host-Route via Gateway</i> <b>oder</b> <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>
<b>Metrik</b>	<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
<b>Beschreibung</b>	Geben Sie eine Beschreibung für die IP-Route ein.
<b>Quellschnittstelle</b>	<p>Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen.</p> <p>Der Standardwert ist <i>Keine</i>.</p>
<b>Quell-IP-Adresse/Netzmaske</b>	Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.
<b>Layer 4-Protokoll</b>	<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>
<b>Quell-Port</b>	<p>Nur für <b>Layer 4-Protokoll</b> = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie den Quellport an.</p>

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


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


Feld	Beschreibung
	<p>bar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist.</p> <ul style="list-style-type: none"> <li>• <i>Verbindlich</i>: Die Route ist immer benutzbar.</li> <li>• <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.</li> <li>• <i>Nie einwählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist.</li> <li>• <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.</li> </ul>

## 14.1.2 Konfiguration von IPv6-Routen

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

### 14.1.2.1 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
<b>Beschreibung</b>	Geben Sie eine Beschreibung für die IPv6-Route an.
<b>Route aktiv</b>	<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>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
<b>Routentyp</b>	<p>Wählen Sie die Art der Route aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standardroute über Schnittstelle</i>: Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist.</li> <li>• <i>Standardroute über Gateway</i>: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist.</li> <li>• <i>Host-Route über Schnittstelle</i>: Route zu einem einzelnen Host über eine spezifische Schnittstelle.</li> <li>• <i>Host-Route via Gateway</i>: Route zu einem einzelnen Host über ein spezifisches Gateway.</li> <li>• <i>Netzwerkroute via Schnittstelle</i>: Route zu einem Netzwerk über eine spezifische Schnittstelle.</li> <li>• <i>Netzwerkroute via Gateway (Standardwert)</i>: Route zu einem Netzwerk über ein spezifisches Gateway.</li> </ul>
<b>Zielschnittstelle</b>	<p>Wählen Sie die IPv6-Schnittstelle aus, welche für diese Route verwendet werden soll.</p> <p>Sie können unter den Schnittstellen wählen, die unter <b>LAN-&gt;IP-Konfiguration-&gt;Schnittstellen-&gt;Neu</b> angelegt sind und für welche die Nutzung von IPv6 aktiviert ist.</p>
<b>Quelladresse/Länge</b>	<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>
<b>Zieladresse/Länge</b>	<p>Geben Sie die IPv6-Zieladresse 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>

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


### 14.1.3 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
<b>Ziel-IP-Adresse</b>	Zeigt die IP-Adresse des Ziel-Hosts bzw. Zielnetzes an.
<b>Netzmaske</b>	Zeigt die Netzmaske des Ziel-Hosts bzw. Zielnetzes an.
<b>Gateway</b>	Zeigt die Gateway IP-Adresse an. Im Falle von per DHCP erhaltenen Routen wird hier nichts angezeigt.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
<b>Metrik</b>	Zeigt die Priorität der Route an.  Je niedriger der Wert, desto höhere Priorität besitzt die Route.
<b>Routentyp</b>	Zeigt den Routentyp an.
<b>Erweiterte Route</b>	Zeigt an, ob eine Route mit erweiterten Parametern konfiguriert worden ist.
<b>Protokoll</b>	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell ( <i>Lokal</i> )

Feld	Beschreibung
	oder über eins der verfügbaren Protokolle.
<b>Löschen</b>	Mithilfe des  -Symbols können Sie Einträge löschen.

### 14.1.4 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
<b>Route</b>	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.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
<b>Metrik</b>	Zeigt die Priorität der Route an.  Je niedriger der Wert, desto höhere Priorität besitzt die Route.
<b>Protokoll</b>	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell ( <i>Lokal</i> ) oder über eins der verfügbaren Protokolle.

### 14.1.5 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
<b>Modus</b>	<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"> <li>• <i>Für alle Schnittstellen aktivieren</i>: Überprüfung der Rückroute wird für alle Schnittstellen aktiviert.</li> <li>• <i>Für bestimmte Schnittstellen aktivieren</i> (Standardwert): Eine Liste aller Schnittstellen wird angezeigt, in der Überprüfung der Rückroute nur für spezifische Schnittstellen aktiviert wird.</li> <li>• <i>Für alle Schnittstellen deaktivieren</i>: Überprüfung der Rückroute wird für alle Schnittstellen deaktiviert.</li> </ul>
<b>Nr.</b>	<p>Nur für <b>Modus</b> = <i>Für bestimmte Schnittstellen aktivieren</i></p> <p>Zeigt die laufende Nummer des Listeneintrags an.</p>
<b>Schnittstelle</b>	<p>Nur für <b>Modus</b> = <i>Für bestimmte Schnittstellen aktivieren</i></p> <p>Zeigt den Namen der Schnittstelle an.</p>
<b>Überprüfung der Rückroute</b>	<p>Nur für <b>Modus</b> = <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>

## 14.2 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 zugeteilten 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 zugeteilten 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 126 sowie die für IPv6 relevanten Parameter im Menü **LAN->IP-Konfiguration->Schnittstellen**).

## 14.2.1 Konfiguration eines Allgemeinen Präfixes

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

### 14.2.1.1 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
<b>Aktiver Allgemeiner Präfix</b>	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.
<b>Name</b>	Geben Sie einen Namen für das Allgemeine Präfix ein.  Ein sprechender Name dient dazu, das Allgemeine Präfix aus einer Präfixliste leichter auswählen zu können.
<b>Typ</b>	Wählen Sie, wie der Adressraum zugewiesen werden soll.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Dynamisch</i> (Standardwert): Der Allgemeine Präfix wird dynamisch mittels einer DHCP-Übertragung festgesetzt, z. B. von einem Provider.</li> <li>• <i>Statisch</i>: Das Präfix wird fest vorgegeben, z. B. durch</li> </ul>

Feld	Beschreibung
	einen Provider.
<b>Von Schnittstelle</b>	<p>Nur bei <b>Typ</b> = <i>Dynamisch</i></p> <p>Wählen Sie die IPv6-Schnittstelle aus, von welcher ein <b>Allgemeiner Präfix</b> bezogen werden soll.</p> <p>Sie können unter den Schnittstellen wählen, die unter <b>LAN-&gt;IP-Konfiguration-&gt;Schnittstellen-&gt;Neu</b> angelegt sind und die folgende Bedingungen erfüllen:</p> <ul style="list-style-type: none"> <li>• <b>IPv6</b> ist <i>Aktiviert</i>.</li> <li>• <b>IPv6-Modus</b> = <i>Host</i></li> <li>• <b>DHCP-Client</b> ist <i>Aktiviert</i>.</li> </ul>
<b>Benutzter Präfix/Länge</b>	<p>Nur bei <b>Typ</b> = <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>
<b>Präfixlänge</b>	<p>Für einen dynamisch bezogenen Präfix müssen Sie hier lediglich die Präfixlänge eingeben. Sie können die Länge des zugewiesenen Präfixes ggf. bei Ihrem Dienstanbieter erfragen. Standardmäßig ist hier eine Länge von <i>56</i> vorgegeben.</p>

## 14.3 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 198).

Konkrete Hinweise für die Konfiguration von NAT finden Sie am Ende des Kapitels unter [NAT - Konfigurationsbeispiel](#) auf Seite 204.

### 14.3.1 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
<b>NAT aktiv</b>	<p>Wählen Sie aus, ob NAT für die Schnittstelle aktiviert werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Loopback aktiv</b>	<p>Mithilfe der NAT-Loopback-Funktion ist Network Address Translation auch bei Anschlüssen möglich, auf denen NAT nicht aktiv ist. Dies wird verwendet, um Anfragen aus dem LAN so zu interpretieren, als ob sie aus dem WAN kämen. Sie können damit Server Services testen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Verwerfen ohne Rückmeldung</b>	<p>Wählen Sie aus, ob IP-Pakete stillschweigend durch NAT abgelehnt werden sollen. Ist diese Funktion deaktiviert, wird der Absender der abgelehnten IP-Pakete mit einer entsprechenden ICMP- oder TCP-RST-Nachricht informiert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>PPTP-Passthrough</b>	<p>Wählen Sie aus, ob auch bei aktiviertem NAT der Aufbau und Betrieb mehrerer gleichzeitiger ausgehender PPTP-Verbindungen von Hosts im Netzwerk erlaubt sein soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn <b>PPTP-Passthrough</b> aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpunkt konfiguriert werden.</p>
<b>Portweiterleitungen</b>	<p>Zeigt die Anzahl der in <b>Netzwerk-&gt;NAT-&gt;NAT-Konfiguration</b> konfigurierten Portweiterleitungsregeln an.</p>

## 14.3.2 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.

### 14.3.2.1 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
<b>Beschreibung</b>	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
<b>Schnittstelle</b>	<p>Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): NAT wird für alle Schnittstellen konfiguriert.</li> <li>• <i>&lt;Schnittstellename&gt;</i>: Wählen Sie eine der Schnittstellen aus der Liste aus.</li> </ul>
<b>Art des Datenverkehrs</b>	<p>Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>eingehend (Ziel-NAT)</i> (Standardwert): Der Datenverkehr, der von außen kommt.</li> <li>• <i>ausgehend (Quell-NAT)</i>: Der Datenverkehr, der nach außen geht.</li> <li>• <i>exklusiv (ohne NAT)</i>: Der Datenverkehr, der von NAT ausgenommen ist.</li> </ul>
<b>NAT-Methode</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i></p> <p>Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-</p>

Feld	Beschreibung
	<p>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"> <li>• <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.</li> <li>• <i>restricted-cone</i> (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen.</li> <li>• <i>port-restricted-cone</i> (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen.</li> <li>• <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.</li> </ul>

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
<p><b>Dienst</b></p>	<p>Nicht für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i> und <b>NAT-Methode</b> = <i>full-cone, restricted-cone</i> oder <i>port-restricted-cone</i>.</p> <p>Wählen Sie einen der vorkonfigurierten Dienste aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Benutzerdefiniert</i> (Standardwert)</li> <li>• <i>&lt;Dienstname&gt;</i></li> </ul>
<p><b>Aktion</b></p>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>exklusiv (ohne NAT)</i></p> <p>Wählen Sie, welche Datenpakete von NAT ausgenommen wer-</p>

Feld	Beschreibung
	<p>den.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Protokoll</b>	<p>Nur für bestimmte Dienste.</p> <p>Nicht für <b>Art des Datenverkehrs</b> = <i>ausgehend</i> (<i>Quell-NAT</i>) und <b>NAT-Methode</b> = <i>full-cone</i>, <i>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 <b>Dienst</b> stehen verschiedene Protokolle zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert)</li> <li>• <i>AH</i></li> <li>• <i>Chaos</i></li> <li>• <i>EGP</i></li> <li>• <i>ESP</i></li> <li>• <i>GGP</i></li> <li>• <i>GRE</i></li> <li>• <i>HMP</i></li> <li>• <i>ICMP</i></li> <li>• <i>IGMP</i></li> <li>• <i>IGP</i></li> <li>• <i>IGRP</i></li> <li>• <i>IP</i></li> <li>• <i>IPinIP</i></li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• IPv6</li> <li>• IPX in IP</li> <li>• ISO-IP</li> <li>• Kryptolan</li> <li>• L2TP</li> <li>• OSPF</li> <li>• PUP</li> <li>• RDP</li> <li>• RSVP</li> <li>• SKIP</li> <li>• TCP</li> <li>• TLSP</li> <li>• UDP</li> <li>• VRRP</li> <li>• XNS-IDP</li> </ul>
<b>Quell-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <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>
<b>Original Ziel-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>eingehend (Ziel-NAT)</i></p> <p>Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
<b>Original Ziel-Port/Bereich</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>eingehend (Ziel-NAT)</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i> und <b>Protokoll</b> = <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>
<b>Originale Quell-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i></p> <p>Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>

Feld	Beschreibung
<b>Original Quell-Port/Bereich</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i>, <b>NAT-Methode</b> = <i>symmetrisch</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i> und <b>Protokoll</b> = <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>
<b>Quell-Port/Bereich</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>exklusiv (ohne NAT)</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i> und <b>Protokoll</b> = <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>
<b>Ziel-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>exklusiv (ohne NAT)</i> bzw. <i>ausgehend (Quell-NAT)</i> und <b>NAT-Methode</b> = <i>symmetrisch</i></p> <p>Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
<b>Ziel-Port/Bereich</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i>, <b>NAT-Methode</b> = <i>symmetrisch</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i> und <b>Protokoll</b> = <i>TCP, UDP, TCP/UDP</i> oder <b>Art des Datenverkehrs</b> = <i>exklusiv (ohne NAT)</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i> und <b>Protokoll</b> = <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
<b>Neue Ziel-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <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>
<b>Neuer Ziel-Port</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>eingehend (Ziel-NAT)</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i> und <b>Protokoll</b> = <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>
<b>Neue Quell-IP-Adresse/Netzmaske</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i> und <b>NAT-Methode</b> = <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>
<b>Neuer Quell-Port</b>	<p>Nur für <b>Art des Datenverkehrs</b> = <i>ausgehend (Quell-NAT)</i>, <b>NAT-Methode</b> = <i>symmetrisch</i>, <b>Dienst</b> = <i>Benutzerdefiniert</i>, <b>Protokoll</b> = <i>TCP, UDP, TCP/UDP</i> und <b>Original Quell-Port/Bereich</b>= <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. Standardmäßig ist <i>Original</i> aktiv.</p> <p>Haben Sie für <b>Original Quell-Port/Bereich</b> <i>Portbereich angeben</i> gewählt, stehen folgende Auswahlmöglichkeiten zur Verfügung:</p>

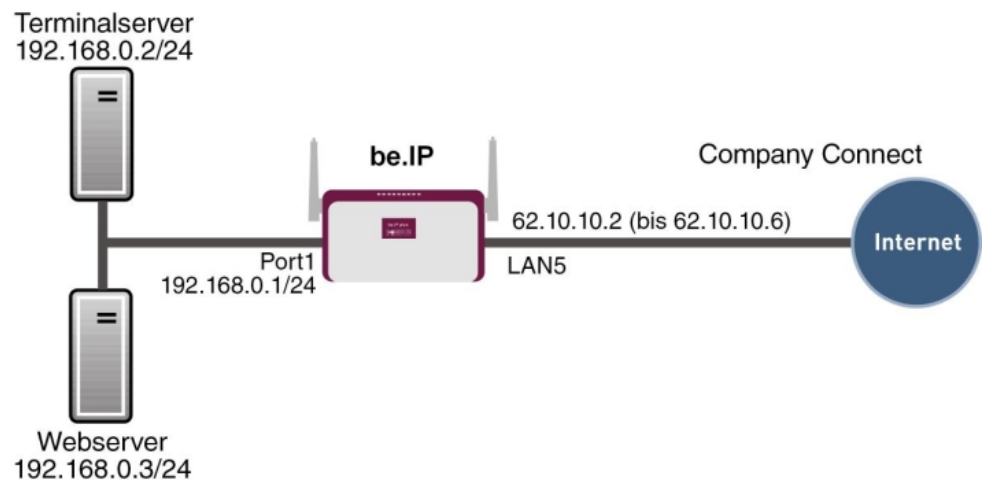
Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Original Quell-Port/Bereich verwenden</i>: Der in <b>Original Quell-Port/Bereich</b> angegebene Bereich wird nicht verändert, die Portnummern bleiben erhalten.</li> <li>• <i>Verwende Port/Bereich beginnend bei</i>: Es erscheint ein Eingabefeld, 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.</li> </ul>

### 14.3.3 NAT - Konfigurationsbeispiel

#### Voraussetzungen

- Grundkonfiguration des Gateways
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang, hier als Beispiel **Company Connect** mit acht IP-Adressen.
- Die Ethernet-Schnittstelle **LAN5** Ihres Geräts ist an den Zugangsrouter 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 **LAN5** 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-Freigabe für GUI

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
Protokoll	Netzwerk->NAT->NAT-Konfiguration->Neu	TCP
Quell IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Beliebig
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 62.10.10.2
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration->Neu	Port angeben, 80
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 127.0.0.1
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	Original deaktiviert, 80

### Webserver

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-	z. B. Webserver

Feld	Menü	Wert
	Konfiguration->Neu	
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
Quell-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Beliebig
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 62.10.10.3
Neue 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. Terminal-Server
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
Protokoll	Netzwerk->NAT->NAT-Konfiguration->Neu	TCP
Quell-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Beliebig
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	Host, z. B. 62.10.10.4
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration->Neu	Port angeben, 3389
Neue Ziel-	Netzwerk->NAT->NAT-	Host, z. B.

Feld	Menü	Wert
IP-Adresse/Netzmaske	Konfiguration->Neu	192.168.0.2
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	Original

## 14.4 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 214.

### 14.4.1 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.

#### 14.4.1.1 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
<b>Gruppenbeschreibung</b>	Geben Sie eine beliebige Beschreibung der Schnittstellen-Gruppe ein.
<b>Verteilungsrichtlinie</b>	<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"> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Berücksichtigen</b>	<p>Nur für <b>Verteilungsrichtlinie</b> = <i>Lastabhängige Bandbreite</i></p> <p>Wählen Sie aus, in welcher Richtung die aktuelle Datenrate berücksichtigt werden soll.</p> <p>Optionen:</p> <ul style="list-style-type: none"> <li>• <i>Download</i>: Nur die Datenrate in Empfangsrichtung wird berücksichtigt.</li> <li>• <i>Upload</i>: Nur die Datenrate in Senderichtung wird berücksichtigt.</li> </ul> <p>Standardmäßig sind die Optionen <i>Download</i> und <i>Upload</i> deaktiviert.</p>
<b>Verteilungsmodus</b>	Wählen Sie aus, welchen Zustand die Schnittstellen der Gruppe haben dürfen, damit sie in die Lastverteilung einbezogen werden.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Immer</i> (Standardwert): Auch Schnittstellen im Zustand ruhend werden einbezogen.</li> <li>• <i>Nur aktive Schnittstellen verwenden</i>: Es werden nur Schnittstellen im Zustand aktiv berücksichtigt.</li> </ul>

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
<b>Gruppenbeschreibung</b>	Zeigt die Beschreibung der Schnittstellen-Gruppe an.
<b>Verteilungsrichtlinie</b>	Zeigt die gewählte Art des Datenverkehrs an.

#### Felder im Menü Schnittstellenauswahl für Verteilung

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

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Routenselektor</b>	Der Parameter <b>Routenselektor</b> ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der

Feld	Beschreibung
	<p>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"> <li>• Ist eine Schnittstelle nur einer Lastverteilungsgruppe zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig.</li> <li>• Ist eine Schnittstelle mehreren Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich.</li> <li>• Innerhalb einer Lastverteilungsgruppe muss der Routenselektor aller Schnittstelleneinträge identisch konfiguriert sein.</li> </ul> <p>Wählen Sie die <b>Ziel-IP-Adresse</b> der gewünschten Route aus.</p> <p>Sie können unter allen Routen und allen erweiterten Routen wählen.</p>
<p><b>IP-Adresse zur Nachverfolgung</b></p>	<p>Mit dem Parameter <b>IP-Adresse zur Nachverfolgung</b> können Sie eine bestimmte Route überwachen lassen.</p> <p>Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die Konfiguration von Host-Überwachungseinträgen zwingend erforderlich. Konfiguriert werden kann dies im Menü <b>Lokale Dienste-&gt;Überwachung-&gt;Hosts</b>. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion <b>Überwachen</b> berücksichtigt werden. Über die Konfiguration der <b>IP-Adresse zur Nachverfolgung</b> im Menü <b>Lastverteilung-&gt;Lastverteilungsgruppen-&gt;Erweiterte Einstellungen</b> 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</p>



Feld	Beschreibung
	<p>soll.</p> <p>Sie können unter den IP-Adressen wählen, die Sie im Menü <b>Lo-kale Dienste-&gt;Überwachung-&gt;Hosts-&gt;Neu</b> unter <b>Überwachte IP-Adresse</b> eingegeben haben und die mit Hilfe des Feldes <b>Auszuführende Aktion</b> überwacht werden (<b>Aktion</b> = <i>Überwa-chen</i>).</p>

## 14.4.2 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 **Ziel-adresse** über dieselbe Schnittstelle wie das erste HTTPS-Paket geroutet.

### 14.4.2.1 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
<b>Admin-Status</b>	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.
<b>Beschreibung</b>	Geben Sie eine Bezeichnung für den Eintrag ein.
<b>Dienst</b>	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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>chargen</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> Der Standardwert ist <i>Benutzerdefiniert</i> .
<b>Protokoll</b>	Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
<b>Ziel-IP-Adresse/Netzmaske</b>	Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert)</li> </ul>

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

Feld	Beschreibung
	Der Standardwert ist <i>900</i> Sekunden.

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

#### Felder im Menü **Erweiterte Einstellungen**

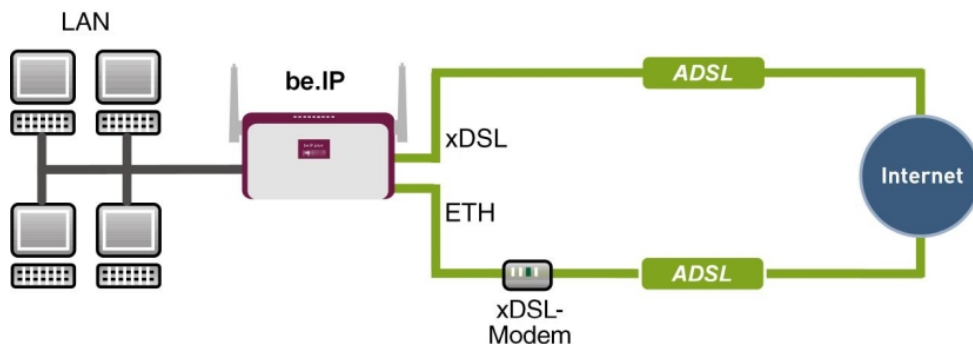
Feld	Beschreibung
<b>Unveränderliche Parameter</b>	<p>Legen Sie fest, ob die beiden Parameter <b>Zieladresse</b> und <b>Zielport</b> bei später gesendeten Datenpaketen denselben Wert haben müssen wie beim ersten Datenpaket, d. h. ob die nachfolgenden Datenpakete über denselben <b>Zielport</b> zur selben <b>Zieladresse</b> geroutet werden müssen.</p> <p>Standardmäßig sind die beiden Parameter <b>Zieladresse</b> und <b>Zielport</b> 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 <b>Quell-IP-Adresse</b> muss bei später gesendeten Datenpaketen immer denselben Wert haben wie beim ersten Datenpaket. Er kann daher nicht deaktiviert werden.</p>

### 14.4.3 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)

Feld	Menü	Wert
Benutzername	Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter	z. B. <i>fes-te_ip@provider.de</i>
Passwort	Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter	z. B. <i>test12345</i>



### 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	<i>Externes xDSL-Modem</i>
Beschreibung	Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter	z. B. <i>ADSL-2</i>
Physischer Ethernet-Port	Assistenten -> Internetzugang->Internetverbindungen->Neu->Weiter	z. B. <i>ETH5</i>
Typ	Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter	<i>Benutzerdefiniert</i>
Benutzername	Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter	z. B. <i>#0001@t-online.de</i>
Passwort	Assistenten->Internetzugang->Internetverbindunge->Neu->Weiter	z. B. <i>test12345</i>

### 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>

Feld	Menü	Wert
nis	lungsgruppen->Neu->Hinzufügen	
Schnittstelle	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	WAN_ADSL-2
Verteilungsverhältnis	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	50

### 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	900 Sekunden

## 14.5 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

### 14.5.1 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**.

#### 14.5.1.1 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
<b>Beschreibung</b>	Geben Sie die Bezeichnung des Filters an.
<b>Dienst</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>chargen</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>Der Standardwert ist <i>any</i>.</p>
<b>Protokoll</b>	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
<b>Typ</b>	<p>Nur für <b>Protokoll</b> = <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>
<b>Verbindungsstatus</b>	<p>Bei <b>Protokoll</b> = <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"> <li>• <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-</li> </ul>



Feld	Beschreibung
	<p>Verbindung öffnen würden.</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.</li> </ul>
<b>IPv4-Zieladresse/-netzmaske</b>	<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"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.</li> </ul>
<b>IPv6-Zieladresse/-länge</b>	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>
<b>Ziel-Port/Bereich</b>	<p>Nur für <b>Protokoll</b> = <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> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>-Alle-</i> (Standardwert): Der Zielport ist nicht näher spezifiziert.</li> <li>• <i>Port angeben</i>: Geben Sie einen Zielport ein.</li> <li>• <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.</li> </ul>
<b>IPv4-Quelladresse/-netzmaske</b>	<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"> <li>• <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Netzmaske</li> </ul>

Feld	Beschreibung
	<p>sind nicht näher spezifiziert.</p> <ul style="list-style-type: none"> <li>• <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die zugehörige Netzmaske ein.</li> </ul>
<b>IPv6-Quelladresse/-länge</b>	<p>Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Länge ist nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>
<b>Quell-Port/Bereich</b>	<p>Nur für <b>Protokoll</b> = <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"> <li>• <i>-Alle-</i> (Standardwert): Der Quellport ist nicht näher spezifiziert.</li> <li>• <i>Port angeben</i>: Geben Sie einen Quellport ein.</li> <li>• <i>Portbereich angeben</i>: Geben Sie einen Quellport-Bereich ein.</li> </ul>
<b>DSCP / Traffic Class Filter (Layer 3)</b>	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt.</li> <li>• <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).</li> <li>• <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</li> <li>• <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der</li> </ul>

Feld	Beschreibung
	<p>IP-Pakete verwendet (Angabe in hexadezimalen Format).</p> <ul style="list-style-type: none"> <li>• <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111.</li> <li>• <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63.</li> <li>• <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.</li> </ul>
<b>COS-Filter (802.1p/Layer 2)</b>	<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>

## 14.5.2 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.

### 14.5.2.1 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
<b>Klassenplan</b>	<p>Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an.</li> <li>• <i>&lt;Name des Klassenplans&gt;</i>: Zeigt einen bereits angelegten Klassenplan, den Sie auswählen und bearbeiten können.</li> </ul>

Feld	Beschreibung
	Sie können neue Filter hinzufügen.
<b>Beschreibung</b>	<p>Nur für <b>Klassenplan</b> = <i>Neu</i></p> <p>Geben Sie die Bezeichnung des Klassenplans ein.</p>
<b>Filter</b>	<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 <b>Netzwerk-&gt;QoS-&gt;QoS-Filter</b> konfiguriert sein.</p>
<b>Richtung</b>	<p>Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Eingehend</i>: Eingehende Datenpakete werden der im Folgenden zu definierenden Klasse (<b>Klassen-ID</b>) zugeordnet.</li> <li>• <i>Ausgehend</i> (Standardwert): Ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (<b>Klassen-ID</b>) zugeordnet.</li> <li>• <i>Beide</i>: Eingehende und ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (<b>Klassen-ID</b>) zugeordnet.</li> </ul>
<b>High-Priority-Klasse</b>	<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>
<b>Klassen-ID</b>	<p>Nur für <b>High-Priority-Klasse</b> nicht aktiv.</p> <p>Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zuweist.</p>

Feld	Beschreibung
	<div data-bbox="539 211 1315 399" style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;">  <p><b>Hinweis</b></p> <p>Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.)</p> </div> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 254.</p>
<p><b>DSCP/Traffic-Class-Filter setzen (Layer 3)</b></p>	<p>Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (<b>Klassen-ID</b>) setzen bzw. ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Erhalten</i> (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert.</li> <li>• <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format).</li> <li>• <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</li> <li>• <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format).</li> <li>• <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111.</li> <li>• <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63.</li> <li>• <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.</li> </ul>
<p><b>Setze COS Wert (802.1p/Layer 2)</b></p>	<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>
<p><b>Schnittstellen</b></p>	<p>Nur für <b>Klassenplan</b> = <i>Neu</i></p>

Feld	Beschreibung
	Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.

### 14.5.3 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.

#### 14.5.3.1 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
<b>Schnittstelle</b>	Wählen Sie die Schnittstelle aus, für die QoS konfiguriert werden soll.

Feld	Beschreibung
<b>Priorisierungsalgorithmus</b>	<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"> <li>• <i>Priority Queueing</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt.</li> <li>• <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.</li> <li>• <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.</li> <li>• <i>Deaktiviert</i> (Standardwert): QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.</li> </ul>
<b>Traffic Shaping</b>	<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>
<b>Maximale Upload-Geschwindigkeit</b>	<p>Nur für <b>Traffic Shaping</b> = aktiviert.</p> <p>Geben Sie für die ausgewählte Schnittstelle eine maximale Datenrate in kBit pro Sekunde in Senderichtung 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>
<b>Größe des Protokoll-Headers unterhalb Layer 3</b>	<p>Nur für <b>Traffic Shaping</b> = aktiviert.</p> <p>Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen</p>

Feld	Beschreibung
	<p>Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Benutzerdefiniert</i> Wert in Byte.</li> </ul> <p>Mögliche Werte sind 0 bis 100.</p> <ul style="list-style-type: none"> <li>• <i>Undefiniert (Protocol Header Offset=0) (Standardwert)</i></li> </ul> <p>Nur für Ethernet-Schnittstellen auswählbar</p> <ul style="list-style-type: none"> <li>• <i>Ethernet</i></li> <li>• <i>Ethernet und VLAN</i></li> <li>• <i>PPP over Ethernet</i></li> <li>• <i>PPPoE und VLAN</i></li> </ul> <p>Nur für IPSec-Schnittstellen auswählbar:</p> <ul style="list-style-type: none"> <li>• <i>IPSec über Ethernet</i></li> <li>• <i>IPSec über Ethernet und VLAN</i></li> <li>• <i>IPSec via PPP over Ethernet</i></li> <li>• <i>IPSec via PPPoE und VLAN</i></li> </ul>
<p><b>Verschlüsselungsmethode</b></p>	<p>Nur wenn als <b>Schnittstelle</b> ein IPSec Peer gewählt ist, <b>Traffic Shaping</b> <i>Aktiviert</i> ist und die <b>Größe des Protokoll-Headers unterhalb Layer 3</b> nicht <i>Undefiniert (Protocol Header Offset=0)</i> ist.</p> <p>Wählen Sie die Verschlüsselungsmethode, die für die IPSec-Verbindung genutzt wird. Der Verschlüsselungsalgorithmus bestimmt die Länge der Blockchiffre, die bei der Bandbreitenkalkulation berücksichtigt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>DES, 3DES, Blowfish, Cast - (Cipher-Blockgröße = 64 Bit)</i></li> <li>• <i>AES128, AES192, AES256, Twofish - (Cipher-Blockgröße = 128 Bit)</i></li> </ul>
<p><b>Real Time Jitter Con-</b></p>	<p>Nur für <b>Traffic Shaping</b> = aktiviert</p>



Feld	Beschreibung
<b>Real Time Jitter Control</b>	<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 (&lt; 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>
<b>Kontrollmodus</b>	<p>Nur für <b>Real Time Jitter Control</b> = aktiviert.</p> <p>Wählen Sie den Modus für die Optimierung der Sprachübertragung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt.</li> <li>• <i>Nur kontrollierte RTP-Streams</i>: Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gateway (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW.</li> <li>• <i>Immer</i>: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.</li> </ul>

#### Felder im Menü Queues/Richtlinie

Feld	Beschreibung
<b>Queues/Richtlinien</b>	<p>Konfigurieren Sie die gewünschten QoS-Queues.</p> <p>Für jede angelegte Klasse aus dem Klassenplan, die mit der ge-</p>

Feld	Beschreibung
	<p>wählten 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 <b>Hinzufügen</b> neue Einträge hinzu. Das Menü <b>Queue/Richtlinie bearbeiten</b> 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
<b>Beschreibung</b>	Geben Sie die Bezeichnung der Queue/Richtlinie an.
<b>Ausgehende Schnittstelle</b>	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
<b>Priorisierungsqueue</b>	<p>Wählen Sie den Typ für die Priorisierung der Queue aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Klassenbasiert</i> (Standardwert): Queue für "normal"-klassifizierte Daten.</li> <li>• <i>Hohe Priorität</i>: Queue für "high-priority"-klassifizierte Daten.</li> <li>• <i>Standard</i>: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.</li> </ul>
<b>Klassen-ID</b>	<p>Nur für <b>Priorisierungsqueue</b> = <i>Klassenbasiert</i></p> <p>Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll.</p> <p>Dazu muss vorher im Menü <b>Netzwerk-&gt;QoS-&gt;QoS-Klassifizierung</b> mindestens eine Klassen-ID vergeben worden sein.</p>
<b>Priorität</b>	Nur für <b>Priorisierungsqueue</b> = <i>Klassenbasiert</i>

Feld	Beschreibung
	<p>Wählen Sie die Priorität der Queue. Mögliche Werte sind <i>1</i> (<i>hohe Priorität</i>) bis <i>254</i> (<i>niedrige Priorität</i>).</p> <p>Der Standardwert ist <i>1</i>.</p>
<b>Gewichtung</b>	<p>Nur für <b>Priorisierungsalgorithmus</b> = <i>Weighted Round Robin</i> oder <i>Weighted Fair Queueing</i></p> <p>Wählen Sie die Gewichtung der Queue. Mögliche Werte sind <i>1</i> bis <i>254</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
<b>RTT-Modus (Realtime-Traffic-Modus)</b>	<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>
<b>Traffic Shaping</b>	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung.</p> <p>Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.)</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Maximale Upload-Geschwindigkeit</b>	<p>Nur für <b>Traffic Shaping</b> = aktiviert.</p> <p>Geben Sie eine maximale Datenrate in kBit pro Sekunde für die ausgewählte Schnittstelle ein.</p>

Feld	Beschreibung
	<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>
<b>Überbuchen zugelassen</b>	<p>Nur für <b>Traffic Shaping</b> = aktiviert.</p> <p>Aktivieren oder deaktivieren Sie die Funktion. Die Funktion steuert das Bandbreitenbegrenzungsverhalten.</p> <p>Bei aktiviertem <b>Überbuchen zugelassen</b> kann die Bandbreitenbegrenzung überschritten werden, die für die Queue eingestellt ist, sofern freie Bandbreite auf der Schnittstelle vorhanden ist.</p> <p>Bei deaktiviertem <b>Überbuchen zugelassen</b> 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>
<b>Burst-Größe</b>	<p>Nur für <b>Traffic Shaping</b> = 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
<b>Dropping-Algorithmus</b>	<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"> <li>• <i>Tail Drop</i> (Standardwert): Das neu hinzugekommene Pa-</li> </ul>

Feld	Beschreibung
	<p>ket wird verworfen.</p> <ul style="list-style-type: none"> <li>• <i>Head Drop</i>: Das älteste Paket in der Queue wird verworfen.</li> <li>• <i>Random Drop</i>: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.</li> </ul>
<b>Vermeidung von Datenstau (RED)</b>	<p>Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen.</p> <p>Pakete, deren Datengröße zwischen <b>Min. Queue-Größe</b> und <b>Max. Queue-Größe</b> 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>
<b>Min. Queue-Größe</b>	<p>Geben Sie den unteren Schwellwert für das Verfahren <b>Vermeidung von Datenstau (RED)</b> in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 0.</p>
<b>Max. Queue-Größe</b>	<p>Geben Sie den oberen Schwellwert für das Verfahren <b>Vermeidung von Datenstau (RED)</b> in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 16384.</p>

## 14.6 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 Zu-

gangsentscheidung 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.

## 14.6.1 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.

### 14.6.1.1 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
<b>Beschreibung</b>	Geben Sie eine Bezeichnung für das Filter ein.
<b>Dienst</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>chargen</i></li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>Der Standardwert ist <i>any</i>.</p>
<b>Protokoll</b>	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
<b>Typ</b>	<p>Nur bei <b>Protokoll</b> = <i>ICMP</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i></li> <li>• <i>Echo reply</i></li> <li>• <i>Destination unreachable</i></li> <li>• <i>Source quench</i></li> <li>• <i>Redirect</i></li> <li>• <i>Echo</i></li> <li>• <i>Time exceeded</i></li> <li>• <i>Timestamp</i></li> <li>• <i>Timestamp reply</i></li> </ul> <p>Der Standardwert ist <i>Beliebig</i>.</p> <p>Siehe RFC 792.</p>
<b>Verbindungsstatus</b>	<p>Nur bei <b>Protokoll</b> = <i>TCP</i></p> <p>Sie können ein Filter definieren, das den Status von TCP-Verbindung berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.</li> <li>• <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-</li> </ul>



Feld	Beschreibung
	Verbindung öffnen würden.
<b>IPv4-Zieladresse/-netzmaske</b>	<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"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.</li> </ul>
<b>IPv6-Zieladresse/-länge</b>	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>
<b>Ziel-Port/Bereich</b>	<p>Nur bei <b>Protokoll</b> = <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"> <li>• <i>-Alle-</i> (Standardwert): Das Filter gilt für alle Port-Nummern</li> <li>• <i>Port angeben</i>: Ermöglicht Eingabe einer Port-Nummer.</li> <li>• <i>Portbereich angeben</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern.</li> </ul>
<b>IPv4-Quelladresse/-netzmaske</b>	<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"> <li>• <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die</li> </ul>

Feld	Beschreibung
	Präfixlänge ein.
<b>IPv6-Quelladresse/-länge</b>	<p>Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>
<b>Quell-Port/Bereich</b>	<p>Nur bei <b>Protokoll</b> = <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"> <li>• <i>-Alle-</i> (Standardwert): Das Filter gilt für alle Port-Nummern</li> <li>• <i>Port angeben</i>: Ermöglicht Eingabe einer Port-Nummer.</li> <li>• <i>Portbereich angeben</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern.</li> </ul>
<b>DSCP / Traffic Class Filter (Layer 3)</b>	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt.</li> <li>• <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).</li> <li>• <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</li> <li>• <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format).</li> <li>• <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111.</li> <li>• <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen For-</li> </ul>


Feld	Beschreibung
	<p>mat angegeben, z. B. 63.</p> <ul style="list-style-type: none"> <li>• <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.</li> </ul>
<b>COS-Filter (802.1p/Layer 2)</b>	<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>

## 14.6.2 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.

### 14.6.2.1 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
<b>Regelkette</b>	<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"> <li>• <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an.</li> <li>• <i>&lt;Name der Regelkette&gt;</i>: Wählen Sie eine bereits angelegte Regelkette aus und fügen ihr somit eine weitere Regel hinzu.</li> </ul>
<b>Beschreibung</b>	Geben Sie die Bezeichnung der Regelkette ein.
<b>Zugriffsfiler</b>	Wählen Sie ein IP-Filter aus.

Feld	Beschreibung
	<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>
<b>Aktion</b>	<p>Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Zulassen, wenn Filter passt</i> (Standardwert): Paket annehmen, wenn das Filter passt.</li> <li>• <i>Zulassen, wenn Filter nicht passt</i>: Paket annehmen, wenn das Filter nicht passt.</li> <li>• <i>Verweigern, wenn Filter passt</i>: Paket abweisen, wenn das Filter passt.</li> <li>• <i>Verweigern, wenn Filter nicht zutrifft</i>: Paket abweisen, wenn das Filter nicht passt.</li> <li>• <i>Nicht beachten</i>: Nächste Regel anwenden.</li> </ul>


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.

### 14.6.3 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.

#### 14.6.3.1 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
<b>Schnittstelle</b>	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
<b>Regelkette</b>	Wählen Sie eine Regelkette aus.
<b>Verwerfen ohne Rückmeldung</b>	<p>Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll.</p> <ul style="list-style-type: none"> <li>• <i>Aktiviert</i> (Standardwert) : Der Absender wird nicht informiert.</li> <li>• <i>Deaktiviert</i>: Der Absender erhält eine ICMP-Nachricht.</li> </ul>
<b>Berichtsmethode</b>	<p>Legen Sie fest, ob bei Abweisung eines IP-Paketes eine Syslog-Meldung erzeugt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Kein Bericht</i>: Keine Syslog-Meldung.</li> <li>• <i>Info</i> (Standardwert): Eine Syslog-Meldung mit Angabe von Protokollnummer, Quell-IPAdresse und Quell-Port-Nummer wird generiert.</li> <li>• <i>Dump</i>: Eine Syslog-Meldung mit dem Inhalt der ersten 64 Bytes des abgewiesenen Pakets wird generiert.</li> </ul>

## 15 Multicast

### Was ist Multicasting?

Viele jüngere Kommunikations-Technologien basieren auf der Kommunikation von einem Sender zu mehreren Empfängern. Daher liegt auf der Reduzierung des Datenverkehrs ein Hauptaugenmerk von modernen Telekommunikationssystemen wie Voice-over-IP oder Video- und Audio-Streaming (z. B. IPTV oder Webradio), z. B. im Rahmen von TriplePlay (Voice, Video, Daten). Multicast bietet eine kostengünstige Lösung zur effektiven Bandbreitennutzung, dadurch dass der Sender das Datenpaket, welches mehrere Empfänger empfangen können, nur einmal senden muss. Dabei wird an eine virtuelle Adresse gesendet, die als Multicast-Gruppe bezeichnet wird. Interessierte Empfänger melden sich bei diesen Gruppen an.

### Weitere Anwendungsbereiche

Ein klassischer Einsatzbereich von Multicast sind Konferenzen (Audio/Video) mit mehreren Empfängern. Allen voran dürften die bekanntesten Mbone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) und das Whiteboard (WB) sein. Mit Hilfe von VAT können Audiokonferenzen durchgeführt werden. Hierzu werden alle Gesprächspartner in einem Fenster sichtbar gemacht und der/die Sprecher mit einem schwarzen Kasten gekennzeichnet. Andere Anwendungsgebiete sind vor allem für Firmen interessant. Hier bietet Multicasting die Möglichkeit, die Datenbanken mehrerer Server gleichzeitig zu synchronisieren, was für multinationale oder auch für Firmen mit nur wenigen Standorten lohnenswert ist.

### Adressbereich für Multicast

Für IPv4 sind im Klasse-D-Netzwerk die IP-Adressen 224.0.0.0 bis 239.255.255.255 (224.0.0.0/4) für Multicast reserviert. Eine IP-Adresse aus diesem Bereich repräsentiert eine Multicast-Gruppe, für die sich mehrere Empfänger anmelden können. Der Multicast-Router leitet dann gewünschte Pakete in alle Subnetze mit angemeldeten Empfängern weiter.

### Multicast Grundlagen

Multicast ist verbindungslos, d. h. eine etwaige Fehlerkorrektur oder Flusskontrolle muss auf Applikationsebene gewährleistet werden.

Auf der Transportebene kommt fast ausschließlich UDP zum Einsatz, da es im Gegensatz

zu TCP nicht an eine Punkt-zu-Punkt-Verbindung angelehnt ist.

Der wesentliche Unterschied besteht somit auf IP-Ebene darin, dass die Zieladresse keinen dedizierten Host adressiert, sondern an eine Gruppe gerichtet ist, d. h. beim Routing von Multicast-Paketen ist allein entscheidend, ob sich in einem angeschlossenen Subnetz ein Empfänger befindet.

Im lokalen Netzwerk sind alle Hosts angehalten, alle Multicast-Pakete zu akzeptieren. Das basiert bei Ethernet oder FDD auf einem sogenannten MAC-Mapping, bei dem die jeweilige Gruppen-Adresse in die Ziel-MAC-Adresse kodiert wird. Für das Routing zwischen mehreren Netzen müssen sich bei den jeweiligen Routern vorerst alle potentiellen Empfänger im Subnetz bekannt machen. Dies geschieht durch sog. Membership-Management-Protokolle wie IGMP bei IPv4 und MLP bei IPv6.

## Membership-Management-Protokoll

IGMP (Internet Group Management Protocol) ist in IPv4 ein Protokoll, mit dem Hosts dem Router Multicast-Mitgliedsinformationen mitteilen können. Hierbei werden für die Adressierung IP-Adressen des Klasse-D-Adressraums verwendet. Eine IP-Adresse dieser Klasse repräsentiert eine Gruppe. Ein Sender (z. B. Internetradio) sendet an diese Gruppe. Die Adressen (IP) der verschiedenen Sender innerhalb einer Gruppe werden als Quell(-Adressen) bezeichnet. Es können somit mehrere Sender (mit unterschiedlichen IP-Adressen) an dieselbe Multicast-Gruppe senden. So kommt eine 1-zu-n-Beziehung zwischen Gruppen- und Quelladressen zustande. Diese Informationen werden an den Router über Reports weitergegeben. Ein Router kann bei eingehenden Multicast-Datenverkehr anhand dieser Informationen entscheiden, ob ein Host in seinem Subnetz diesen empfangen will oder nicht. Ihr Gerät unterstützt die aktuelle Version IGMP V3, welche abwärtskompatibel ist, d. h. es können sowohl V3- als auch V1- und V2-Hosts verwaltet werden.

Ihr Gerät unterstützt folgende Multicast-Mechanismen:

- Forwarding (Weiterleiten): Dabei handelt es sich um statisches Forwarding, d.h. eingehender Datenverkehr für eine Gruppe wird auf jeden Fall weitergeleitet. Dies bietet sich an, wenn Multicast-Datenverkehr permanent weitergeleitet werden soll.
- IGMP: Mittels IGMP werden Informationen über die potentiellen Empfänger in einem Subnetz gesammelt. Bei einem Hop kann dadurch eingehender Multicast-Datenverkehr ausgesondert werden.



### Tipp

Bei Multicast liegt das Hauptaugenmerk auf dem Ausschluss von Datenverkehr ungewünschter Multicast-Gruppen. Beachten Sie daher, dass bei einer etwaigen Kombination von Forwarding mit IGMP die Pakete an die im Forwarding angegebenen Gruppen auf jeden Fall weitergeleitet werden können.

## 15.1 Allgemein

### 15.1.1 Allgemein

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

Das Menü besteht aus den folgenden Feldern:

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Multicast-Routing</b>	Wählen Sie aus, ob <b>Multicast-Routing</b> verwendet werden soll.  Mit <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion nicht aktiv.

## 15.2 IGMP

Mit IGMP (Internet Group Management Protocol, siehe RFC 3376) werden die Informationen über die Gruppen (zugehörigkeit) in einem Subnetz signalisiert. Somit gelangen nur diejenigen Pakete in das Subnetz, die explizit von einem Host gewünscht sind.

Spezielle Mechanismen sorgen für die Vereinigung der Wünsche der einzelnen Clients. Derzeit gibt es drei Versionen von IGMP (V1 - V3), wobei aktuelle Systeme meist V3, seltener V2, benutzen.

Bei IGMP spielen zwei Paketarten die zentrale Rolle: Queries und Reports.


Queries werden ausschließlich von einem Router versendet. Sollten mehrere IGMP-Router in einem Netzwerk existieren, so wird der Router mit der niedrigeren IP-Adresse der sogenannte Querier. Hierbei unterscheidet man das General Query (versendet an 224.0.0.1), die Group-Specific Query (versendet an jeweilige Gruppenadresse) und die Group-and-Source-Specific Query (versendet an jeweilige Gruppenadresse). Reports werden ausschließlich von Hosts versendet, um Queries zu beantworten.

### 15.2.1 IGMP

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



### 15.2.1.1 Bearbeiten oder Neu

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

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

#### Felder im Menü IGMP-Einstellungen

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

### 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
<b>IGMP Proxy</b>	Wählen Sie aus, ob Ihr Gerät die IGMP-Meldungen der Hosts im Subnetz über seine definierte <b>Proxy-Schnittstelle</b> weiterleiten soll.
<b>Proxy-Schnittstelle</b>	<p>Nur für <b>IGMP Proxy</b> = aktiviert</p> <p>Wählen Sie die Schnittstelle Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen.</p>
<b>Fallback-</b>	Nur für <b>IGMP Proxy</b> = aktiviert

Feld	Beschreibung
<b>Proxy-Schnittstelle 1</b>	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 <b>Proxy-Schnittstelle</b> nicht ausgeführt werden kann.
<b>Fallback-Proxy-Schnittstelle 2</b>	Nur für <b>IGMP Proxy</b> = 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 <b>Fallback-Proxy-Schnittstelle 1</b> nicht ausgeführt werden kann.

## 15.2.2 Optionen

In diesem Menü haben Sie die Möglichkeit, IGMP auf Ihrem System zu aktivieren bzw. zu deaktivieren. Außerdem können Sie bestimmen, ob IGMP im Kompatibilitätsmodus verwendet werden soll oder nur IGMP V3-Hosts akzeptiert werden sollen.

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

### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>IGMP-Status</b>	Wählen Sie den IGMP-Status aus.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Auto</i> (Standardwert): Multicast wird für Hosts automatisch eingeschaltet, wenn diese Anwendungen öffnen, die Multicast verwenden.</li> <li>• <i>Aktiv</i>: Multicast ist immer aktiv.</li> <li>• <i>Inaktiv</i>: Multicast ist immer inaktiv.</li> </ul>
<b>Modus</b>	Nur für <b>IGMP-Status</b> = <i>Aktiv</i> oder <i>Auto</i>  Wählen Sie den Multicast-Modus aus.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Kompatibilitätsmodus</i> (Standardwert): Der Router verwendet IGMP Version 3. Bemerkt er eine niedrigere Version im Netz, verwendet er die niedrigste Version, die er erkennen konnte.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Nur Version 3</i>: Nur IGMP Version 3 wird verwendet.</li> </ul>
<b>Maximale Gruppen</b>	<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>
<b>Maximale Quellen</b>	<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>
<b>Maximale Anzahl der IGMP-Statusmeldungen</b>	<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>

Der Abschnitt **Erweiterte Einstellungen** ermöglicht es, die Funktion des IGMP Snooping an- und auszuschalten. IGMP Snooping stellt sicher, dass Multicast-Datenverkehr nur an diejenigen Clients gesendet wird, die einen bestimmten Multicast Stream auch angefordert haben.

Die Funktion ist standardmäßig aktiv.

## 15.3 Weiterleiten

### 15.3.1 Weiterleiten

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

#### 15.3.1.1 Neu

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

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

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Alle Multicast-Gruppen</b>	<p>Wählen Sie aus, ob alle Multicast-Gruppen, d. h. der komplette Multicast-Adressraum 224.0.0.0/4, von der definierten <b>Quellschnittstelle</b> an die definierte <b>Zielschnittstelle</b> weitergeleitet werden soll. Setzen Sie dazu den Haken für <i>Aktiviert</i>.</p> <p>Möchten Sie nur eine definierte Multicast-Gruppe an eine bestimmte Schnittstelle weiterleiten, deaktivieren Sie die Option.</p> <p>Standardmäßig ist die Option nicht aktiv.</p>
<b>Multicast-Gruppen-Adresse</b>	<p>Nur für <b>Alle Multicast-Gruppen</b> = nicht aktiv</p> <p>Geben Sie hier die Adresse der Multicast-Gruppe ein, die Sie von einer definierten <b>Quellschnittstelle</b> an eine definierte <b>Zielschnittstelle</b> weiterleiten möchten.</p>
<b>Quellschnittstelle</b>	<p>Wählen Sie die Schnittstelle Ihres Geräts aus, an dem die gewünschte Multicast-Gruppe eingeht.</p>
<b>Zielschnittstelle</b>	<p>Wählen Sie die Schnittstelle Ihres Geräts aus, zu der die gewünschte Multicast-Gruppe weitergeleitet werden soll.</p>

## 16 WAN

Dieses Menü stellt Ihnen verschiedene Möglichkeiten zur Verfügung, Zugänge bzw. Verbindungen aus Ihrem LAN zum WAN zu konfigurieren. Außerdem können Sie hier die Sprachübertragung bei Telefongesprächen über das Internet optimieren.

### 16.1 Internet + Einwählen

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

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

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

Wenn Sie einen Internetzugang herstellen wollen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider (ISP) einrichten. Für Breitband-Internetzugänge stellt Ihr Gerät die Protokolle PPP-over-Ethernet (PPPoE), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung.



#### Hinweis

Beachten Sie die Vorgaben Ihres Providers!

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
<input type="checkbox"/>	nicht verbunden (Wählverbindung); Verbindungsaufbau möglich
<input type="checkbox"/>	nicht verbunden (z. B. ist aufgrund eines Fehlers beim Aufbau einer ausgehenden Verbindung ein erneuter Versuch erst nach

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

## 16.1.1 PPPoE

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

PPP over Ethernet (PPPoE) ist die Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird heute bei ADSL-Anschlüssen in Deutschland verwendet. In Österreich wurde ursprünglich für ADSL-Zugänge das Point To Point Tunneling Protocol (PPTP) verwendet. Mittlerweile wird allerdings PPPoE auch dort von einigen Providern angeboten.

### 16.1.1.1 Neu

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

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

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Beschreibung</b>	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.
<b>PPPoE-Modus</b>	<p>Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE ( <i>Standard</i> ) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll ( <i>Mehrfachverbindung</i> ). Wählen Sie <i>Mehrfachverbindung</i>, so können Sie mehrere DSL-Verbindungen eines Providers über PPP als statische Bündel koppeln, um mehr Bandbreite zu erhalten. Jede dieser DSL-Verbindungen sollte dafür eine separate Ethernet-Verbindung nutzen. Aktuell ist bei vielen Providern die Funktion PPPoE Multilink erst in Vorbereitung.</p> <p>Wir empfehlen Ihnen, für PPPoE Multilink den Ethernet Switch Ihres Geräts im Split-Port-Modus zu betreiben und für jede PPPoE-Verbindung eine eigene Ethernet-Schnittstelle zu benutzen, z. B. <i>en1-1</i>, <i>en1-2</i>.</p>

Feld	Beschreibung
	<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><b>PPPoE-Ethernet-Schnittstelle</b></p>	<p>Nur für <b>PPPoE-Modus</b> = <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 <b>WAN-&gt;ATM-&gt;Profile-&gt;Neu</b> 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 <b>ATM</b> eine Schnittstelle angelegt sein muss, für einen VDSL-Zugang ist dies nicht notwendig.</p>
<p><b>PPPoE-Schnittstelle für Mehrfachlink</b></p>	<p>Nur für <b>PPPoE-Modus</b>= <i>Mehrfachverbindung</i></p> <p>Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die <b>Hinzufügen</b>-Schaltfläche, um weitere Einträge anzulegen.</p>
<p><b>Benutzername</b></p>	<p>Geben Sie den Benutzernamen ein.</p>
<p><b>Passwort</b></p>	<p>Geben Sie das Passwort ein.</p>
<p><b>VLAN</b></p>	<p>Einige Internet Service Provider erfordern eine VLAN-ID. Aktivieren Sie diese Funktion, um unter <b>VLAN-ID</b> einen Wert eingeben zu können.</p>
<p><b>VLAN-ID</b></p>	<p>Nur wenn <b>VLAN</b> aktiviert ist.</p> <p>Geben Sie die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.</p>
<p><b>Immer aktiv</b></p>	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p>



Feld	Beschreibung
	<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>
<b>Timeout bei Inaktivität</b>	<p>Nur wenn <b>Immer aktiv</b> 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
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> <li>• <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.</li> </ul> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <a href="#">Firewall</a> auf Seite 343 konfigurieren.</p>
<b>IP-Adressmodus</b>	<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>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse.</li> <li>• <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.</li> </ul>
<b>Standardroute</b>	<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>
<b>NAT-Eintrag erstellen</b>	<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>
<b>Lokale IP-Adresse</b>	<p>Nur bei <b>IP-Adressmodus</b> = <i>Statisch</i></p> <p>Geben Sie die statische IP-Adresse des Verbindungspartners ein.</p>
<b>Routeneinträge</b>	<p>Nur bei <b>IP-Adressmodus</b> = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit <b>Hinzufügen</b> neue Einträge hinzu.</p> <ul style="list-style-type: none"> <li>• <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes.</li> <li>• <i>Netzmaske</i>: Netzmaske zu <b>Entfernte IP-Adresse</b>. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske.</li> <li>• <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.</li> </ul>

#### Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
<b>IPv6</b>	<p>Wählen Sie aus, ob die gewählte PPPoE- Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p>

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Sicherheitsrichtlinie</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> </ul> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> </ul> <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 343 konfigurieren.</p>
<b>IPv6-Modus</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Die gewählte PPPoE-Schnittstelle wird im Host-Modus betrieben.</p>
<b>Router Advertisement annehmen</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i> und <b>IPv6-Modus</b> = <i>Host</i></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>
<b>DHCP-Client</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i> und <b>IPv6-Modus</b> = <i>Host</i></p> <p>Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll.</p>

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>IPv6-Adressen</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Sie können der gewählten Schnittstelle <b>IPv6-Adressen</b> zuordnen.</p> <p>Mit <b>Hinzufügen</b> können Sie einen oder mehrere Adresseinträge 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 (<b>IPv6-Modus</b> = <i>Host</i>, <b>Router Advertisement annehmen</b> <i>Aktiviert</i> und <b>DHCP-Client</b> <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 (<b>IPv6-Modus</b> = <i>Router</i> (<i>Router-Advertisement übermitteln</i>), <b>Router Advertisement übertragen</b> <i>Aktiviert</i> und <b>DHCP-Server</b> <i>Aktiviert</i>), so müssen Sie hier seine IPv6-Adressen konfigurieren.</p>

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

#### Felder im Menü Link-Präfix

Feld	Beschreibung
<b>Art der Einrichtung</b>	<p>Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Von Allgemeinem Präfix</i> (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet.</li> <li>• <i>Statisch</i>: Sie können den Link-Präfix eingeben.</li> </ul>
<b>Allgemeiner Präfix</b>	<p>Nur für <b>Art der Einrichtung</b> = <i>Von Allgemeinem Präfix</i></p>

Feld	Beschreibung
	<p>Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter <b>Netzwerk-&gt;Allgemeine IPv6-Präfixe-&gt;Konfiguration eines Allgemeinen Präfixes-&gt;Neu</b> angelegt sind.</p>
<b>Automatische Subnetzerstellung</b>	<p>Nur wenn <b>Art der Einrichtung</b> = <i>Von Allgemeinem Präfix</i> und wenn ein <b>Allgemeiner Präfix</b> gewählt ist.</p> <p>Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID <i>0</i> verwendet, für das zweite Subnetz die Subnetz-ID <i>1</i>, usw.</p> <p>Mögliche Werte für die <b>Subnetz-ID</b> sind <i>0</i> bis <i>65535</i>.</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> <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>
<b>Subnetz-ID</b>	<p>Nur wenn <b>Automatische Subnetzerstellung</b> 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 <i>0</i> bis <i>65535</i>.</p> <p>Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.</p>
<b>Link-Präfix</b>	<p>Nur für <b>Art der Einrichtung</b> = <i>Statisch</i></p> <p>Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit <i>::</i> enden. Seine Länge ist mit <i>64</i> vorgegeben.</p>

**Felder im Menü Host-Adresse**

Feld	Beschreibung
<b>Erzeugungsmethode</b>	<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"> <li>• Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt.</li> <li>• In die entstandene Lücke wird <i>FFFF</i> eingefügt, um 64 Bit zu erhalten.</li> <li>• Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt.</li> <li>• Im ersten 8-Bit-Feld wird Bit 7 auf <i>1</i> gesetzt.</li> </ul>
<b>Statische Adressen</b>	<p>Sie können, unabhängig von der automatischen Erzeugung, die unter <b>Erzeugungsmethode</b> festgelegt ist, mit <b>Hinzufügen</b> 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></p>

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>Blockieren nach Verbindungsfehler für</b>	<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>
<b>Maximale Anzahl der erneuten Einwählversuche</b>	<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>
<b>Authentifizierung</b>	<p>Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen.</li> <li>• <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen.</li> <li>• <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen.</li> <li>• <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen.</li> <li>• <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.)</li> <li>• <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen.</li> <li>• <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.</li> </ul>
<p><b>DNS-Aushandlung</b></p>	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für <b>Primärer DNS-Server</b> und <b>Sekundärer DNS-Server</b> vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p><b>TCP-ACK-Pakete priorisieren</b></p>	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p><b>LCP-Erreichbarkeitsprüfung</b></p>	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

### Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
<b>MTU</b>	<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>

## 16.1.2 Dual Stack Lite (DS-Lite)

Dual Stack Lite ermöglicht die Nutzung von IPv4-Verbindungen, auch wenn der zur Verfügung stehende Internetanschluss ausschließlich mit IPv6 betrieben wird. Das ist z. B. dann der Fall, wenn Sie weiterhin IPv4-Verbindungen benötigen, der Internetanbieter allerdings aufgrund knapper IPv4-Adressen nur eine IPv6-Adresse zur Verfügung stellt.

Bei DS-Lite werden IPv4-Pakete in IPv6-Pakete "eingepackt". Die so getunnelten Pakete werden zum AFTR-Server (Address Family Transition Router) des Internetanbieters gesendet, der die IPv4-Pakete "auspackt" und in den IPv4-Bereich des Internet weiterleitet.

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

### 16.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Dual-Stack-Lite-Schnittstellen einzurichten.

Das Menü **WAN->Internet + Einwählen->Dual Stack Lite->Neu** besteht aus folgenden Feldern:

#### Felder im Menü Basisparameter



Feld	Beschreibung
<b>Beschreibung</b>	Weisen Sie Ihrer Dual-Stack-Lite-Verbindung einen Namen zu.
<b>IPv6-Schnittstelle</b>	Wählen Sie die IPv6-Schnittstelle aus, die für die DS-Lite-Verbindung verwendet wird. Dies ist normalerweise die Schnittstelle Ihrer Internetverbindung. Über diese Schnittstelle gesendete IPv4-Pakete werden in IPv6-Pakete verpackt.
<b>AFTR</b>	Geben Sie die IPv6-Adresse oder den Domännennamen Ihres AFTR (Address Family Transition Router) ein. Sie erhalten die Adresse vom Anbieter Ihrer IPv6-Internetverbindung.
<b>Standardroute</b>	Wählen Sie aus, ob Sie diese Verbindung als Standardroute verwenden wollen. Die Einstellung ist sinnvoll, um den gesamten IPv4-Datenverkehr, der über das Internet gehen soll, auch wirklich über die IPv6-Verbindung senden zu können. Andernfalls müssen Sie entsprechende Einstellungen im Routing vornehmen.  Mit <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion aktiv.

### 16.1.3 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.

#### 16.1.3.1 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
<b>Beschreibung</b>	Geben Sie einen beliebigen Namen ein, um die Internetverbindung eindeutig zu benennen.

Feld	Beschreibung
	In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
<b>PPTP-Ethernet-Schnittstelle</b>	<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 <b>Physikalische Schnittstellen-&gt;ATM-&gt;Profile-&gt;Neu</b> für diese Verbindung konfigurierte EthoA-Schnittstelle z. B. <i>ethoa50-0</i>, aus.</p>
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.
<b>Passwort</b>	Geben Sie das Passwort ein.
<b>Immer aktiv</b>	<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>
<b>Timeout bei Inaktivität</b>	<p>Nur wenn <b>Immer aktiv</b> deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte sind <i>0</i> bis <i>3600</i> (Sekunden). <i>0</i> deaktiviert den Timeout.</p> <p>Der Standardwert ist <i>300</i>.</p> <p>Bsp. <i>10</i> für FTP-Übertragungen, <i>20</i> für LAN-zu-LAN-Übertragungen, <i>90</i> für Internetverbindungen.</p>

#### Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> <li>• <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.</li> </ul> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 343 konfigurieren.</p>
<b>IP-Adressmodus</b>	<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"> <li>• <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine temporär gültige IP-Adresse vom Provider.</li> <li>• <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.</li> </ul>
<b>Standardroute</b>	<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>
<b>NAT-Eintrag erstellen</b>	<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>
<b>Lokale IP-Adresse</b>	<p>Nur für <b>IP-Adressmodus</b> = <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>

Feld	Beschreibung
<b>Routeneinträge</b>	<p>Nur bei <b>IP-Adressmodus</b> = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen PPTP-Partner.</p> <p>Fügen Sie mit <b>Hinzufügen</b> neue Einträge hinzu.</p> <ul style="list-style-type: none"> <li>• <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes.</li> <li>• <i>Netzmaske</i>: Netzmaske zu <b>Entfernte IP-Adresse</b>. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske.</li> <li>• <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.</li> </ul>

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Blockieren nach Verbindungsfehler für</b>	<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>
<b>Maximale Anzahl der erneuten Einwählversuche</b>	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind 0 bis 100.</p> <p>Der Standardwert ist 5.</p>
<b>Authentifizierung</b>	<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"> <li>• <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen.</li> <li>• <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen.</li> <li>• <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen.</li> <li>• <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.)</li> <li>• <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen.</li> <li>• <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.</li> </ul>
<b>DNS-Aushandlung</b>	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für <b>Primärer DNS-Server</b> und <b>Sekundärer DNS-Server</b> 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>
<b>TCP-ACK-Pakete priorisieren</b>	<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>
<b>PPTP-Adressmodus</b>	<p>Zeigt den Adressmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Statisch</i>: Die <b>Lokale PPTP-IP-Adresse</b> wird dem ausgewählten Ethernet-Port zugewiesen.</li> </ul>
<b>Lokale PPTP-IP-Adresse</b>	<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>
<b>Entfernte PPTP-IP-Adresse</b>	<p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p> <p>Der Standardwert ist <i>10.0.0.138</i>.</p>

Feld	Beschreibung
<b>LCP-Erreichbarkeitsprüfung</b>	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

## 16.1.4 PPPoA

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

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

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

### 16.1.4.1 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
<b>Beschreibung</b>	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.
<b>ATM PVC</b>	Wählen Sie ein im Menü <b>ATM-&gt;Profile</b> angelegtes ATM-Profil, dargestellt durch die vom Provider vorgegebenen globalen ID VPI und VCI.
<b>Benutzername</b>	Geben Sie den Benutzernamen ein.

Feld	Beschreibung
<b>Passwort</b>	Geben Sie das Passwort für die PPPoA-Verbindung ein.
<b>Immer aktiv</b>	<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>
<b>Timeout bei Inaktivität</b>	<p>Nur wenn <b>Immer aktiv</b> 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
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> <li>• <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.</li> </ul> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <a href="#">Firewall</a> auf Seite 343 konfigurieren.</p>
<b>IP-Adressmodus</b>	Wählen Sie aus, ob Ihr Gerät eine statische IP-Adresse hat

Feld	Beschreibung
	<p>oder diese dynamisch erhält.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse.</li> <li>• <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.</li> </ul>
<b>Standardroute</b>	<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>
<b>NAT-Eintrag erstellen</b>	<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>
<b>Lokale IP-Adresse</b>	<p>Nur für <b>IP-Adressmodus</b> = <i>Statisch</i></p> <p>Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.</p>
<b>Routeneinträge</b>	<p>Nur bei <b>IP-Adressmodus</b> = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit <b>Hinzufügen</b> neue Einträge hinzu.</p> <ul style="list-style-type: none"> <li>• <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes.</li> <li>• <i>Netzmaske</i>: Netzmaske zu <b>Entfernte IP-Adresse</b>. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske.</li> <li>• <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.</li> </ul>

#### Felder im Menü IPv6-Einstellungen



Feld	Beschreibung
<b>IPv6</b>	<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>
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung das gewählte ATM-Profil betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> </ul> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> </ul> <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 343 konfigurieren.</p>
<b>IPv6-Modus</b>	<p>Nur für <b>IPv6 = Aktiviert</b></p> <p>Das gewählte ATM-Profil wird im Host-Modus betrieben.</p>
<b>Router Advertisement annehmen</b>	<p>Nur für <b>IPv6 = Aktiviert</b> und <b>IPv6-Modus = Host</b></p> <p>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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>DHCP-Client</b>	<p>Nur für <b>IPv6 = Aktiviert</b> und <b>IPv6-Modus = Host</b></p> <p>Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll.</p>

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>IPv6-Adressen</b>	<p>Nur für <b>IPv6</b> = <i>Aktiviert</i></p> <p>Sie können der gewählten Schnittstelle <b>IPv6-Adressen</b> zuordnen.</p> <p>Mit <b>Hinzufügen</b> können Sie einen oder mehrere Adresseinträge 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 (<b>IPv6-Modus</b> = <i>Host</i>, <b>Router Advertisement annehmen</b> <i>Aktiviert</i> und <b>DHCP-Client</b> <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 (<b>IPv6-Modus</b> = <i>Router</i> (<i>Router-Advertisement übermitteln</i>), <b>Router Advertisement übertragen</b> <i>Aktiviert</i> und <b>DHCP-Server</b> <i>Aktiviert</i>), so müssen Sie hier seine IPv6-Adressen konfigurieren.</p>

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

#### Felder im Menü Link-Präfix

Feld	Beschreibung
<b>Art der Einrichtung</b>	<p>Wählen Sie, auf welche Weise der Link-Präfix festgelegt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Von Allgemeinem Präfix</i> (Standardwert): Der Link-Präfix wird von einem allgemeinen Präfix abgeleitet.</li> <li>• <i>Statisch</i>: Sie können den Link-Präfix eingeben.</li> </ul>
<b>Allgemeiner Präfix</b>	Nur für <b>Art der Einrichtung</b> = <i>Von Allgemeinem Präfix</i>

Feld	Beschreibung
	<p>Wählen Sie den Allgemeinen Präfix, von dem der Link-Präfix abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter <b>Netzwerk-&gt;Allgemeine IPv6-Präfixe-&gt;Konfiguration eines Allgemeinen Präfixes-&gt;Neu</b> angelegt sind.</p>
<b>Automatische Subnetzerstellung</b>	<p>Nur wenn <b>Art der Einrichtung</b> = <i>Von Allgemeinem Präfix</i> und wenn ein <b>Allgemeiner Präfix</b> gewählt ist.</p> <p>Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID <i>0</i> verwendet, für das zweite Subnetz die Subnetz-ID <i>1</i>, usw.</p> <p>Mögliche Werte für die <b>Subnetz-ID</b> sind <i>0</i> bis <i>65535</i>.</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> <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>
<b>Subnetz-ID</b>	<p>Nur wenn <b>Automatische Subnetzerstellung</b> 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 <i>0</i> bis <i>65535</i>.</p> <p>Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.</p>
<b>Link-Präfix</b>	<p>Nur für <b>Art der Einrichtung</b> = <i>Statisch</i></p> <p>Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit <i>::</i> enden. Seine Länge ist mit <i>64</i> vorgegeben.</p>

**Felder im Menü Host-Adresse**

Feld	Beschreibung
<b>Erzeugungsmethode</b>	<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"> <li>• Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt.</li> <li>• In die entstandene Lücke wird <i>FFFF</i> eingefügt, um 64 Bit zu erhalten.</li> <li>• Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt.</li> <li>• Im ersten 8-Bit-Feld wird Bit 7 auf <i>1</i> gesetzt.</li> </ul>
<b>Statische Adressen</b>	<p>Sie können, unabhängig von der automatischen Erzeugung, die unter <b>Erzeugungsmethode</b> festgelegt ist, mit <b>Hinzufügen</b> 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></p>

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>Blockieren nach Verbindungsfehler für</b>	<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>
<b>Maximale Anzahl der erneuten Einwählversuche</b>	<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>
<b>Authentifizierung</b>	<p>Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen.</li> <li>• <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen.</li> <li>• <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen.</li> <li>• <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen.</li> <li>• <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.)</li> <li>• <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen.</li> <li>• <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.</li> </ul>
<p><b>DNS-Aushandlung</b></p>	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für <b>Primärer DNS-Server</b> und <b>Sekundärer DNS-Server</b> vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p><b>TCP-ACK-Pakete priorisieren</b></p>	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p><b>LCP-Erreichbarkeitsprüfung</b></p>	<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>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

## 16.1.5 IP Pools



### Hinweis


Beachten Sie, dass das Menü **IP Pools** nur dann verfügbar ist wenn ein Port im Menü **Physikalische Schnittstellen -> ISDN-Ports -> ISDN-Konfiguration** in den externen Betrieb (TE-Modus) geschaltet ist. Dafür muss ein Adapte angeschlossen sein (als Zubehör erhältlich).

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.

### 16.1.5.1 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
<b>IP-Poolname</b>	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
<b>IP-Adressbereich</b>	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.

Feld	Beschreibung
<b>DNS-Server</b>	<p><b>Primär:</b> 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><b>Sekundär:</b> Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

## 16.2 ATM

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

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

In einem ATM-Netz können unterschiedliche Anwendungen wie z. B. Sprache, Video und Daten nebeneinander im asynchronen Zeitmultiplexverfahren übertragen werden. Jedem Sender werden dabei Zeitabschnitte zum Übertragen seiner Daten zur Verfügung gestellt. Beim asynchronen Verfahren werden ungenutzte Zeitabschnitte eines Senders von einem anderen Sender verwendet.

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

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

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

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

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

## 16.2.1 Profile

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

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



### 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](http://www.ietf.org/rfc.html)).

### 16.2.1.1 Neu

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

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

#### Felder im Menü ATM-Profilparameter

Feld	Beschreibung
<b>Provider</b>	Wählen Sie eines der vorkonfigurierten ATM-Profile für Ihren Provider aus der Liste aus oder definieren Sie mit <code>-- Benutzerdefiniert --</code> ein Profil.
<b>Beschreibung</b>	Nur für <b>Provider</b> = <code>-- Benutzerdefiniert --</code> Geben Sie eine beliebige Beschreibung für die Verbindung ein.
<b>ATM-Schnittstelle</b>	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.
<b>Typ</b>	Nur für <b>Provider</b> = <code>-- Benutzerdefiniert --</code>



Feld	Beschreibung
	<p>Wählen Sie das Protokoll für die ATM-Verbindung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Ethernet über ATM</i> (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet.</li> <li>• <i>Geroutete Protokolle über ATM</i>: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) werden geroutete Protokolle über ATM (RPoA) verwendet.</li> <li>• <i>PPP über ATM</i>: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.</li> </ul>
<b>Virtual Path Identifier (VPI)</b>	<p>Nur für <b>Provider</b> = <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 <i>0</i> bis <i>255</i>.</p> <p>Der Standardwert ist <i>8</i>.</p>
<b>Virtual Channel Identifier (VCI)</b>	<p>Nur für <b>Provider</b> = <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 <i>32</i> bis <i>65535</i>.</p> <p>Der Standardwert ist <i>32</i>.</p>
<b>Enkapsulierung</b>	<p>Nur für <b>Provider</b> = <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"> <li>• <i>LLC Bridged no FCS</i> (Standardwert für Ethernet über ATM): Wird nur für <b>Typ</b> = <i>Ethernet über ATM</i> angezeigt.</li> </ul>

Feld	Beschreibung
	<p>Bridged Ethernet mit LLC/SNAP-Encapsulierung ohne Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> <li>• <i>LLC Bridged FCS</i>: Wird nur für <b>Typ = Ethernet über ATM</b> angezeigt.</li> </ul>
	<p>Bridged Ethernet mit LLC/SNAP-Encapsulierung mit Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> <li>• <i>Nicht ISO</i> (Standardwert für Geroutete Protokolle über ATM): Wird nur für <b>Typ = Geroutete Protokolle über ATM</b> angezeigt.</li> </ul>
	<p>Encapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing.</p> <ul style="list-style-type: none"> <li>• <i>LLC</i>: Wird nur für <b>Typ = PPP über ATM</b> angezeigt.</li> </ul>
	<p>Encapsulierung mit LLC-Header.</p> <ul style="list-style-type: none"> <li>• <i>VC-Multiplexing</i> (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Encapsulierung (Null Einkapselung) mit Frame Check Sequence (Prüfsummen).</li> </ul>

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

Feld	Beschreibung
<b>Standard-Ethernet für PPPoE-Schnittstellen</b>	<p>Nur für <b>Typ = Ethernet über ATM</b></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>
<b>Adressmodus</b>	<p>Nur für <b>Typ = Ethernet über ATM</b></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"> <li>• <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in <b>IP-Adresse / Netzmaske</b> zugewiesen.</li> <li>• <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-</li> </ul>

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

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

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

Feld	Beschreibung
<b>TCP-ACK-Pakete priorisieren</b>	<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
<b>Client-Typ</b>	<p>Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Auf Anforderung</i> (Standardwert): Die PPPoA wird nur bei Bedarf aufgebaut, z. B. für den Internetzugang.</li> </ul> <p>Zusätzliche Informationen zu PPP über ATM finden Sie unter <a href="#">PPPoA</a> auf Seite 264.</p>

## 16.2.2 Dienstkategorien

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

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



#### Achtung

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

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

### 16.2.2.1 Neu

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

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

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Virtual Channel Connection (VCC)</b>	Wählen Sie die bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus, für welche die Dienstkategorie festgelegt werden soll.
<b>ATM-Dienstkategorie</b>	<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"> <li>• <i>Unspecified Bit Rate (UBR)</i> (Standardwert): Der Verbindung wird keine bestimmte Datenrate garantiert. Die <b>Peak Cell Rate (PCR)</b> legt die Grenze fest, bei deren Überschreiten Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen.</li> <li>• <i>Constant Bit Rate (CBR)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen, die von der <b>Peak Cell Rate (PCR)</b> bestimmt wird. Diese Kategorie eignet sich für kritische Anwendungen (Real-Time), die eine garantierte Datenrate voraussetzen.</li> <li>• <i>Variable Bit Rate V.1 (VBR.1)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen - <b>Sustained Cell Rate (SCR)</b>. Diese darf insgesamt um das in <b>Maximale Burst-Größe (MBS)</b> konfigurierte Volumen überschritten werden. Jeglicher weiterer ATM-Traffic wird verworfen. Die <b>Peak Cell Rate (PCR)</b> bildet dabei die maximal mögliche Datenrate. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen.</li> <li>• <i>Variable Bit Rate V.3 (VBR.3)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen - <b>Sustained Cell Rate (SCR)</b>. Diese darf insgesamt um das in <b>Maximale Burst-Größe (MBS)</b> konfigurierte Volumen überschritten werden.</li> </ul>

Feld	Beschreibung
	<p>Weiterer ATM-Traffic wird markiert und je nach Auslastung des Zielnetzes mit niedriger Priorität behandelt, d. h. wird bei Bedarf verworfen. Die <b>Peak Cell Rate (PCR)</b> bildet dabei die maximal mögliche Datenrate. Diese Kategorie eignet sich für kritische Anwendungen mit stoßweisem Datenaufkommen.</p>
<b>Peak Cell Rate (PCR)</b>	<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>
<b>Sustained Cell Rate (SCR)</b>	<p>Nur für <b>ATM-Dienstkategorie</b> = <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>
<b>Maximale Burst-Größe (MBS)</b>	<p>Nur für <b>ATM-Dienstkategorie</b> = <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>

### 16.2.3 OAM-Regelung

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



### Hinweis

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

Zur Überwachung der ATM-Verbindung stehen zwei Mechanismen zur Verfügung: 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.

#### 16.2.3.1 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
<b>OAM-Fluss-Level</b>	<p>Wählen Sie den zu überwachenden OAM-Fluss-Level.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>F5</i>: (Virtual Channel Level) Die OAM-Einstellungen werden auf den virtuellen Kanal angewendet (Standardwert).</li> <li>• <i>F4</i>: (Virtual Path Level) Die OAM-Einstellungen werden auf den virtuellen Pfad angewendet.</li> </ul>
<b>Virtual Channel Connection (VCC)</b>	<p>Nur für <b>OAM-Fluss-Level = F5</b></p> <p>Wählen Sie die zu überwachende bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI)</p>

Feld	Beschreibung
	aus.
<b>Virtual Path Connection (VPC)</b>	Nur für <b>OAM-Fluss-Level = F4</b> Wählen Sie die zu überwachende bereits konfigurierte Virtual Path Connection (angezeigt durch den VPI) aus.

#### Felder im Menü Loopback

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



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

#### Felder im Menü CC-Aktivierung

Feld	Beschreibung
<b>Continuity Check (CC) Ende-zu-Ende</b>	<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"> <li>• <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet.</li> <li>• <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet.</li> <li>• <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet.</li> <li>• <i>Keine Aushandlung</i>: Je nach Einstellung im Feld <b>Richtung</b> werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine CC-Aushandlung statt.</li> <li>• <i>Passiv</i>: Die Funktion ist nicht aktiv.</li> </ul> <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"> <li>• <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Senke</i>: CC-Daten werden empfangen.</li> <li>• <i>Quelle</i>: CC-Daten werden generiert.</li> </ul>
<b>Continuity Check (CC) Segment</b>	<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"> <li>• <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet.</li> <li>• <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet.</li> <li>• <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet.</li> <li>• <i>Keine Aushandlung</i>: Je nach Einstellung im Feld <b>Richtung</b> werden OAM CC Requests entweder gesendet und/oder beantwortet, es findet keine CC-Aushandlung statt.</li> <li>• <i>Keiner</i>: Die Funktion ist nicht aktiv.</li> </ul> <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"> <li>• <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert.</li> <li>• <i>Senke</i>: CC-Daten werden empfangen.</li> <li>• <i>Quelle</i>: CC-Daten werden generiert.</li> </ul>

## 16.3 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 wäh-

rend eines Telefongesprächs bei Bedarf reduziert.

## 16.3.1 Regulierte Schnittstellen

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

### 16.3.1.1 Neu

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

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

#### Felder im Menü Grundeinstellungen

Feld	Beschreibung
<b>Schnittstelle</b>	Legen Sie fest, für welche Schnittstellen die Sprachübertragung optimiert werden soll.
<b>Kontrollmodus</b>	<p>Wählen Sie den Modus für die Optimierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert.</li> <li>• <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt.</li> <li>• <i>Immer</i>: Die Optimierung für die Übertragung der Sprachdaten wird immer durchgeführt.</li> </ul>
<b>Maximale Upload-Geschwindigkeit</b>	Geben Sie die maximal zur Verfügung stehende Bandbreite in Upload-Richtung in kbit/s für die gewählte Schnittstelle ein.

## 17 VPN

Als VPN (Virtual Private Network) wird eine Verbindung bezeichnet, die das Internet als "Transportmedium" nutzt, aber nicht öffentlich zugänglich ist. Nur berechtigte Benutzer haben Zugang zu einem solchen VPN, das anschaulich auch als VPN-Tunnel bezeichnet wird. Üblicherweise werden die über ein VPN transportierten Daten verschlüsselt.

Über ein VPN kann z. B. ein Außendienstmitarbeiter oder ein Mitarbeiter im Home Office auf die Daten im Firmennetz zugreifen. Filialen können ebenfalls über VPN an die Zentrale angebunden werden.

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.

### 17.1 IPSec

IPSec ermöglicht den Aufbau von gesicherten Verbindungen zwischen zwei Standorten (VPN). Hierdurch lassen sich sensible Unternehmensdaten auch über ein unsicheres Medium wie z. B. das Internet übertragen. Die eingesetzten Geräte agieren hierbei als Endpunkte des VPN Tunnels. Bei IPSec handelt es sich um eine Reihe von Internet-Engineering-Task-Force-(IETF)-Standards, die Mechanismen zum Schutz und zur Authentifizierung von IP-Paketen spezifizieren. IPSec bietet Mechanismen, um die in den IP-Paketen übermittelten Daten zu verschlüsseln und zu entschlüsseln. Darüber hinaus kann die IPSec Implementierung nahtlos in eine Public-Key-Umgebung (PKI, siehe [Zertifikate](#) auf Seite 75) 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 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 angeben.

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 sich die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten entsprechen muss.

## 17.1.1 IPSec-Peers

Als Peer wird ein Endpunkt einer Kommunikation in einem Computernetzwerk bezeichnet. Jeder Peer bietet dabei seine Dienste an und nutzt die Dienste der anderen Peers.

Im Menü **VPN->IPSec->IPSec-Peers** wird eine Liste aller 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 462.

### 17.1.1.1 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
<b>Administrativer Status</b>	<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"> <li>• <i>Aktiv</i> (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung.</li> <li>• <i>Inaktiv</i>: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.</li> </ul>
<b>Beschreibung</b>	<p>Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
<b>Peer-Adresse</b>	<p>Wählen Sie die <b>IP-Version</b> aus. Sie können wählen, ob IPv4 oder IPv6 bevorzugt verwendet werden soll oder ob nur eine der beiden IP-Versionen erlaubt sein soll.</p> <div data-bbox="539 1128 1315 1282" style="border: 1px solid gray; background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> <p> <b>Hinweis</b></p> <p>Diese Auswahl ist nur relevant, wenn ein Host-Name als Peer-Adresse eingegeben wird.</p> </div> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>IPv4 bevorzugt</i></li> <li>• <i>IPv6 bevorzugt</i></li> <li>• <i>Nur IPv4</i></li> <li>• <i>Nur IPv6</i></li> </ul> <p>Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein.</p>

Feld	Beschreibung
	<p>Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.</p>
<b>Peer-ID</b>	<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"> <li>• <i>Fully Qualified Domain Name (FQDN)</i>: Beliebige Zeichenkette</li> <li>• <i>E-Mail-Adresse</i></li> <li>• <i>IPV4-Adresse</i></li> <li>• <i>ASN.1-DN (Distinguished Name)</i></li> <li>• <i>Schlüssel-ID</i>: Beliebige Zeichenkette</li> </ul> <p>Auf dem Peer-Gerät entspricht diese ID dem Parameter <b>Lokaler ID-Wert</b>.</p>
<b>IKE (Internet Key Exchange)</b>	<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"> <li>• <i>IKEv1</i> (Standardwert): Internet Key Exchange Protocol Version 1</li> <li>• <i>IKEv2</i>: Internet Key Exchange Protocol Version 2</li> </ul>
<b>Authentifizierungsmethode</b>	<p>Nur für <b>IKE (Internet Key Exchange) = IKEv2</b></p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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 <b>IPSec-Peers</b> konfiguriert. Der Preshared Key ist das gemeinsame Passwort.</li> <li>• <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden</li> </ul>

Feld	Beschreibung
	unter Nutzung des RSA-Algorithmus authentifiziert.
<b>Lokaler ID-Typ</b>	<p>Nur für <b>IKE (Internet Key Exchange) = IKEv2</b></p> <p>Wählen Sie den Typ der lokalen ID aus.</p> <p>Mögliche ID-Typen:</p> <ul style="list-style-type: none"> <li>• <i>Fully Qualified Domain Name (FQDN)</i></li> <li>• <i>E-Mail-Adresse</i></li> <li>• <i>IPV4-Adresse</i></li> <li>• <i>ASN.1-DN (Distinguished Name)</i></li> <li>• <i>Schlüssel-ID</i>: Beliebige Zeichenkette</li> </ul>
<b>Lokale ID</b>	<p>Nur für <b>IKE (Internet Key Exchange) = IKEv2</b></p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für <b>Authentifizierungsmethode = DSA-Signatur</b> oder <b>RSA-Signatur</b> wird die Option <b>Subjektnamen aus Zertifikat verwenden</b> angezeigt.</p> <p>Wenn Sie die Option <b>Subjektnamen aus Zertifikat verwenden</b> aktivieren, wird der im Zertifikat angegebene Subjektnamen verwendet.</p>
<b>Preshared Key</b>	<p>Geben Sie das mit dem Peer vereinbarte Passwort ein.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer 0x am Anfang des Eintrags.</p>
<b>IP-Version des Tunnelnetzwerks</b>	<p>Wählen Sie aus, ob IPv4 oder IPv6 oder beide Versionen für den VPN-Tunnel verwendbar sein sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>IPv4</i></li> <li>• <i>IPv6</i></li> <li>• <i>IPv4 und IPv6</i></li> </ul>

#### Felder im Menü IPv4-Schnittstellenrouten



Feld	Beschreibung
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i> (Standardwert) : Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> <li>• <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde.</li> </ul> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <a href="#">Firewall</a> auf Seite 343 konfigurieren.</p>
<b>IPv4-Adressvergabe</b>	<p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Statisch</i> (Standardwert): Geben Sie eine statische IP-Adresse ein.</li> <li>• <i>Client im IKE-Konfigurationsmodus</i>: Wählen Sie diese Option, wenn Ihr Gateway als IPsec-Client vom Server eine IP-Adresse erhalten soll.</li> <li>• <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 <b>IP-Zuordnungspool</b> entnommen.</li> </ul>
<b>Konfigurationsmodus</b>	<p>Nur bei <b>IPv4-Adressvergabe</b> = <i>Server im IKE-Konfigurationsmodus</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Pull</i> (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage.</li> <li>• <i>Push</i>: Das Gateway schlägt dem Client eine IP-Adresse vor und der Client muss diese akzeptieren oder zurückweisen.</li> </ul> <p>Dieser Wert muss für beide Seiten des Tunnels identisch sein.</p>

Feld	Beschreibung
<b>IP-Zuordnungspool</b>	<p>Nur bei <b>IPv4-Adressvergabe</b> = <i>Server im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie einen im Menü <b>VPN-&gt;IPSec-&gt;IP Pools</b> konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung <i>Noch nicht definiert</i>.</p>
<b>Standardroute</b>	<p>Nur für <b>IPv4-Adressvergabe</b> = <i>Statisch oder Client im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Lokale IP-Adresse</b>	<p>Nur für <b>IPv4-Adressvergabe</b> = <i>Statisch oder Server im IKE-Konfigurationsmodus</i></p> <p>Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.</p>
<b>Metrik</b>	<p>Nur für <b>IPv4-Adressvergabe</b> = <i>Statisch oder Client im IKE-Konfigurationsmodus</i> und <b>Standardroute</b> = <i>Aktiviert</i></p> <p>Wählen Sie die Priorität der Route aus.</p> <p>Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.</p> <p>Wertebereich von 0 bis 15. der Standardwert ist 1.</p>
<b>Routeneinträge</b>	<p>Nur für <b>IPv4-Adressvergabe</b> = <i>Statisch oder Client im IKE-Konfigurationsmodus</i></p> <p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> <li>• <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs.</li> <li>• <i>Netzmaske</i>: Netzmaske zu <i>Entfernte IP-Adresse</i>.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 - 15). der Standardwert ist 1.</li> </ul>

#### Felder im Menü Zusätzlicher Filter des IPv4-Datenverkehrs

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

#### Felder im Menü IPv6-Schnittstellenrouten

Feld	Beschreibung
<b>Sicherheitsrichtlinie</b>	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Nicht Vertrauenswürdig</i>: Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde.</li> </ul> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> <li>• <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.</li> </ul> <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 <a href="#">Firewall</a> auf Seite 343 konfigurieren.</p>
<b>Lokales IPv6-Netzwerk</b>	<p>Wählen Sie ein Netzwerk aus. Sie können unter den Link-Präfixen wählen, die unter <b>LAN-&gt;IP-Konfiguration-&gt;Schnittstellen-&gt;Neu</b> 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>
<b>Entferntes IPv6-Netzwerk</b>	<p>Fügen Sie mit <b>Hinzufügen</b> einen neuen <b>Präfix</b> hinzu. Geben Sie die Adresse der Tunnelgegenstelle ein. Standardmäßig ist eine <b>Länge</b> von 64 und eine <b>Priorität</b> von 1 vorgegeben. Je</p>

Feld	Beschreibung
	niedriger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.

### 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 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.

Fügen Sie weitere Filter mit **Hinzufügen** hinzu.

### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie eine Bezeichnung für das Filter ein.
<b>Protokoll</b>	Wählen Sie ein Protokoll aus.  Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
<b>Quell-IP-Adresse/Netzmaske</b>	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Beliebig</i></li> <li>• <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i> (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.</li> </ul>
<b>Quell-Port</b>	Nur für <b>Protokoll</b> = <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.
<b>Ziel-IP-Adresse/Netzmaske</b>	Geben Sie die Ziel-IP-Adresse und die zugehörige Netzmaske der Datenpakete ein.
<b>Ziel-Port</b>	Nur für <b>Protokoll</b> = <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
<b>Phase-1-Profil</b>	<p>Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in <b>VPN-&gt;IPsec-&gt;Phase-1-Profile</b> als Standard markiert ist</li> <li>• <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 .</li> <li>• <i>&lt;Profilname&gt;</i>: Verwendet ein Profil, das im Menü <b>VPN-&gt;IPsec-&gt;Phase-1-Profile</b> für Phase 1 konfiguriert wurde.</li> </ul>
<b>Phase-2-Profil</b>	<p>Wählen Sie ein Profil für die Phase 2 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in <b>VPN-&gt;IPsec-&gt;Phase-2-Profile</b> als Standard markiert ist</li> <li>• <i>*Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 2 die Proposals 3DES/MD5, AES-128/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü <b>VPN-&gt;IPsec-&gt;Phase-2-Profile</b>.</li> <li>• <i>&lt;Profilname&gt;</i>: Verwendet ein Profil, das im Menü <b>VPN-&gt;IPsec-&gt;Phase-2-Profile</b> für Phase 2 konfiguriert wurde.</li> </ul>
<b>XAUTH-Profil</b>	<p>Wählen Sie ein in <b>VPN-&gt;IPsec-&gt;XAUTH-Profile</b> 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>
<b>Anzahl erlaubter Verbindungen</b>	<p>Wählen Sie aus, wieviele Benutzer sich mit diesem Peer-Profil verbinden dürfen.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Ein Benutzer</i> (Standardwert): Es kann sich nur ein Peer mit den in diesem Profil definierten Daten verbinden.</li> <li>• <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.</li> </ul> <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 <b>Lokale ID</b> verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen. Informationen, wie dieser Parameter für Ihren IPSec-Client einzustellen ist, entnehmen Sie der entsprechenden Dokumentation.</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>
<b>Startmodus</b>	<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"> <li>• <i>Auf Anforderung</i> (Standardwert): Der Peer wird durch einen Trigger in den aktiven Zustand versetzt.</li> <li>• <i>Immer aktiv</i>: Der Peer ist immer aktiv.</li> </ul>
<b>Backup Peer</b>	<p>Nur für Peers mit IKEv2.</p> <p>Wenn der Peer im <b>Startmodus</b> <i>Immer aktiv</i> ist, können Sie hier einen weiteren bereits konfigurierten Peer als Rückfalloption auswählen. Wenn der aktuelle Peer z. B. aufgrund einer Störung des zentralen VPN-Einwahlknotens inaktiv wird, kann der Backup Peer eine Verbindung zu einem Backup-VPN-Einwahlknoten aufbauen. Im Fall der Wiedererreichbarkeit des primären zentralen Einwahlknotens wird die Verbindung nahtlos wieder dorthin aufgebaut.</p> <p>Bei dieser Lösung ist zu beachten, dass für beide Peers das Routing so konfiguriert ist, dass eine Verbindung zur Gegenstelle auch tatsächlich über beide Peers erfolgen kann. Darüber</p>

Feld	Beschreibung
	hinaus sollte die Metrik der Routen für den Backup Peer schlechter sein als die für den primären Peer. Nur so ist gewährleistet, dass der Tunnel wieder über den primären Peer aufgebaut wird, sobald dessen Verbindung wieder verfügbar ist.
<b>Verzögerung bis zur Rückkehr zum primären Peer</b>	Wenn im Fall eines Fallbacks der primäre Peer wieder erreichbar ist, kann es wünschenswert sein, die Nutzung des primären Peers und damit den Reset des sekundären Peers zu verzögern. Diese Option definiert die gewünschte Verzögerungszeit.

### Felder im Menü Erweiterte IP-Optionen

Feld	Beschreibung
<b>Öffentliche Schnittstelle</b>	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 <b>Öffentlicher Schnittstellenmodus</b> diese Schnittstelle verwendet.
<b>Öffentlicher Schnittstellenmodus</b>	Nur wenn unter <b>Öffentliche Schnittstelle</b> eine Schnittstelle ausgewählt ist.  Legen Sie fest, wie strikt die Einstellung gehandhabt wird.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Erzwingen</i>: Unabhängig von den Prioritäten der aktuellen Routingtabelle wird nur die ausgewählte Schnittstelle verwendet.</li> <li>• <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.</li> </ul>
<b>Öffentliche IPv4-Quelladresse</b>	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 <b>Öffentliche IPv4-Quelladresse</b> aktiviert werden soll.  Mit <i>Aktiviert</i> wird die Funktion aktiv.



Feld	Beschreibung
	<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>
<p><b>Öffentliche IPv6-Quelladresse</b></p>	<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 <b>Öffentliche IPv6-Quelladresse</b> 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>
<p><b>Überprüfung der IPv4-Rückroute</b></p>	<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>
<p><b>MobiKE</b></p>	<p>Nur für Peers mit IKEv2.</p> <p><b>MobiKE</b> 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>
<p><b>IPv4 Proxy ARP</b></p>	<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"> <li>• <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen</li> </ul>

Feld	Beschreibung
	<p>IPSec-Peer.</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> </ul>
<b>CA-Zertifikate</b>	<p>Nur verfügbar, wenn auf dem Gerät Zertifikate verwendet werden.</p> <p>Wenn Sie die Option <b>Folgenden CA-Zertifikaten vertrauen</b> aktivieren, können Sie CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen.</p> <p>Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.</p>

### 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, benötigen Sie eine kostenfreie Zusatzlizenz.

Diese Lizenz erhalten Sie bei Bedarf über Ihren Vertriebspartner oder über unseren Support.

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 303 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
<b>Modus</b>	<p>Wählen Sie den Callback-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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).</li> </ul>
<b>Ankommende Rufnummer</b>	<p>Nur für <b>Modus</b> = <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</p>

Feld	Beschreibung
	auch Wildcards verwendet werden.
<b>Ausgehende Rufnummer</b>	<p>Nur für <b>Modus</b> = <i>Aktiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.</p>
<b>Eigene IP-Adresse per ISDN/GSM übertragen</b>	<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>
<b>Übertragungsmodus</b>	<p>Nur für <b>Eigene IP-Adresse per ISDN/GSM übertragen</b> = 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"> <li>• <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.)</li> <li>• <i>Nur D-Kanalmodi automatisch erkennen</i>: Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen.</li> <li>• <i>Spezifischen D-Kanalmodus verwenden</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld <b>Modus</b> eingestellten Modus zu übertragen.</li> <li>• <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld <b>Modus</b> eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übertragen. (Dies verursacht Kosten.)</li> <li>• <i>Nur B-Kanalmodus verwenden</i>: Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.</li> </ul>
<b>Modus des D-Kanals</b>	Nur für <b>Übertragungsmodus</b> = <i>Spezifischen D-</i>

Feld	Beschreibung
	<p><i>Kanalmodus verwenden</i> <b>oder</b> <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> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>LLC</i> (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen.</li> <li>• <i>SUBADDR</i>: Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen.</li> <li>• <i>LLC und SUBADDR</i>: Die IP-Adresse wird sowohl in den "LLC-" als auch in den "Subaddress Information Elements" übertragen.</li> </ul>

## 17.1.2 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.

### 17.1.2.1 Neu

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

Das Menü **VPN->IPSec->Phase-1-Profile->Neues IKEv1-Profil erstellen** besteht aus folgenden Feldern:

#### Felder im Menü Phase-1-Parameter (IKE) / Phase-1-Parameter (IKEv2)

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie eine Beschreibung ein, welche die Art der Regel eindeutig identifiziert.
<b>Proposals</b>	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 Propo-

Feld	Beschreibung
	<p>sal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden.</p> <p>Verschlüsselungsalgorithmen (<b>Verschlüsselung</b>):</p> <ul style="list-style-type: none"> <li>• <i>3DES</i> : 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.</li> <li>• <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.</li> <li>• <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden.</li> <li>• <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES.</li> <li>• <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird.</li> <li>• <i>AES</i> (Standardwert): 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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <i>AES-256</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit</li> </ul>



Feld	Beschreibung
	<p>keit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet.</p> <p>Hash-Algorithmen (<b>Authentifizierung</b>):</p> <ul style="list-style-type: none"> <li>• <i>MD5</i>: MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.</li> <li>• <i>SHA1</i> (Standardwert): 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.</li> <li>• <i>RipeMD 160</i>: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt.</li> <li>• <i>Tiger192</i>: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus.</li> <li>• <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.</li> <li>• <i>SHA2-384</i>: SHA-2 mit 384 Bit Hash-Länge.</li> <li>• <i>SHA2-512</i>: SHA-2 mit 512 Bit Hash-Länge.</li> </ul> <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>
<b>DH-Gruppe</b>	<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"> <li>• 1 (768 Bit)</li> <li>• 2 (1024 Bit)</li> <li>• 5 (1536 Bit)</li> <li>• 14 (2048 Bit)</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>15 (3072 Bit)</i></li> <li>• <i>16 (4096 Bit)</i></li> </ul> <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
<b>Lebensdauer</b>	<p>Legen Sie die Lebensdauer für Phase-1-Schlüssel fest.</p> <p>Folgende Optionen stehen für die Definition der <b>Lebensdauer</b> zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Eingabe in <b>Sekunden</b>: 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.</li> <li>• Eingabe in <b>kBytes</b>: 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.</li> </ul>
<b>Authentifizierungsmethode</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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 <b>VPN-&gt;IPSec-&gt;IPSec-Peers</b> konfiguriert. Der Preshared Key ist das gemeinsame Passwort.</li> <li>• <i>DSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert.</li> <li>• <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert.</li> <li>• <i>RSA-Verschlüsselung</i>: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.</li> </ul>
<b>Lokales Zertifikat</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p>

Feld	Beschreibung
	<p>Nur für <b>Authentifizierungsmethode</b> = <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. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>
<b>Modus</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p> <p>Wählen Sie den Phase-1-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> </ul> <p>Wählen Sie weiterhin aus, ob der gewählte Modus ausschließlich verwendet werden darf (<b>Strikt</b>) oder der Peer auch einen anderen Modus vorschlagen kann.</p>
<b>Lokaler ID-Typ</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p> <p>Wählen Sie den Typ der lokalen ID aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Fully Qualified Domain Name (FQDN)</i></li> <li>• <i>E-Mail-Adresse</i></li> <li>• <i>IPV4-Adresse</i></li> <li>• <i>ASN.1-DN (Distinguished Name)</i></li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Schlüsse-ID</i></li> </ul>
<b>Lokaler ID-Wert</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für <b>Authentifizierungsmethode</b> = <i>DSA-Signatur</i>, <i>RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i> wird die Option <b>Subjektnamen aus Zertifikat verwenden</b> angezeigt.</p> <p>Wenn Sie die Option <b>Subjektnamen aus Zertifikat verwenden</b> aktivieren, wird der im Zertifikat angegebene Subjektnamen verwendet.</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
<b>Erreichbarkeitsprüfung</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p> <p>Wählen Sie die Methode aus, mit der die Funktionalität der IP-Sec-Verbindung überprüft werden soll.</p> <p>Neben dem Standardverfahren Dead Peer Detection (DPD) ist auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Automatische Erkennung</i> (Standardwert): Ihr Gerät er-</li> </ul>

Feld	Beschreibung
	<p>kennt und verwendet den Modus, den die Gegenstelle unterstützt.</p> <ul style="list-style-type: none"> <li>• <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option.</li> <li>• <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen.</li> <li>• <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen.</li> <li>• <i>Heartbeats (Senden &amp; Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.</li> <li>• <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.</li> <li>• <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.</li> </ul>
	<p> <b>Hinweis</b></p> <p>Da die beiden Verfahren zur Erreichbarkeitsprüfung unterschiedliche Methoden verwenden, empfiehlt es sich nicht, sie in Phase 1 und Phase 2 kombiniert zu verwenden. In Phase 2 werden lediglich Heartbeats unterstützt, so dass diese deaktiviert werden sollten, wenn in Phase 1 Dead Peer Detection vorgeschrieben ist.</p>
	<p>Nur für <b>Phase-1-Parameter (IKEv2)</b></p> <p>Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
<b>Blockzeit</b>	<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 <math>-1</math> bis <math>86400</math> (Sekunden), der Wert <math>-1</math> bedeutet die Übernahme des Wertes im Standardprofil, der Wert <math>0</math>, dass der Peer in keinem Fall blockiert wird.</p> <p>Der Standardwert ist <math>30</math>. Wenn ein Peer im Modus "Immer aktiv" konfiguriert ist, besteht eine implizite Minimalblockzeit von 15 Sekunden, die unabhängig vom eingegebenen Wert angewendet wird.</p>
<b>NAT-Traversal</b>	<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"> <li>• <i>Aktiviert</i> (Standardwert): NAT-Traversal ist aktiv.</li> <li>• <i>Deaktiviert</i>: NAT-Traversal ist deaktiviert.</li> <li>• <i>Erzwingen</i>: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde.</li> </ul> <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>
<b>CA-Zertifikate</b>	<p>Nur für <b>Phase-1-Parameter (IKE)</b></p> <p>Nur für <b>Authentifizierungsmethode</b> = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p>

Feld	Beschreibung
	<p>Wenn Sie die Option <b>Folgenden CA-Zertifikaten vertrauen</b> aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen.</p> <p>Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.</p>

### 17.1.3 Phase-2-Profile

Ebenso wie für Phase 1 können Sie Profile für die Phase 2 des Tunnelaufbaus definieren.

Im Menü **VPN->IPSec->Phase-2-Profile** wird eine Liste aller konfigurierten IPSec-Phase-2-Profile angezeigt.

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

#### 17.1.3.1 Neu

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

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

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

Feld	Beschreibung
<b>Beschreibung</b>	<p>Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
<b>Proposals</b>	<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 (<b>Verschlüsselung</b>):</p> <ul style="list-style-type: none"> <li>• <i>3DES</i>: 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.</li> <li>• <i>-- ALLE --</i>: Alle Optionen können verwendet werden.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>AES</i> (Standardwert): 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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden.</li> <li>• <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES.</li> <li>• <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird.</li> </ul> <p>Hash-Algorithmen (<b>Authentifizierung</b>):</p> <ul style="list-style-type: none"> <li>• <i>MD5</i>: MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.</li> <li>• -- <i>ALLE</i> --: Alle Optionen können verwendet werden.</li> <li>• <i>SHA1</i> (Standardwert): SHA 1 (Secure Hash Algorithmus #1)</li> </ul>




Feld	Beschreibung
	<p>ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet.</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>SHA2-384</i>: SHA-2 mit 384 Bit Hash-Länge.</li> <li>• <i>SHA2-512</i>: SHA-2 mit 512 Bit Hash-Länge.</li> </ul> <p>Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.</p> <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
<p><b>PFS-Gruppe verwenden</b></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 <b>DH-Gruppe</b> im Menü <b>VPN-&gt;IPSec-&gt;Phase-1-Profile</b> . 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"> <li>• <i>1 (768 Bit)</i></li> <li>• <i>2 (1024 Bit)</i></li> <li>• <i>5 (1536 Bit)</i></li> <li>• <i>14 (2048 Bit)</i></li> <li>• <i>15 (3072 Bit)</i></li> <li>• <i>16 (4096 Bit)</i></li> </ul> <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
<p><b>Lebensdauer</b></p>	<p>Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablauf-</p>

Feld	Beschreibung
	<p>fen 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 <b>Lebensdauer</b> zur Verfügung:</p> <ul style="list-style-type: none"> <li>• Eingabe in <b>Sekunden</b>: 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.</li> <li>• Eingabe in <b>kBytes</b>: Geben Sie die Lebensdauer für Phase-2- Schlüssel als Menge der verarbeiteten Daten in kBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist 0.</li> </ul> <p><b>Schlüssel erneut erstellen nach</b>: 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
<b>IP-Komprimierung</b>	<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>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
<b>Erreichbarkeitsprüfung</b>	<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"> <li>• <i>Automatische Erkennung</i> (Standardwert): Automatische Erkennung, ob die Gegenstelle ein bintec elmeg-Gerät ist. Wenn ja, wird <i>Heartbeats (Senden &amp;Erwarten)</i> (bei Gegenstelle mit bintec elmeg) oder <i>Inaktiv</i> (bei Gegenstelle ohne bintec elmeg) gesetzt.</li> <li>• <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option.</li> <li>• <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen.</li> <li>• <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen.</li> <li>• <i>Heartbeats (Senden &amp;Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.</li> </ul> <div data-bbox="539 1158 1319 1550" style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p> <b>Hinweis</b></p> <p>In Phase 1 und Phase 2 unterstützt Ihr Gerät unterschiedliche Verfahren zur Erreichbarkeitsprüfung: In Phase 1 die sog. Dead Peer Detection sowie Heartbeats, in Phase 2 lediglich Heartbeats. Da die beiden Verfahren zur Erreichbarkeitsprüfung unterschiedliche Methoden verwenden, empfiehlt es sich nicht, sie in Phase 1 und Phase 2 kombiniert zu verwenden. In Phase 2 sollten Heartbeats daher deaktiviert werden, wenn in Phase 1 Dead Peer Detection vorgeschrieben ist.</p> </div>
<b>PMTU propagieren</b>	Wählen Sie aus, ob während der Phase 2 die PMTU (Path Ma-

Feld	Beschreibung
	<p>ximum Transfer Unit) propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

## 17.1.4 XAUTH-Profil

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

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

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

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

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. Mehrere Benutzer können sich entweder nacheinander einzeln oder über einen Multi Peer gleichzeitig einwählen. 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 eine Firmenzentrale über IPSec mit mehreren Filialen verbunden ist, können mehrere Peers konfiguriert werden, zum Beispiel ein Peer für je eine Filiale. Für jeden dieser Peers, also für jede Filiale, wird ein Passwort vergeben. Neben dieser Möglichkeit der Authentifizierung pro Filiale bietet XAuth eine zusätzliche Möglichkeit, mit der sich ein Benutzer individuell und unabhängig vom Standort über sein persönliches Passwort anmelden kann. Damit kann ein bestimmter Benutzer den IPSec-Tunnel über verschiedene Peers nutzen. Das ist zum Beispiel nützlich, wenn ein Angestellter abwechselnd in verschiedenen Filialen arbeitet und er jeweils vor Ort individuellen Zugriff auf den Tunnel benötigt.

Bei einem sogenannten Multi Peer verwenden alle Benutzer dasselbe Passwort, also ein Gruppenpasswort. Auch hier eröffnet XAuth einem Benutzer eine individuelle Authentifizierungsmöglichkeit. Wenn zum Beispiel in einer Filiale mehrere Benutzer über einen Multi Peer Zugriff auf den Tunnel haben, kann es bei unterschiedlichen Aufgaben der Benutzer von Vorteil sein, wenn sich jeder Benutzer mit seinem individuellen Passwort einwählt.

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

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

### 17.1.4.1 Neu

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

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

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie eine Beschreibung für dieses XAuth-Profil ein.  Mit den Einstellungen <b>Rolle</b> = <i>Server</i> und <b>Modus</b> = <i>Lokal</i> oder <b>Rolle</b> = <i>Client</i> (siehe unten) können Sie bis zu 10 XAuth-Profile anlegen.
<b>Rolle</b>	Wählen Sie die Rolle des Gateways bei der XAuth-Authentifizierung aus.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Server</i> (Standardwert): Das Gateway fordert einen Berechtigungsnachweis an.</li> <li>• <i>Client</i>: Das Gateway weist seine Berechtigung nach.</li> </ul>
<b>Modus</b>	Nur für <b>Rolle</b> = <i>Server</i>  Wählen Sie aus, wie die Authentifizierung durchgeführt wird.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>RADIUS</i> (Standardwert): Die Authentifizierung wird über einen RADIUS-Server durchgeführt. Dieser wird im Menü <b>Systemverwaltung-&gt;Remote Authentifizierung-&gt;RADIUS</b> konfiguriert und im Feld <b>RADIUS-Server Gruppen-ID</b> ausgewählt.</li> <li>• <i>Lokal</i>: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.</li> </ul>
<b>Name</b>	Nur für <b>Rolle</b> = <i>Client</i>  Geben Sie den Authentifizierungsnamen des Clients ein.


Feld	Beschreibung
<b>Passwort</b>	Nur für <b>Rolle = Client</b>  Geben Sie das Authentifizierungspasswort ein.
<b>RADIUS-Server Gruppen-ID</b>	Nur für <b>Rolle = Server</b>  Wählen Sie die gewünschte in <b>Systemverwaltung -&gt; Remote Authentifizierung -&gt; RADIUS</b> konfigurierte RADIUS-Gruppe aus.
<b>Benutzer</b>	Nur für <b>Rolle = Server</b> und <b>Modus = Lokal</b>  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 ( <b>Name</b> ) und das Authentifizierungspasswort ( <b>Passwort</b> ) eingeben. Fügen Sie weitere Mitglieder mit <b>Hinzufügen</b> hinzu.  Die Zahl der Benutzer pro XAuth-Profil ist unbeschränkt.

## 17.1.5 IP Pools

Im Menü **IP Pools** wird eine Liste aller IP Pools für Ihre konfigurierten IPSec-Verbindungen angezeigt.

Wenn Sie bei einem IPSec-Peer für **IPv4-Adressenvergabe Server im IKE-Konfigurationsmodus** eingestellt haben, müssen Sie hier die IP-Pools, aus denen die IP-Adressen vergeben werden, definieren.

### 17.1.5.1 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
<b>IP-Poolname</b>	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
<b>IP-Adressbereich</b>	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld)

Feld	Beschreibung
	IP-Adresse des IP-Adress-Pools ein.
<b>DNS-Server</b>	<p><b>Primär:</b> 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><b>Sekundär:</b> Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

## 17.1.6 Optionen

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

### Felder im Menü Globale Optionen

Feld	Beschreibung
<b>IPSec aktivieren</b>	<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>
<b>Vollständige IPSec-Konfiguration löschen</b>	<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 <b>IPSec aktivieren</b> = nicht aktiviert.</p>
<b>IPSec-Debug-Level</b>	<p>Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Notfall</i> (höchste Priorität)</li> <li>• <i>Alarm</i></li> <li>• <i>Kritisch</i></li> <li>• <i>Fehler</i></li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Warnung</i></li> <li>• <i>Benachrichtigung</i></li> <li>• <i>Information</i></li> <li>• <i>Debug</i> (Standardwert, niedrigste Priorität)</li> </ul> <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
<b>IPSec über TCP</b>	<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>
<b>Initial Contact Message senden</b>	<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>
<b>SAs mit dem Status der ISP-Schnittstelle</b>	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich</p>



Feld	Beschreibung
<b>synchronisieren</b>	<p>der Status von <i>Aktiv</i> zu <i>Inaktiv</i>, <i>Ruhend</i> oder <i>Blockiert</i> geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Zero Cookies verwenden</b>	<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>
<b>Größe der Zero Cookies</b>	<p>Nur für <b>Zero Cookies verwenden</b> = 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>
<b>Dynamische RADIUS-Authentifizierung</b>	<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>

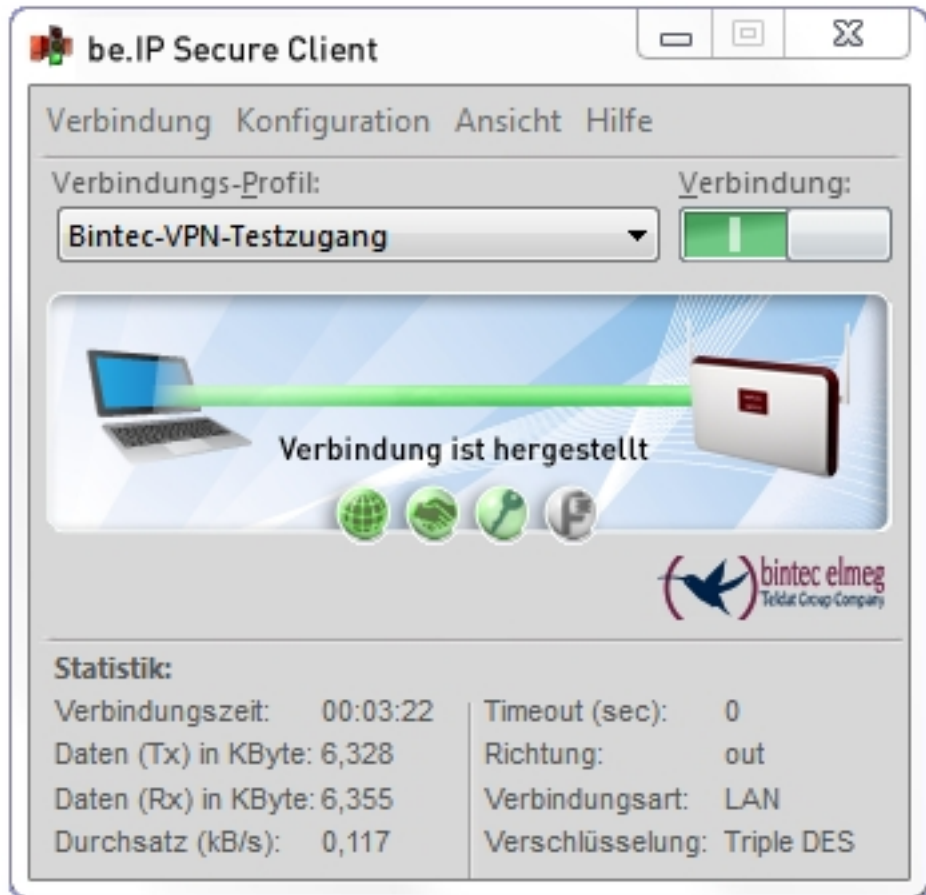
#### Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
<b>Zertifikatsanforderungs-Payloads nicht beachten</b>	<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>
<b>Zertifikatsanforderungs-Payloads senden</b>	<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>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
<b>Zertifikatsketten senden</b>	<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>
<b>CRLs senden</b>	<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>
<b>Key Hash Payloads senden</b>	<p>Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen.</p> <p>Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung. Aktivieren Sie diese Funktion mit <i>Aktiviert</i>, um dieses Verhalten zu unterdrücken.</p>

## 17.2 be.IP Secure Client

Hier können Sie die aktuelle Secure IPsec Client Software herunterladen. Weitere Informationen finden Sie auf [www.bintec-elmeg.com](http://www.bintec-elmeg.com).



## 17.3 LISP Light

Das Locator/ID Separation Protocol (LISP) bietet eine neue Art der Adressierung für eine bessere Strukturierung des Internets.

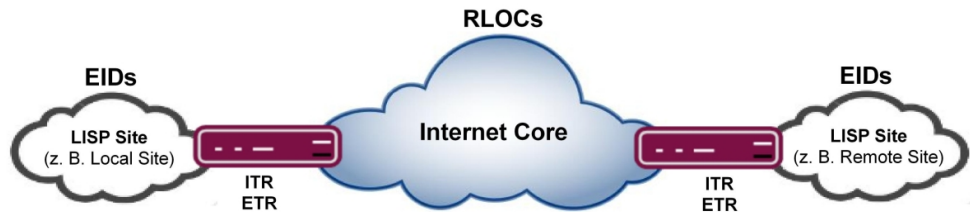
Es gibt viele Gründe, LISP einzuführen. Einer der wichtigsten ist die zunehmende Verbreitung mobiler Endgeräte. Wenn beim Ortswechsel eines Geräts immer die komplette IP-Adresse geändert werden muss, so ist das umständlich und lässt Routing-Tabellen unnötig anwachsen.

LISP basiert auf der Idee, die Angabe der Identität und des Standortes eines Geräts im Netz zu trennen. Dabei beschreibt der Parameter Routing Locator (RLOC) den Standort und der Parameter Endpoint Identifier (EID) die Identität. Ein Mapping-System verbindet beide Parameter.

Wenn man das LISP-Konzept auf Personen überträgt, leuchtet es unmittelbar ein: Wenn jemand seinen Wohnungssitz von Berlin nach Hamburg verlegt, ist er immer noch derselbe, er wohnt lediglich in einer anderen Stadt.

Bei der Verwendung herkömmlicher IP-Adressen sind Identität und Aufenthaltsort in der IP-Adresse zusammengefasst. Wenn ein Gerät über DHCP in einem anderen Netz eine neue IP-Adresse bekommt, hat diese nichts mit der vorher zugeteilten Adresse zu tun, d.h. nicht nur der Ort hat sich geändert sondern es wurde eine völlig neue Adresse vergeben. Dadurch verlieren alle Routen zur ursprünglichen Adresse ihre Gültigkeit.

Die Struktur des Internets kann man sich mit LISP unter dem Aspekt der Adressierung folgendermaßen vorstellen: Das Internet besteht aus einem öffentlichen Bereich, dem Internet Core, und aus privaten, LISP-fähigen Netzwerken, den LISP-Standorten (LISP Sites), die mit dem Internet Core verbunden sind. An den Übergangsstellen zwischen beiden arbeiten LISP-Router als Ingress Tunnel Router (ITR) und als Egress Tunnel Router (ETR). Ingress Tunnel Router sind Eingangsroutern in den Internet Core, Egress Tunnel Router sind Ausgangsroutern aus dem Internet Core. Beide Funktionen können auf ein und demselben Gerät realisiert sein:



Die beiden Parameter Routing Locator (RLOC) und Endpoint Identifier (EID) sind in der Praxis zwei "normale" IPv4- oder IPv6-Adressen. (IPv6-Adressen werden allerdings zur Zeit von LISP Light nicht unterstützt.) Der Routing Locator (RLOC) beschreibt das Routing über eine öffentliche, weltweit routbare IP-Adresse zu einer LISP-Site, also zu einem Standort im Internet. Mit dem Endpoint Identifier (EID) wird ein Rechner mit einer privaten Adresse innerhalb der LISP-Site angesprochen. Diese private IP-Adresse muss nur über alle miteinander verbundenen Sites eindeutig sein.

Wenn ein IP-Paket von einer LISP-Site zu einer anderen geroutet werden soll (z. B. von der Local Site zu einer Remote Site), muss das entsprechende RLOC-EID-Paar bekannt sein. Map Server und Map Resolver sorgen dafür, dass die Zuordnung von RLOC zu EID zur Verfügung steht. Map Server "lernen" RLOC-EID-Einträge von Egress Tunnel Routern und legen sie in einer Datenbank ab. Map Resolver akzeptieren die Map-Anfragen von Ingress Tunnel Routern und fragen die RLOC-EID-Einträge aus der Datenbank ab.

Beim Routen eines IP-Pakets packt der Ingress Tunnel Router das Paket ein, das den EID (Absender- und einer Empfängeradresse) bereits in seinem sogenannten "inneren" Header enthält. Das IP-Paket bekommt dadurch einen zusätzlichen Header, den sogenannten "äußeren" Header, mit dem RLOC, der ebenfalls aus Absender- und Empfängeradresse be-

steht. Wenn das IP-Paket mittels RLOC an der gewünschten LISP-Site eingetroffen ist, packt es der Egress Tunnel Router wieder aus. Über den EID im inneren Header gelangt das IP-Paket zum gewünschten Rechner.

Die Bezeichnung **LISP Light** bedeutet, dass eine Teilmenge der LISP-Spezifikation aus RFC 6830 implementiert wurde.

## 17.3.1 (ITR / ETR) Router

Im Menü **VPN->LISP Light-> (ITR / ETR) Router** wird eine Liste aller konfigurierten Egress Tunnel Router (ETR, oben) und aller Ingress Tunnel Router (ITR, unten) angezeigt. Das Gerät agiert also sowohl als Egress Tunnel Router als auch als Ingress Tunnel Router.

### 17.3.1.1 Egress Tunnel Router Hinzufügen

Hier können Sie Einstellungen für die Rolle als Egress Tunnel Router vornehmen. Für eine übliche LISP-Konfiguration müssen Sie mindestens einen Map Server konfigurieren.



#### Hinweis

Die Funktion eines Map Servers wird von LISP Light nicht zur Verfügung gestellt. Ähnlich einem externen DNS-Server müssen Sie diesen Dienst in Ihrem Netzwerk anderweitig zur Verfügung stellen. Informieren Sie sich anhand der Dokumentation ihres Servers, welche Einstellungen vorzunehmen sind.

Die eigene IP-Adresse wird dem Map Server bzw. den Map Servern mitgeteilt, um zu signalisieren, dass das Gerät Datenpakete empfangen kann bzw. über welche RLOC das Gerät als ETR erreichbar ist.

Ein Egress Tunnel Router (ETR) veröffentlicht EID-RLOC-Einträge für "seine" LISP-Sites, empfängt LISP-Daten, packt sie aus und schickt sie an die Rechner der Site, die im EID angegeben sind.

Das Menü **VPN->LISP Light->(ITR / ETR) Router-> Egress Tunnel Router Hinzufügen** besteht aus folgenden Feldern:

#### Felder im Menü Map-Server

Feld	Beschreibung
<b>IP-Adresse des Map-Server</b>	Geben Sie die IP-Adresse des Map Servers ein, der periodisch Map-Request-Meldungen erhalten soll.
<b>Schlüsseltyp (HMAC-Algorithmus)</b>	Die Nachrichten, die an den Map Server gesendet werden, können signiert werden. Hier können Sie den Algorithmus für die

Feld	Beschreibung
	<p>Signatur wählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>HMAC-SHA1-96</i></li> <li>• <i>HMAC-SHA2-256-128</i></li> <li>• <i>Keiner</i></li> </ul> <p><i>Keiner</i> schaltet die Signatur aus.</p>
<b>Schlüssel zur Authentisierung</b>	Der <b>Schlüssel zur Authentisierung</b> muss auch dem Map Server bekannt sein, damit er die Authentizität der Nachricht überprüfen kann.

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Map-Register-Dauer (in Sek.)</b>	<p>Konfigurieren Sie den zeitlichen Abstand zwischen zwei Registrierungs-Meldungen beim Map Server in Sekunden.</p> <p>Der Standardwert ist <i>60</i>.</p>
<b>HMAC Truncation</b>	<p>Die Signatur kann vollständig (<b>HMAC Truncation <i>Keine</i></b>) oder in einer verkürzten Form (<b>HMAC Truncation <i>Aktiviert</i></b>) in das Paket geschrieben werden.</p> <p><b>HMAC Truncation <i>Keine</i></b> ist die Standardeinstellung.</p>

### 173.1.2 Ingress Tunnel Router Hinzufügen

Hier können Sie Einstellungen für die Rolle als Ingress Tunnel Router vornehmen. Für eine übliche LISP-Konfiguration müssen Sie mindestens einen Map Resolver konfigurieren.



#### Hinweis

Die Funktion eines Map Resolver wird von LISP Light nicht zur Verfügung gestellt. Ähnlich einem externen DNS-Server müssen Sie diesen Dienst in Ihrem Netzwerk anderweitig zur Verfügung stellen. Informieren Sie sich anhand der Dokumentation ihres Map Resolver, welche Einstellungen vorzunehmen sind.

Ein Ingress Tunnel Router (ITR) ist dafür zuständig, EID-RLOC-Paare zu finden und in seinem Mapping Cache zu speichern. Dazu sendet er Map-Anfragen an einen Map Resolver.

Ein Ingress Tunnel Router packt die Daten ein und sendet Sie mithilfe der im RLOC angegebenen Adresse zur passenden LISP-Site.

Das Menü **VPN->LISP Light->Router (ITR/ETR)-> Ingress Tunnel Router Hinzufügen** besteht aus folgenden Feldern:

#### Felder im Menü Map-Resolvers

Feld	Beschreibung
<b>IP-Adresse des Map-Server</b>	Geben Sie die IP-Adresse des Map Resolvers ein, der die Map-Anfrage des ITR beantworten soll.  Um Ausfallsicherheit zu gewährleisten, kann mehr als ein Map Resolver konfiguriert werden.

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Minimale Map-Request-Dauer (in Sek.)</b>	Geben Sie die Zeit in Sekunden ein, die zwischen zwei Anfragen für dieselbe EID an diesen Map Resolver mindestens verstreichen soll. Dieser Parameter soll eine Überlastung des Map Resolvers verhindern.  Der Standardwert ist eine Sekunde.
<b>Max. Anzahl ausstehender Map-Requests</b>	Legen Sie fest, wieviel aufeinanderfolgende Map-Anfragen unbeantwortet bleiben dürfen, bevor zum nächsten Map Resolver weitergeschaltet wird.  Dieser Parameter definiert die Toleranz gegenüber Datenverlust.  Der Standardwert ist 2.
<b>Max. Verzögerung vor dem Umschalten zum nächster</b>	Legen Sie die Zeit in Sekunden fest, die bis zum Beantworten einer Map-Anfrage verstreichen darf, bevor zum nächsten Map Resolver weitergeschaltet wird.  Dieser Parameter definiert die Toleranz gegenüber Netzwerkverzögerungen.

Feld	Beschreibung
	Der Standardwert ist 3.

## 17.3.2 Lokale / Entfernte Standorte

"LISP-fähige" Netzwerke werden als LISP-Sites bezeichnet. Unter Local Site versteht man die Gesamtheit aller IP-Adressen (EIDs), die zum lokalen Netz gehören und ohne Tunnel erreichbar sind. Remote Sites sind Adressräume (EIDs), die nur über einen Tunnel erreichbar sind.

Im Menü **VPN->LISP Light->Lokale / Entfernte Standorte** wird eine Liste aller konfigurierten LISP-Sites angezeigt, getrennt nach Local Sites (oben) und Remote Sites (unten).

### 17.3.2.1 Lokalen Standort Hinzufügen

Hier können Sie Local Sites konfigurieren.

Das Menü **VPN->LISP Light->Lokale / Entfernte Standorte->Lokalen Standort Hinzufügen** besteht aus folgenden Feldern:

#### Felder im Menü Lokaler Standort

Feld	Beschreibung
<b>Instanz-ID</b>	Sie können eine Instance ID wählen, wenn Sie im Menü <b>VPN-&gt;LISP Light-&gt;EID Präfix Segregation (LISP Instanzen)-&gt; Instanz Hinzufügen</b> eine LISP Instance angelegt haben. Wenn Sie die Standardeinstellung <i>Not defined</i> belassen, wird eine Standard-Instanz verwendet.
<b>EID-Präfix (IP-Adresse / Länge)</b>	Geben Sie den gewünschten IP-Präfix des Endpoint Identifier (EID) ein. Verwenden Sie eine LAN-Adresse aus Ihrem Netz.
<b>IP-Adresse des Routing Locator (RLOC)</b>	Damit der Tunnel-Router auf der Gegenseite weiß, unter welcher IP-Adresse Sie erreichbar sind, wird eine global routbare IP-Adresse (RLOC in ETR-Rolle) automatisch gesetzt und angezeigt.

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Schnittstellenbindung</b>	Die Wahl einer Schnittstelle ist optional. Wenn derselbe EID für



Feld	Beschreibung
	mehrere Schnittstellen verwendet wird, kann man hier die Schnittstelle zuordnen.
<b>Lebensdauer des Datenbankeintrags (in Min.)</b>	Bezeichnet die Lebensdauer des Cache-Eintrags, die dem Map Server gemeldet wird, in Minuten  Der Standardwert ist <i>60</i> Minuten.
<b>EID Präfix aus dem Adressbaum ausschließen</b>	Wenn Sie einen zusammenhängenden Adressbereich verwenden wollen, belassen Sie die Standardeinstellung <i>auto</i> .  Aus einem bereits definierten Adressbereich können Sie einen Teilbereich entfernen. Dafür verwenden Sie separate Einträge mit der Einstellung <i>negative</i> .

### 17.3.2 Entfernten Standort Hinzufügen

Hier können Sie Remote Sites konfigurieren.

Das Menü **VPN->LISP Light->Lokale / Entfernte Standorte->Entfernten Standort Hinzufügen** besteht aus folgenden Feldern:

#### Felder im Menü Entfernter Standort

Feld	Beschreibung
<b>ID</b>	Sie können eine Instance ID wählen, wenn Sie im Menü <b>VPN-&gt;LISP Light-&gt;EID Präfix Segregation (LISP Instanzen)-&gt; Instanz Hinzufügen</b> eine LISP Instance angelegt haben. Wenn Sie die Standardeinstellung <i>Not defined</i> belassen, wird eine Standard-Instance verwendet.
<b>EID-Präfix (IP-Adresse / Länge)</b>	Geben Sie einen Adressbereich ein, der über Tunnel erreichbar ist.

### 17.3.3 EID Präfix Segregation (LISP Instanzen)

Im Menü **VPN->LISP Light->EID Präfix Segregation (LISP Instanzen)** wird eine Liste aller konfigurierten LISP Instanzen angezeigt.



### Hinweis

Wenn Sie nur ein einziges Netz verwenden wollen, brauchen Sie keine Instanzen anzulegen. Für diesen Fall wird eine Standard-Instanz verwendet.

Wenn Sie mehrere getrennte Netze verwenden wollen (gegebenenfalls mit überlappenden Adressräumen), müssen Sie für jedes Netz eine eigene Instanz anlegen.

### 173.3.1 Instanz Hinzufügen

Hier können Sie Instanzen konfigurieren.

Das Menü **VPN->LISP Light->EID Präfix Segregation (LISP Instanzen)-> Instanz Hinzufügen** besteht aus folgenden Feldern:

#### Felder im Menü LISP-Instanz

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie der Instanz einen Namen, damit Sie sie von anderen Instanzen unterscheiden können.
<b>Instanz-ID</b>	Für die erste Instanz, die Sie konfigurieren, können Sie den voreingestellten Wert <i>0</i> belassen. Bei allen folgenden Instanzen, die Sie konfigurieren, geben Sie jeweils einen anderen ganzzahligen Wert ein.  Für jede Instanz wird eine virtuelle Schnittstelle angelegt.

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Proxy-ETR-RLOC</b>	Geben Sie bei Bedarf die IP-Adresse eines Proxy-ETR an, an den alle IP-Pakete getunnelt werden, bei denen der Map Resolver "natives Weiterleiten" mitteilt.
<b>MTU der LISP-Schnittstelle</b>	Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die Verbindung zwischen den virtuellen LISP-Schnittstellen verwendet werden darf.  Der Standardwert ist <i>1444</i> .
<b>Maximale Anzahl der</b>	Geben Sie die maximale Anzahl der EID/RLOC-Einträge im Ca-

Feld	Beschreibung
<b>EID/RLOC-Einträge im Cache</b>	<p>che an.</p> <p>Der Standardwert ist <i>100</i>.</p>
<b>Maximale Anzahl von RLOC-Adressen pro EID/RLOC-Eintrag</b>	<p>Geben Sie die maximale Anzahl der RLOC-Einträge pro EID im Cache an.</p> <p>Der Standardwert ist <i>10</i>.</p>
<b>Standard TTL eines EID/RLOC-Eintragsim Cache (in Min.)</b>	<p>Normalerweise teilt der Server einen Wert für die TTL (time to live) mit. Hier können Sie einen Wert angeben, falls vom Server kein Wert angegeben wird (<b>Standard TTL-Modus = <i>Fallback</i></b>) oder dieser ignoriert werden soll (<b>Standard TTL-Modus = <i>Fest eingestellt</i></b>).</p>
<b>Standard TTL-Modus</b>	<p>Hier können Sie den Default TTL Mode wählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Fallback</i> (Standardwert): Vom Server wird kein TTL-Wert zur Verfügung gestellt. Der unter <b>Standard TTL eines EID/RLOC-Eintragsim Cache (in Min.)</b> eingegebene Wert wird verwendet.</li> <li>• <i>Fest eingestellt</i>: Der vom Server zur Verfügung gestellte TTL-Wert wird ignoriert. Der unter <b>Standard TTL eines EID/RLOC-Eintragsim Cache (in Min.)</b> eingegebene Wert wird verwendet.</li> </ul>

## 17.4 L2TP

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

Ihr bintec elmeg-Gerät unterstützt die folgenden zwei Modi:

- L2TP-LNS-Modus (L2TP Network Server): nur für eingehende Verbindungen
- L2TP-LAC-Modus (L2TP Access Concentrator): nur für ausgehende Verbindungen.

Folgendes ist bei der Konfiguration von Server und Client zu beachten: Auf beiden Seiten (LAC und LNS) muss jeweils ein L2TP-Tunnelprofil angelegt werden. Auf der Auslöserseite (LAC) wird das entsprechende L2TP-Tunnelprofil für den Verbindungsaufbau verwendet. Auf der Responderseite (LNS) wird das L2TP-Tunnelprofil für die Verbindungsannahme

benötigt.

## 17.4.1 Tunnelprofile

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

### 17.4.1.1 Neu

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

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

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Beschreibung</b>	<p>Geben Sie eine Beschreibung für das aktuelle Profil ein.</p> <p>Ihr Gerät benennt die Profile automatisch mit <i>L2TP</i> und nummeriert diese, der Wert kann jedoch geändert werden.</p>
<b>Lokaler Hostname</b>	<p>Geben Sie den Hostnamen für LNS bzw. LAC ein.</p> <ul style="list-style-type: none"> <li>• <i>LAC</i>: Der lokale Hostname wird in abgehenden Tunnelaufbaumeldungen zur Identifizierung dieses Geräts aufgenommen und wird dem entfernten Hostnamen eines der am LNS konfigurierten Tunnelprofile zugeordnet. Bei diesen Tunnelaufbaumeldungen handelt es sich um die vom LAC ausgesandten SCCRQs (Start Control Connection Request) und die vom LNS ausgesandten SCCRPs (Start Control Connection Reply).</li> <li>• <i>LNS</i>: Entspricht dem Wert für <b>Entfernter Hostname</b> der eingehenden Tunnelaufbaumeldung vom LAC.</li> </ul>
<b>Entfernter Hostname</b>	<p>Geben Sie den Hostnamen des LNS bzw. LAC ein:</p> <ul style="list-style-type: none"> <li>• <i>LAC</i>: Definiert den Wert für <b>Lokaler Hostname</b> des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). Ein im LAC konfigurierter <b>Lokaler Hostname</b> muss zu <b>Entfernter Hostnamen</b> passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt.</li> <li>• <i>LNS</i>: Definiert den <b>Lokaler Hostnamen</b> des LAC. Falls das Feld <b>Entfernter Hostname</b> auf dem LNS leer bleibt, wird das dazugehörige Profil als Standardeintrag qualifiziert, der für al-</li> </ul>

Feld	Beschreibung
	le ankommenden Rufe benutzt wird, für die kein Profil mit passendem entfernten Hostnamen gefunden werden kann.
<b>Passwort</b>	<p>Geben Sie das Passwort ein, welches für die Tunnel-Authentifizierung benutzt wird. Die Authentifizierung zwischen LAC und LNS erfolgt in beiden Richtungen, d. h. der LNS prüft den <b>Lokaler Hostnamen</b> und das <b>Passwort</b>, die in der SCCRP des LAC enthalten sind und vergleicht sie mit denen, die im relevanten Profil angegeben sind. Der LAC macht das Gleiche mit den jeweiligen Feldern der SCCRP des LNS.</p> <p>Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.</p>

#### Felder im Menü Parameter des LAC-Modus

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

Feld	Beschreibung
	Mögliche Werte sind <i>0</i> bis <i>65535</i> . Der Standardwert ist <i>1701</i> (RFC 2661).

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>Lokale IP-Adresse</b>	Geben Sie die IP-Adresse ein, die als Quelladresse für alle L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.  Falls dieses Feld frei gelassen wird, nutzt Ihr Gerät die IP-Adresse der Schnittstelle, über das der L2TP-Tunnel die entfernte IP-Adresse erreicht.
<b>Hello-Intervall</b>	Geben Sie den Zeitabstand (in Sekunden) zwischen dem Senden von zwei L2TP-HELLO-Meldungen ein. Diese Meldungen dienen dazu, den Tunnel offen zu halten.  Verfügbare Werte sind <i>0</i> bis <i>255</i> , der Standardwert ist <i>30</i> . Der Wert <i>0</i> bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.
<b>Minimale Zeit zwischen Versuchen</b>	Geben Sie die Mindestzeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat.  Die Wartezeit wird dynamisch verlängert, bis sie die <b>Maximale Zeit zwischen Versuchen</b> erreicht hat. Verfügbare Werte sind <i>1</i> bis <i>255</i> , der Standardwert ist <i>1</i> .
<b>Maximale Zeit zwischen Versuchen</b>	Geben Sie die maximale Zeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat.  Verfügbare Werte sind <i>8</i> bis <i>255</i> , der Standardwert ist <i>16</i> .
<b>Maximale Anzahl Wiederholungen</b>	Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden.  Verfügbare Werte sind <i>8</i> bis <i>255</i> , der Standardwert ist <i>5</i> .

Feld	Beschreibung
<b>Sequenznummern der Datenpakete</b>	<p>Wählen Sie aus, ob Ihr Gerät für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folgenummern benutzen soll oder nicht.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

## 17.4.2 Benutzer

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

### 17.4.2.1 Neu

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

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

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Beschreibung</b>	<p>Geben Sie einen beliebigen Namen ein, um den L2TP-Partner eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden. Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.</p>
<b>Verbindungstyp</b>	<p>Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerkserver (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>LNS</i> (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt.</li> <li>• <i>LAC</i>: Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.</li> </ul>

Feld	Beschreibung
<b>Tunnelprofil</b>	Nur für <b>Verbindungstyp</b> = <i>LAC</i>  Wählen Sie ein im Menü <b>Tunnelprofil</b> erstelltes Profil für die Verbindung zu diesem L2TP-Partner aus.
<b>Benutzername</b>	Geben Sie die Kennung Ihres Geräts ein.
<b>Passwort</b>	Geben Sie das Passwort ein.
<b>Immer aktiv</b>	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.  Mit <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion nicht aktiv.
<b>Timeout bei Inaktivität</b>	Nur wenn <b>Immer aktiv</b> deaktiviert ist  Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.  Zur Verfügung stehen Werte von <i>0</i> bis <i>3600</i> (Sekunden). <i>0</i> deaktiviert den Short Hold. Der Standardwert ist <i>300</i> .

#### Felder im Menü IP-Modus und Routen

Feld	Beschreibung
<b>IP-Adressmodus</b>	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein.</li> <li>• <i>IP-Adresse bereitstellen</i>: Nur für <b>Verbindungstyp</b> = <i>LNS</i>. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse.</li> <li>• <i>IP-Adresse abrufen</i>: Nur für <b>Verbindungstyp</b> = <i>LAC</i>. Ihr Gerät erhält dynamisch eine IP-Adresse.</li> </ul>
<b>IP-Zuordnungspool (IPCP)</b>	Nur für <b>IP-Adressmodus</b> = <i>IP-Adresse bereitstellen</i>  Wählen Sie einen im Menü <b>WAN-&gt;Internet + Einwählen-&gt;IP</b>



Feld	Beschreibung
	<b>Pools</b> konfigurierten IP Pool aus.
<b>Standardroute</b>	Nur für <b>IP-Adressmodus</b> = <i>IP-Adresse abrufen</i> und <i>Statisch</i>  Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.  Mit <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion nicht aktiv .
<b>NAT-Eintrag erstellen</b>	Nur für <b>IP-Adressmodus</b> = <i>IP-Adresse abrufen</i> und <i>Statisch</i>  Wählen Sie aus, ob Network Address Translation (NAT) für diese Verbindung aktiviert werden soll.  Mit <i>Aktiviert</i> wird die Funktion aktiv.  Standardmäßig ist die Funktion nicht aktiv.
<b>Lokale IP-Adresse</b>	Nur für <b>IP-Adressmodus</b> = <i>Statisch</i>  Geben Sie die WAN-IP-Adresse Ihres Geräts ein.
<b>Routeneinträge</b>	Nur für <b>IP-Adressmodus</b> = <i>Statisch</i>  Geben Sie <b>Entfernte IP-Adresse</b> und <b>Netzmaske</b> des LANs des L2TP-Partners und die dazugehörige <b>Metrik</b> ein. Fügen Sie weitere Einträge mit <b>Hinzufügen</b> hinzu.

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>Blockieren nach Verbindungsfehler für</b>	Geben Sie ein, für wie viele Sekunden nach einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.  Der Standardwert ist <i>300</i> .
<b>Authentifizierung</b>	Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>PAP/CHAP/MS-CHAP</i> (Standardwert): Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.)</li> <li>• <i>PAP</i>: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen.</li> <li>• <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen.</li> <li>• <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen.</li> <li>• <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen.</li> <li>• <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen.</li> <li>• <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.</li> </ul>
<b>Verschlüsselung</b>	<p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Wenn <b>Verschlüsselung</b> gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i>: Es wird keine MPP-Verschlüsselung angewendet.</li> <li>• <i>Aktiviert</i> (Standardwert): Die MPP-Verschlüsselung V2 mit 128 Bit wird nach RFC 3078 angewendet.</li> <li>• <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.</li> </ul>
<b>LCP-Erreichbarkeitsprüfung</b>	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

### Felder im Menü IP-Optionen

Feld	Beschreibung
<b>OSPF-Modus</b>	<p>Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing-Informationen berücksichtigt und über aktive Schnittstellen propagiert.</li> <li>• <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet.</li> <li>• <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.</li> </ul>
<b>Proxy-ARP-Modus</b>	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner.</li> <li>• <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>Aktiv</i> (aktiv) oder <i>Ruhend</i> (ruhend) ist. Bei <i>Ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will.</li> <li>• <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner</li> </ul>

Feld	Beschreibung
	(aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner besteht.
<b>DNS-Aushandlung</b>	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für <b>Primärer DNS-Server</b> und <b>Sekundärer DNS-Server</b> und <b>WINS-Server Primär</b> und <b>Sekundär</b> vom L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

### 17.4.3 Optionen

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

#### Felder im Menü Globale Optionen

Feld	Beschreibung
<b>UDP-Zielport</b>	<p>Geben Sie den Port ein, der vom LNS auf ankommende L2TP-Tunnelverbindungen überwacht werden soll.</p> <p>Verfügbare Werte sind alle ganzen Zahlen von <i>1</i> bis <i>65535</i>, der Standardwert ist <i>1701</i>, wie es in RFC 2661 vorgegeben ist.</p>
<b>UDP-Quellportauswahl</b>	<p>Wählen Sie aus, ob der LNS nur den überwachten Port (<b>UDP-Zielport</b>) als lokalen Quellport für die L2TP-Verbindung nutzen soll.</p> <p>Mit <i>Fest eingestellt</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

## 18 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 *Konfiguration* auf Seite 358.

## 18.1 Richtlinien

### 18.1.1 IPv4-Filterregeln


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


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

### 18.1.1.1 Neu



#### Hinweis

Informationen zur Auswahl der Vertrauenswürdige Schnittstellen finden Sie hier: [IPv4-Filterregeln](#) auf Seite 345.

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
<b>Quelle</b>	<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 <b>Firewall-&gt;Schnittstellen-&gt;Gruppen</b>), Adressen (siehe <b>Firewall-&gt;Adressen-&gt;Adressliste</b>) und Adressgruppen (siehe <b>Firewall-&gt;Adressen-&gt;Gruppen</b>) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.</p>
<b>Ziel</b>	<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 <b>Firewall-&gt;Schnittstellen-&gt;Gruppen</b>), Adressen (siehe <b>Firewall-&gt;Adressen-&gt;Adressliste</b>) und Adressgruppen (siehe <b>Firewall-&gt;Adressen-&gt;Gruppen</b>) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.</p>
<b>Dienst</b>	<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>



Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>ftp</i></li> <li>• <i>telnet</i></li> <li>• <i>smtp</i></li> <li>• <i>dns</i></li> <li>• <i>http</i></li> <li>• <i>nntp</i></li> <li>• <i>Internet</i></li> <li>• <i>Netmeeting</i></li> </ul> <p>Weitere Dienste werden in <b>Firewall-&gt;Dienste-&gt;Dienstliste</b> angelegt.</p> <p>Außerdem stehen die in <b>Firewall-&gt;Dienste-&gt;Gruppen</b> konfigurierten Dienstgruppen zur Auswahl.</p>
<b>Aktion</b>	<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"> <li>• <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet.</li> <li>• <i>Verweigern</i>: Die Pakete werden abgewiesen.</li> <li>• <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.</li> </ul>

## 18.1.2 IPv6-Filterregeln

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

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

enswürdigen 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.

### 18.1.2.1 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
<b>Quelle</b>	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des

Feld	Beschreibung
	<p>Pakets aus.</p> <p>In der Liste stehen alle WAN-/ LAN-Schnittstellen, Schnittstellengruppen (siehe <b>Firewall-&gt;Schnittstellen-&gt;IPv6-Gruppen</b>), Adressen (siehe <b>Firewall-&gt;Adressen-&gt;Adressliste</b>) und Adressgruppen (siehe <b>Firewall-&gt;Adressen-&gt;Gruppen</b>) zur Auswahl, für die IPv6 aktiviert ist.</p>
<b>Ziel</b>	<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 <b>Firewall-&gt;Schnittstellen-&gt;IPv6-Gruppen</b>), Adressen (siehe <b>Firewall-&gt;Adressen-&gt;Adressliste</b>) und Adressgruppen (siehe <b>Firewall-&gt;Adressen-&gt;Gruppen</b>) zur Auswahl, für die IPv6 aktiviert ist.</p>
<b>Dienst</b>	<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"> <li>• <i>ftp</i></li> <li>• <i>telnet</i></li> <li>• <i>smtp</i></li> <li>• <i>dns</i></li> <li>• <i>http</i></li> <li>• <i>nntp</i></li> </ul> <p>Weitere Dienste werden in <b>Firewall-&gt;Dienste-&gt;Diensteliste</b> angelegt.</p> <p>Außerdem stehen die in <b>Firewall-&gt;Dienste-&gt;Gruppen</b> konfigurierten Dienstgruppen zur Auswahl.</p>
<b>Aktion</b>	<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"> <li>• <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Verweigern</i>: Die Pakete werden abgewiesen.</li> <li>• <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.</li> </ul>

### 18.1.3 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
<b>Status der IPv4-Firewall</b>	<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>
<b>Protokollierte Aktionen</b>	<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"> <li>• <i>Alle</i> (Standardwert): Alle Firewall-Aktivitäten werden angezeigt.</li> <li>• <i>Verweigern</i>: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion".</li> <li>• <i>Annehmen</i>: Nur Accept-Ereignisse werden angezeigt.</li> <li>• <i>Keiner</i>: Systemprotokoll-Nachrichten werden nicht erzeugt.</li> </ul>
<b>Vollständige IPv4-Filterung</b>	<p>Bei TCP-Sessions überwacht die SIF im ersten Schritt, ob eine</p>

Feld	Beschreibung
	<p>Session korrekt und vollständig aufgebaut wird. Unvollständige Sessions werden blockiert. Im zweiten Schritt erfolgt die eigentliche Filterung. Für diesen "Normalfall" ist die Standardeinstellung <b>Vollständige IPv4-Filterung</b> <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, so ist die TCP-Session aus Sicht der SIF unvollständig und der Router würde diesen Datenverkehr nicht zulassen.</p> <p>Um Datenverkehr solcher unvollständiger TCP-Sessions beim Spezialfall identischer Eingangs- und Ausgangsschnittstelle zu erlauben, müssen Sie <b>Vollständige IPv4-Filterung</b> deaktivieren. Etwaige existierende SIF-Filterregeln dazu werden ignoriert.</p>
<b>STUN Handler</b>	<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>
<b>Port-STUN-Server</b>	<p>Nur für <b>STUN Handler</b> = 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
<b>UDP-Inaktivität</b>	<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>
<b>TCP-Inaktivität</b>	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine TCP - Session als abgelaufen betrachtet werden soll (in Sekunden).</p>

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

#### Felder im Menü Firewall auf Werkseinstellungen zurücksetzen

Feld	Beschreibung
<b>Firewall auf Werkseinstellungen zurücksetzen</b>	Klicken Sie auf <b>Zurücksetzen</b> um die Firewall auf Werkseinstellungen zurückzusetzen.

## 18.2 Schnittstellen

### 18.2.1 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.

#### 18.2.1.1 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
<b>Beschreibung</b>	Geben Sie eine beliebige Beschreibung der IPv4-Schnittstellen-Gruppe ein.
<b>Mitglieder</b>	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte <b>Auswahl</b> .

## 18.2.2 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.

### 18.2.2.1 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
<b>Beschreibung</b>	Geben Sie eine beliebige Beschreibung der IPv6-Schnittstellen-Gruppe ein.
<b>Mitglieder</b>	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte <b>Auswahl</b> .

## 18.3 Adressen

### 18.3.1 Adressliste

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

### 18.3.1.1 Neu

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

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

#### Felder im Menü Basisparameter

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



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

## 18.3.2 Gruppen

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

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

### 18.3.2.1 Neu

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



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

#### Felder im Menü Basisparameter

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

## 18.4 Dienste

## 18.4.1 Dienstliste

Im Menü **Firewall->Dienste->Dienstliste** wird eine Liste aller zur Verfügung stehender Dienste angezeigt. Wählen Sie das Symbol , um vorhandenen Einträge zu bearbeiten. Mithilfe des -Symbols können Sie Einträge löschen.



### Hinweis

Dienst wird auch aus der Liste der NAT-Dienste gelöscht! Wiederherstellung nur durch Factory Reset möglich.

### 18.4.1.1 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
<b>Beschreibung</b>	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
<b>Protokoll</b>	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
<b>Zielportbereich</b>	Nur für <b>Protokoll</b> = <i>TCP, UDP/TCP</i> oder <i>UDP</i>  Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll.  Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen.  Mögliche Werte sind 1 bis 65535.
<b>Quellportbereich</b>	Nur für <b>Protokoll</b> = <i>TCP, UDP/TCP</i> oder <i>UDP</i>  Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port

Feld	Beschreibung
	<p>an.</p> <p>Soll ein Portnummernbereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Portbereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen.</p> <p>Mögliche Werte sind 1 bis 65535.</p>
<b>Typ</b>	<p>Nur für <b>Protokoll</b> = <i>ICMP</i></p> <p>Das Feld <b>Typ</b> gibt die Klasse der ICMP-Nachrichten an, das Feld <b>Code</b> spezifiziert die Art der Nachricht genauer.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert)</li> <li>• <i>Echo Reply</i></li> <li>• <i>Destination Unreachable</i></li> <li>• <i>Source Quench</i></li> <li>• <i>Redirect</i></li> <li>• <i>Echo</i></li> <li>• <i>Time Exceeded</i></li> <li>• <i>Parameter Problem</i></li> <li>• <i>Timestamp</i></li> <li>• <i>Timestamp Reply</i></li> <li>• <i>Information Request</i></li> <li>• <i>Information Reply</i></li> <li>• <i>Address Mask Request</i></li> <li>• <i>Address Mask Reply</i></li> </ul>
<b>Code</b>	<p>Nur für <b>Typ</b> = <i>Destination Unreachable</i> stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert)</li> <li>• <i>Net Unreachable</i></li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Host Unreachable</i></li> <li>• <i>Protocol Unreachable</i></li> <li>• <i>Port Unreachable</i></li> <li>• <i>Fragmentation Needed</i></li> <li>• <i>Communication with Destination Network is Administratively Prohibited</i></li> <li>• <i>Communication with Destination Host is Administratively Prohibited</i></li> </ul>

## 18.4.2 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.

### 18.4.2.1 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
<b>Beschreibung</b>	Geben Sie eine beliebige Beschreibung der Service-Gruppe ein.
<b>Mitglieder</b>	Wählen Sie aus den zur Verfügung stehenden Service-Aliasen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte <b>Auswahl</b> .

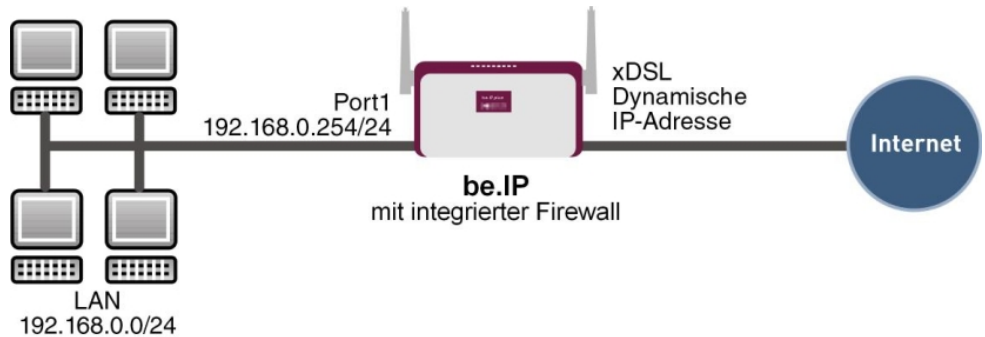
## 18.5 Konfiguration

### 18.5.1 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>
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</i> und <i>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> 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	ANY
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	be.IP
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	any
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Verweigern

**Filterregel 4: Zugriff auf alle Dienste im Internet erlauben (Geschäftsführer)**

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Geschäftsführer
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	ANY
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	any
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Zugriff

**Filterregel 5: Zugriff auf das Internet erlauben (Mitarbeiter)**

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Netzwerk_Intern
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	ANY
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Internetports
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Zugriff



## 19 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)
- Bereitstellung öffentlicher Internetzugänge (Hotspot)
- Ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten (Wake-On-LAN)
- Eine Aufzeichnung des Datenverkehrs über eine bestimmte Schnittstelle (Trace-Schnittstelle)

### 19.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu

ermöglichen.

## Name-Server

Unter **Lokale Dienste->DNS->DNS-Server->Neu** werden die IP-Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der schnittstellengebundenen 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 entsprechenden 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.

### 19.1.1 Globale Einstellungen

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Domänenname</b>	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
<b>WINS-Server</b> <b>Primär</b> <b>Sekundär</b>	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
<b>Positiver Cache</b>	<p>Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Negativer Cache</b>	<p>Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Cache-Größe</b>	<p>Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein.</p> <p>Wird dieser Wert erreicht, wird bei einem neu hinzukommenden</p>

Feld	Beschreibung
	<p>Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird <b>Cache-Größe</b> vom Benutzer heruntersgesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. <b>Cache-Größe</b> 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>
<b>Maximale TTL für positive Cacheeinträge</b>	<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 <b>Maximale TTL für positive Cacheeinträge</b> überschreitet.</p> <p>Der Standardwert ist <i>86400</i>.</p>
<b>Maximale TTL für negative Cacheeinträge</b>	<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>
<b>Alternative Schnittstelle, um DNS-Server zu erhalten</b>	<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
<b>Als DHCP-Server</b>	<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"> <li>• <i>Keiner</i>: Es wird keine Name-Server-Adresse übermittelt.</li> <li>• <i>Eigene IP-Adresse</i> (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>DNS-Einstellung</i>: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.</li> </ul>
<b>Als IPCP-Server</b>	<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"> <li>• <i>Keiner</i>: Es wird keine Name-Server-Adresse übermittelt.</li> <li>• <i>Eigene IP-Adresse</i>: Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt.</li> <li>• <i>DNS-Einstellung</i> (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.</li> </ul>

## 19.1.2 DNS-Server

Im Menü **Lokale Dienste->DNS->DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

### 19.1.2.1 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
<b>Admin-Status</b>	<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.
<b>Beschreibung</b>	Geben Sie eine Beschreibung für den DNS-Server ein.
<b>Priorität</b>	<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) oder mehreren Schnittstellen mehrere Paare von DNS-Servern (<b>Primärer DNS-Server</b> und <b>Sekundärer DNS-Server</b>) 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>
<b>Schnittstellenmodus</b>	<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"> <li>• <i>Statisch</i></li> <li>• <i>Dynamisch</i> (Standardwert)</li> </ul>
<b>Schnittstelle</b>	<p>Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll.</p> <p>Die gewählte Schnittstelle ist für ausgehende DNS-Anfragen relevant. Diese Schnittstelle wird für DNS-Client-Anfragen verwendet, die an den Router gerichtet sind oder vom Router selbst erzeugt wurden.</p> <p>Bei <b>Schnittstellenmodus</b> = <i>Statisch</i></p> <p>Mit der Einstellung <i>Beliebig</i> wird ein DNS-Server für alle Schnittstellen konfiguriert.</p>
<b>IP-Version</b>	<p>Wählen Sie die verwendete IP-Version aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul> <p>Standardmäßig ist IPv4 ausgewählt.</p>
<b>Primärer IPv4-DNS-Server</b>	<p>Nur bei <b>Schnittstellenmodus</b> = <i>Statisch</i></p> <p>Geben Sie die IPv4-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
<b>Sekundärer IPv4-DNS-Server</b>	<p>Nur bei <b>Schnittstellenmodus</b> = <i>Statisch</i></p> <p>Geben Sie optional die IPv4-Adresse eines alternativen Name-Servers ein.</p>
<b>Primärer IPv6-DNS-Server</b>	<p>Nur bei <b>Schnittstellenmodus</b> = <i>Statisch</i></p> <p>Geben Sie die IPv6-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
<b>Sekundärer IPv6-DNS-Server</b>	<p>Nur bei <b>Schnittstellenmodus</b> = <i>Statisch</i></p> <p>Geben Sie optional die IPv6-Adresse eines alternativen Name-Servers ein.</p>

### 19.1.3 Statische Hosts

Im Menü **Lokale Dienste->DNS->Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

#### 19.1.3.1 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
<b>Standarddomäne</b>	Hier wird die Domäne angezeigt, die Sie im Menü <b>DNS-&gt;Globale Einstellungen</b> als Domännennamen eingetragen haben.
<b>DNS-Hostname</b>	Geben Sie den Host-Namen ein, dem die in diesem Menü definierte <b>IP-Adresse</b> zugeordnet werden soll, wenn eine DNS-

Feld	Beschreibung
	<p>Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage negativ beantwortet wird, wird keine Adresse mitgeteilt.</p> <p>Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.bintec-elmeg.com.</p> <p>Wenn Sie einen einfachen Namen angeben (z. B. <i>router</i>), wird dieser durch die Standarddomäne zu einem vollständigen DNS-Namen (Fully Qualified Domain Name, FQDN) ergänzt. Wenn Sie einen Namen in der Struktur eines FQDN eingeben (also durch "." getrennte Zeichenfolgen), so wird der Eintrag als FQDN interpretiert und nicht erweitert. Der für einen vollständigen FQDN erforderliche, schließende "." wird ggf. automatisch ergänzt.</p> <p>Einträge mit Leerzeichen sind nicht erlaubt.</p>
<b>Antwort</b>	<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"> <li>• <i>Negativ</i>: Eine DNS-Anfrage nach <b>DNS-Hostname</b> wird negativ beantwortet.</li> <li>• <i>Positiv</i> (Standardwert): Eine DNS-Anfrage nach <b>DNS-Hostname</b> wird mit der dazugehörigen <b>IP-Adresse</b> beantwortet.</li> <li>• <i>Keine</i>: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.</li> </ul>
<b>IPv4-Adresse</b>	<p>Nur bei <b>Antwort</b> = <i>Positiv</i></p> <p>Geben Sie die IPv4-Adresse ein, die nach <b>DNS-Hostname</b> zugeordnet wird.</p>
<b>IPv6-Adresse</b>	<p>Nur bei <b>Antwort</b> = <i>Positiv</i></p> <p>Geben Sie die IPv6-Adresse ein, die nach <b>DNS-Hostname</b> zugeordnet wird.</p>



## 19.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste->DNS->Domänenweiterleitung** wird eine Liste aller konfigurierten Weiterleitungen für definierte Domänen angezeigt.

### 19.1.4.1 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
<b>Weiterleiten</b>	<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"> <li>• <i>Host</i> (Standardwert)</li> <li>• <i>Domäne</i></li> </ul>
<b>Host</b>	<p>Nur für <b>Weiterleiten</b> = <i>Host</i></p> <p>und <b>Weiterleiten an</b> = <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 <b>OK</b> der Eintrag mit dem im Menü <b>Lokale Dienste-&gt;DNS-&gt;Globale Einstellungen</b> unter <b>Domänenname</b> eingetragenen Namen ergänzt.</p>
<b>Domäne</b>	<p>Nur für <b>Weiterleiten</b> = <i>Domäne</i></p> <p>und <b>Weiterleiten an</b> = <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</p>

Feld	Beschreibung
	nach Bestätigung mit <b>OK</b> automatisch eine führende Wildcard "*" eingefügt.
<b>Weiterleiten an</b>	<p>Wählen Sie aus, ob zutreffende DNS-Anfragen an den DNS-Server einer <b>Schnittstelle</b> oder an einen manuell konfigurierten <b>DNS-Server</b> weitergeleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Schnittstelle</i> (Standardwert): Anfragen werden an den DNS-Server entweder einer automatisch gewählten oder einer manuell konfigurierten Schnittstelle weitergeleitet.</li> <li>• <i>DNS-Server</i>: Anfragen werden an einen definierten <b>DNS-Server</b> weitergeleitet.</li> </ul>
<b>Zielschnittstelle</b>	<p>Nur für <b>Weiterleiten an</b> = <i>Schnittstelle</i></p> <p>Wählen Sie die Schnittstelle aus, an deren DNS-Server Anfragen weitergeleitet werden sollen.</p>
<b>Quellschnittstelle</b>	<p>Hier können Sie eine Quellschnittstelle der DNS-Anfragen für die Domainweiterleitung festlegen. Diese Option steht sowohl für Weiterleitungen an eine Schnittstelle als auch für Weiterleitungen an bestimmte DNS-Server zu Verfügung. Dies ermöglicht es, DNS-Anfragen aus verschiedenen Netzsegmenten auch an verschiedene DNS-Server zu senden. So können Sie z. B. die Anfragen aus einem Gästernetz an einen Webfilter-DNS leiten und unerwünschte Inhalte ausfiltern.</p>
<b>Primärer DNS-Server (IPv4/IPv6)</b>	<p>Nur für <b>Weiterleiten an</b> = <i>DNS-Server</i></p> <p>Geben Sie die IPv4/IPv6-Adresse des primären DNS-Servers ein.</p>
<b>Sekundärer DNS-Server (IPv4/IPv6)</b>	<p>Nur für <b>Weiterleiten an</b> = <i>DNS-Server</i></p> <p>Geben Sie IPv4/IPv6-Adresse des sekundären DNS-Servers ein.</p>

## 19.1.5 Dynamische Hosts

Im Menü **Lokale Dienste->DNS->Dynamische Hosts** sehen Sie die relevanten Angaben zu den Dynamischen DNS-Einträgen.

## 19.1.6 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.

## 19.1.7 Statistik

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

### Felder im Menü DNS-Statistiken

Feld	Beschreibung
<b>Empfangene DNS-Pakete</b>	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
<b>Ungültige DNS-Pakete</b>	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
<b>DNS-Anfragen</b>	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
<b>Cache-Treffer</b>	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
<b>Weitergeleitete Anfragen</b>	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
<b>Cache-Trefferrate (%)</b>	Zeigt die Anzahl der <b>Cache-Treffer</b> pro DNS-Anfrage in Prozent an.
<b>Erfolgreich beantwortete Anfragen</b>	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.

Feld	Beschreibung
<b>Serverfehler</b>	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

## 19.2 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.

### 19.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü HTTPS-Parameter

Feld	Beschreibung
<b>HTTPS-TCP-Port</b>	<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>
<b>Lokales Zertifikat</b>	<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"> <li><i>Intern</i> (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möchten.</li> <li>&lt;Zertifikatsname&gt;: Wählen Sie ein unter <b>Systemverwaltung-&gt;Zertifikate-&gt;Zertifikatsliste</b> eingetragenes Zertifikat aus.</li> </ul>

## 19.3 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.

### 19.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

#### 19.3.1.1 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
<b>Hostname</b>	Geben Sie den vollständigen Hostnamen genau so ein, wie er beim DynDNS-Provider registriert ist.

Feld	Beschreibung
<b>Schnittstelle</b>	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internetanbieters).
<b>Benutzername</b>	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
<b>Passwort</b>	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
<b>Provider</b>	<p>Wählen Sie den DynDNS-Provider aus, bei dem die eingegebenen Daten registriert sind.</p> <p>Es stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden.</p> <p>Weitere DynDNS-Provider können im Menü <b>Lokale Dienste-&gt;DynDNS-Client-&gt;DynDNS-Provider</b> konfiguriert werden.</p> <p>Der Standardwert ist <i>DynDNS</i>.</p>
<b>Aktualisierung aktivieren</b>	<p>Wählen Sie aus, ob der hier konfigurierte DynDNS-Eintrag aktiviert und die aktuelle IP-Adresse der ausgewählten Schnittstelle an den Anbieter übermittelt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>HTTPS/SSL</b>	<p>Diese Option steht nur zur Verfügung, wenn der von Ihnen ausgewählte DynDNS-Anbieter SSL unterstützt. Im Menü <b>Lokale Dienste-&gt;DynDNS-Client-&gt;DynDNS-Provider</b> können Sie ggf. selbst einen Anbieter mit dieser Option einrichten.</p> <p>Aktivieren Sie die Option, um zwischen Ihrem Gerät und dem DynDNS-Anbieter eine verschlüsselte Verbindung mittels SSL aufzubauen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Zertifikatsüberprüfung</b>	Aktivieren Sie diese Funktion, um das SSL-Zertifikat des Ser-

Feld	Beschreibung
	vers zu überprüfen.
<b>IP-Version</b>	<p>Diese Option steht nur zur Verfügung, wenn der von Ihnen ausgewählte DynDNS-Anbieter für beide IP-Versionen über entsprechende Server-Adressen verfügt. Wählen Sie die IP-Version der Adresse, die Sie beim DynDNS-Anbieter aktualisieren wollen.</p> <p>Mögliche Werte:</p> <p>IPv4</p> <p>IPv6.</p> <p>Um ggf. sowohl eine IPv4- als auch die IPv6-Adresse einer Schnittstelle zu aktualisieren, legen sie zwei Einträge mit ansonsten gleichen Einstellungen an. Informieren Sie sich bei Ihrem Anbieter, ob dieser Mehrfachaktualisierungen unterstützt!</p>

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Mail-Exchanger (MX)</b>	<p>Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll.</p> <p>Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.</p>
<b>Wildcard</b>	<p>Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von <b>Hostname</b> zur aktuellen IP-Adresse von <b>Schnittstelle</b> aktiviert werden soll (Erweiterte Namensauflösung).</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

### 19.3.2 DynDNS-Provider

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

### 19.3.2.1 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
<b>Providername</b>	Tragen Sie einen Namen für diesen Eintrag ein.
<b>Server</b>	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
<b>Aktualisierungspfad</b>	Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist.  Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
<b>Port</b>	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll.  Erfragen Sie den entsprechenden Port bei Ihrem Provider.  Der Standardwert ist <i>80</i> .
<b>Protokoll</b>	Wählen Sie eines der implementierten Protokolle aus. Welches Protokoll Ihr Anbieter verwendet, erfahren Sie in dessen Anleitung.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>DynDNS</i> (Standardwert)</li> <li>• <i>Static DynDNS</i></li> <li>• <i>ODS</i></li> <li>• <i>HN</i></li> <li>• <i>DYNS</i></li> <li>• <i>GnuDIP-HTML</i></li> <li>• <i>GnuDIP-TCP</i></li> <li>• <i>Custom DynDNS</i></li> <li>• <i>DnsExit</i></li> </ul>



Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>dyndnss</i></li> <li>• <i>dyndns2</i></li> </ul>
<b>Aktualisierungsintervall</b>	<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>
<b>IPv6-Server</b>	Geben Sie den Host-Namen oder die IPv6-Adresse des DynDNS-Servers ein, wenn Sie IPv6-Adressen aktualisieren wollen.
<b>Supports SSL</b>	<p>Aktivieren Sie diese Option, wenn Ihr DynDNS-Anbieter SSL zur Absicherung der Datenübertragung unterstützt.</p> <p>Standardmäßig ist die Option deaktiviert.</p>
<b>Homepage</b>	Hier können Sie eine Web-Adresse angeben, mit der Sie direkt auf die Seite des Anbieters gelangen.

## 19.4 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 386) finden Sie am Ende des Kapitels unter [DHCP - Konfigurationsbeispiel](#) auf Seite 387.

## 19.4.1 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.

### 19.4.1.1 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
<b>IP-Poolname</b>	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
<b>IP-Adressbereich</b>	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
<b>DNS-Server</b>	<p><b>Primär:</b> 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><b>Sekundär:</b> Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

## 19.4.2 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.

#### 19.4.2.1 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
<b>Schnittstelle</b>	<p>Wählen Sie die Schnittstelle aus, über welche die in <b>IP-Adressbereich</b> definierten Adressen an anfragende DHCP-Clients vergeben werden.</p> <p>Wenn eine DHCP-Anfrage über diese <b>Schnittstelle</b> eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.</p>
<b>IP-Poolname</b>	<p>Wählen Sie einen im Menü <b>Lokale Dienste-&gt;DHCP-Server-&gt;IP-Pool-Konfiguration</b> konfigurierten IP-Poolnamen aus.</p>
<b>Pool-Verwendung</b>	<p>Wählen Sie aus, ob der DHCP-Pool für Anfragen von DHCP-Clients in einem direkt an die <b>Schnittstelle</b> 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"> <li>• <i>Lokal</i> (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen aus einem direkt an die <b>Schnittstelle</b> angeschlossenen Ethernet verwendet.</li> <li>• <i>Relais</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-</li> </ul>

Feld	Beschreibung
	<p>Anfragen aus einem über Gateways erreichbaren Ethernet verwendet.</p> <ul style="list-style-type: none"> <li>• <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.</li> </ul>
<b>Beschreibung</b>	Geben Sie eine beliebige Beschreibung ein, um den DHCP-Pool eindeutig zu benennen.

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

#### Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
<b>Gateway</b>	<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"> <li>• <i>Router als Gateway verwenden</i> (Standardwert): Hier wird die für die <b>Schnittstelle</b> definierte IP-Adresse übertragen.</li> <li>• <i>Kein Gateway</i>: Hier wird keine IP-Adresse übermittelt.</li> <li>• <i>Angeben</i>: Geben Sie die entsprechende IP-Adresse ein.</li> </ul>
<b>Lease Time</b>	<p>Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll.</p> <p>Nachdem <b>Lease Time</b> abgelaufen ist, kann die Adresse durch den Server neu vergeben werden.</p> <p>Der Standardwert ist <i>120</i>.</p>
<b>DHCP-Optionen</b>	<p>Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen.</p> <p>Mögliche Werte für <b>Option</b>:</p> <ul style="list-style-type: none"> <li>• <i>Zeitserver</i> (Standardwert): Geben Sie die IP-Adresse des Zeitserver ein, die dem Client übermittelt werden soll.</li> <li>• <i>DNS-Server</i>: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll.</li> <li>• <i>DNS-Domänenname</i>: Geben Sie die DNS Domain ein, die</li> </ul>

Feld	Beschreibung
	<p>dem Client übermittelt werden soll.</p> <ul style="list-style-type: none"> <li>• <i>WINS/NBNS-Server</i>: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll.</li> <li>• <i>WINS/NBT Node Type</i>: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll.</li> <li>• <i>TFTP-Server</i>: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll.</li> <li>• <i>CAPWAP Controller</i>: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll.</li> <li>• <i>URL (Provisionierungsserver)</i>: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln.</li> </ul> <p>Verwenden Sie diese Option, um anfragenden <b>IP1x0</b>-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form <code>http://&lt;IP-Adresse des Provisionierungsservers&gt;/eg_prov</code> haben.</p> <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche <b>Hinzufügen</b> ein.</p>


### Herstellerspezifische Informationen (DHCP-Option 43)

Mit den Optionen für einen **Hersteller-String** bzw. eine herstellerspezifische Gruppe von DHCP-Optionen (**Herstellergruppe**) können Sie einen DHCP Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen oder Konfigurationseinstellungen übermitteln oder auch ganze Gruppen von DHCP-Optionen festlegen, die dem Client übermittelt werden.



#### Hinweis

Für einige Produkte sind in diesem Bereich Einstellungen hinterlegt, die für eine reibungslose Einbindung von Telefonen oder LTE-Zugangsroutern notwendig sind. Diese Einstellungen sollten weder geändert noch entfernt werden.

Wählen Sie das Symbol , um einen vorhandenen Eintrag zu bearbeiten oder eine der Schaltflächen zum Hinzufügen entsprechender Einträge. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server zum Beispiel für bestimmte Telefone.

#### Felder im Menü Basisparameter für Hersteller-Strings

Feld	Beschreibung
<b>Hersteller auswählen</b>	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Sonstige</i> (Standardwert)</li> <li>• <i>-bintec-</i></li> </ul>
<b>APN</b>	Nur für <b>Hersteller auswählen</b> = <i>-bintec-</i>  Geben Sie den Access Point Namen (APN) der SIM-Karte ein.
<b>PIN</b>	Nur für <b>Hersteller auswählen</b> = <i>-bintec-</i>  Geben Sie die PIN der SIM-Karte ein.
<b>Herstellerbeschreibung</b>	Nur für <b>Hersteller auswählen</b> = <i>Sonstige</i>  Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
<b>Hersteller-ID</b>	Nur für <b>Hersteller auswählen</b> = <i>Sonstige</i> Um das Gerät zu identifizieren, geben Sie hier die Hersteller-ID ein.
<b>Herstellerspezifische Informationen</b>	Nur für <b>Hersteller auswählen</b> = <i>Sonstige</i> Geben Sie die Hersteller spezifischen Konfigurationsparameter ein.

#### Felder im Menü Basisparameter für Herstellergruppen

Feld	Beschreibung
<b>Hersteller auswählen</b>	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Siemens</i> (Standardwert)</li> <li>• <i>Sonstige</i></li> </ul>
<b>Provisioning-Server (code 3)</b>	Nur für <b>Hersteller auswählen</b> = <i>Siemens</i>  Geben Sie ein, welcher herstellerepezifische Wert übermittelt werden soll.

Feld	Beschreibung
	Für die Einstellung <b>Hersteller auswählen</b> = <i>Siemens</i> wird der Standardwert <i>sdlp</i> angezeigt.  Sie können die IP-Adresse des gewünschten Servers ergänzen.
<b>Herstellerbeschreibung</b>	Nur für <b>Hersteller auswählen</b> = <i>Sonstige</i>  Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
<b>Hersteller-ID</b>	Nur für <b>Hersteller auswählen</b> = <i>Sonstige</i> Um das Gerät zu identifizieren, geben Sie hier die Hersteller-ID ein.
<b>Benutzerdefinierte DHCP-Optionen</b>	Nur für <b>Hersteller auswählen</b> = <i>Sonstige</i>  Fügen Sie mit <b>Hinzufügen</b> weitere Einträge hinzu.  Sie können DHCP-Optionen hinzufügen.

### 19.4.3 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** dem DHCP-Server ein gültiger IP-Pool zugewiesen ist.

#### 19.4.3.1 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
<b>Beschreibung</b>	Geben Sie den Namen des Hosts ein, an dessen <b>MAC-Adresse</b> die <b>IP-Adresse</b> gebunden wird.  Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.
<b>IP-Adresse</b>	Geben Sie die IP-Adresse ein, die der in <b>MAC-Adresse</b> angegebenen MAC-Adresse zugewiesen werden soll.
<b>MAC-Adresse</b>	Geben Sie die MAC-Adresse ein, der die in <b>IP-Adresse</b> angegebene IP-Adresse zugewiesen werden soll.

### 19.4.4 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
<b>Primärer DHCP-Server</b>	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen.  Der Standardwert ist <i>0.0.0.0</i> .
<b>Sekundärer DHCP-Server</b>	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein.  Der Standardwert ist <i>0.0.0.0</i> .

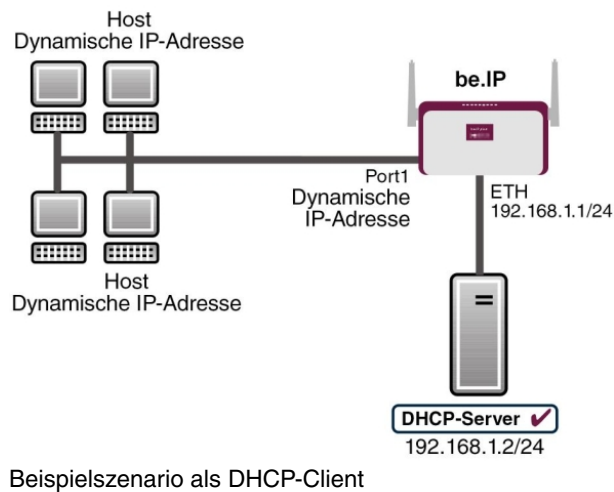
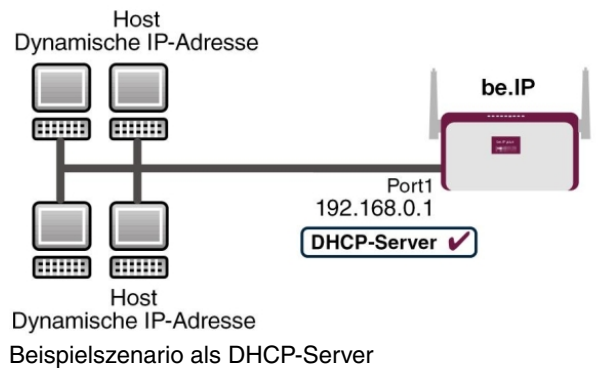


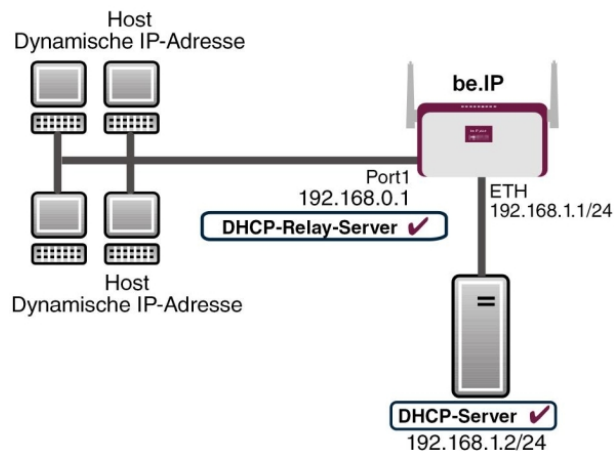
## 19.4.5 DHCP - Konfigurationsbeispiel

### Voraussetzungen

- Optional ein DHCP-Server

### Beispiel-Szenarien





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-Pool-Konfiguration ->Neu	z. B. <i>192.168.0.2</i> und <i>192.168.0.10</i>
Schnittstelle	Lokale Dienste->DHCP-Server->DHCP-Konfiguration ->Neu	z. B. <i>en1-0</i>
IP-Poolname	Lokale Dienste->DHCP-Server->DHCP-Konfiguration ->Neu	<i>IP-Pool-1</i>
Pool-Verwendung	Lokale Dienste->DHCP-Server->DHCP-Konfiguration ->Neu	<i>Lokal</i>
Gateway	Lokale Dienste->DHCP-Server->DHCP-Konfiguration ->Neu->Erweiterte Einstellungen	<i>Router als Gateway verwenden</i>

Feld	Menü	Wert
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-Relay-Einstellungen	falls vorhanden

## 19.5 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 **Bevorzugte 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**

## 19.5.1 DHCPv6-Server

Hier können Sie - bezogen auf eine Schnittstelle - in einem Option Set Adresspools anlegen und DHCP-Options definieren.


### 19.5.1.1 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
<b>Name</b>	Geben Sie einen Namen für das Option Set ein.
<b>Schnittstelle</b>	<p>Wählen Sie die IPv6-Schnittstelle, an die das Option Set gebunden sein soll.</p> <p>Zur Auswahl stehen Schnittstellen mit folgender Konfiguration:</p> <ul style="list-style-type: none"> <li>• IPv6 ist aktiviert.</li> <li>• Die Option <b>DHCP-Server</b> ist aktiviert.</li> </ul> <p>Im Auslieferungszustand ist IPv6 für alle Schnittstellen deaktiviert. Erscheint die gewünschte Schnittstelle nicht in der Auswahl, konfigurieren Sie sie im Menü <b>LAN-&gt;IP-Konfiguration-&gt;Schnittstellen</b> gemäß den in der Einleitung genannten Vorgaben.</p>
<b>Address assignment</b>	<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 <b>Hinzufügen</b> können Sie dem IPv6 Option Set einen oder mehrere IPv6-Link-Präfixe zuordnen.</p>


Feld	Beschreibung
	<div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;">  <p><b>Hinweis</b></p> <p>Bitte beachten Sie, dass hier ausschließlich die IPv6-Link-Präfixe zur Auswahl stehen, die der gewählten Schnittstelle zugewiesen sind.</p> </div>

### Felder im Menü Server-Optionen

Feld	Beschreibung
<b>DNS-Domänen-Suchliste</b>	Mit <b>Hinzufügen</b> 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.

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

### Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
<b>DNS-Server</b>	<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 <b>DNS-Propagation</b> im Menü <b>LAN-&gt;IP-Konfiguration-&gt;Schnittstellen-&gt;</b>  <b>-&gt;Erweiterte Einstellungen</b> mit <b>IPv6 = Aktiviert</b> konfiguriert.)</p> <p>Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option <b>RA oder globalen Fallback-DNS-Server verwenden</b> und erstellen Sie mit <b>Hinzufügen</b> die gewünschten DNS-Server-Einträge.</p>
<b>SNTP-Server</b>	Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit <b>Hinzufügen</b> können Sie die gewünschten Zeitserver-Einträge anlegen.

## 19.5.2 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
<b>DNS-Domänen-Suchliste</b>	Mit <b>Hinzufügen</b> 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.

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

### Felder im Menü Server-Priorität

Feld	Beschreibung
<b>Server-Priorität</b>	<p>In den vom DHCPv6 Server an die Clients gesendeten DHCPv6 Advertisements kann die DHCPv6-Option 7 Preference enthalten sein.</p> <p>Mögliche Werte sind <math>0 \dots 255</math>. 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 <math>0</math> bedeutet "nicht spezifiziert" (niedrigste Priorität), <math>255</math> bedeutet höchste Priorität.</p>

### Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
<b>DNS-Server</b>	<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 <b>DNS-Propagation</b> im Menü <b>LAN-&gt;IP-Konfiguration-&gt;Schnittstellen-&gt;</b>  <b>-&gt;Erweiterte Einstellungen</b> mit <b>IPv6 = Aktiviert</b> konfiguriert.)</p> <p>Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option <b>RA oder globalen Fallback-DNS-Server verwenden</b> und erstellen Sie mit <b>Hinzufügen</b> die gewünschten DNS-Server-Einträge.</p>
<b>SNTP-Server</b>	<p>Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit <b>Hinzufügen</b> können Sie die gewünschten Zeitserver-Einträge anlegen.</p>


### 19.5.3 Zustandsbehaftete Clients

Hier sehen Sie Informationen zu zustandsbehafteten Clients, sobald diese eine IPv6-Adresse bezogen haben.

### 19.5.4 Konfiguration von zustandsbehafteten Clients

Bei einer zustandsbezogenen Konfiguration von IPv6 Clients, wird dem Client neben den DHCP-Optionen auch der IPv6-Präfix übermittelt.

#### 19.5.4.1 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
<b>DUID</b>	<p>Ein Client verwendet das Feld <b>DUID</b> (DHCP Unique Identifier), um sich zu identifizieren und eine IP-Adresse vom DHCPv6-Server zu beziehen.</p> <p>Wenn Sie mit der Schaltfläche <b>Neu</b> einen Eintrag anlegen, können Sie die <b>DUID</b> 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.</p>
<b>Client FQDN akzeptieren</b>	Wenn <b>Client FQDN akzeptieren</b> aktiviert ist, wird der Client mit dem Parameter FQDN (Fully Qualified Domain Name) im Cache des Domain Name Servers eingetragen.
<b>Administrative FQDNs</b>	Mit <b>Hinzufügen</b> können Sie - auch bei automatisch angelegten Einträgen - den Parameter FQDN (Fully Qualified Domain Name) eingeben.
<b>Kennung der statischen Schnittstelle</b>	Das Feld <b>Kennung der statischen Schnittstelle</b> ist der Host-Anteil der IPv6-Adresse, d.h. die letzten 64 Bit der IPv6-Adresse. Dieser Präfix muss mit <code>::</code> anfangen.

## 19.6 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.

## 19.6.1 Benutzer

Im Menü **Lokale Dienste->CAPI-Server->Benutzer** wird eine Liste aller konfigurierten CAPI Benutzer angezeigt.

### 19.6.1.1 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
<b>Benutzername</b>	Geben Sie den Benutzernamen ein, für den der Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll.
<b>Passwort</b>	Geben Sie das Passwort ein, mit dem sich der Benutzer <b>Benutzername</b> identifizieren muss, um Zugang zum CAPI Dienst zu erhalten.
<b>Zugriff</b>	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.

## 19.6.2 Optionen

Das Menü **Lokale Dienste->CAPI-Server->Optionen** besteht aus folgenden Feldern:

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Server aktivieren</b>	Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll.

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Faxkopfzeile</b>	<p>Wählen Sie aus, ob am oberen Seitenrand von ausgehenden Faxen die Faxkopfzeile gedruckt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>TCP-Port des CAPI-Servers</b>	<p>Das Feld ist nur editierbar, wenn <b>Server aktivieren</b> aktiviert ist.</p> <p>Geben Sie die TCP-Port-Nummer für Remote-CAPI-Verbindungen ein.</p> <p>Der Standardwert ist <i>2662</i>.</p>

## 19.7 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 417.



### 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.

## 19.7.1 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.

### 19.7.1.1 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
<b>Ereignisliste</b>	<p>Mit <i>Neu</i> (Standardwert) können Sie eine neue Ereignisliste anlegen. Mit <b>Beschreibung</b> 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>

Feld	Beschreibung
<b>Beschreibung</b>	<p>Nur für <b>Ereignisliste</b> = <i>Neu</i></p> <p>Geben Sie eine beliebige Bezeichnung für die Ereignisliste ein.</p>
<b>Ereignistyp</b>	<p>Wählen Sie den Typ des Ereignisses aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Zeit</i> (Standardwert): Die in <b>Aktionen</b> konfigurierten und zugewiesenen Aktionen werden zu bestimmten Zeitpunkten ausgelöst.</li> <li>• <i>MIB/SNMP</i>: Die in <b>Aktionen</b> konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen.</li> <li>• <i>Schnittstellenstatus</i>: Die in <b>Aktionen</b> konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die definierten Schnittstellen einen bestimmten Status annehmen.</li> <li>• <i>Schnittstellenverkehr</i>: Die in <b>Aktionen</b> konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn der Datenverkehr auf den angegebenen Schnittstellen den definierten Wert unter- oder überschreitet.</li> <li>• <i>Ping-Test</i>: Die in <b>Aktionen</b> konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist.</li> <li>• <i>Lebensdauer eines Zertifikats</i>: Die in <b>Aktionen</b> konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist.</li> <li>• <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 <b>Schedule-Intervall</b> 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.</li> <li>• <i>Status der GEO-Zone</i>: Die in <b>Aktionen</b> konfigurierten</li> </ul>

Feld	Beschreibung
	<p>und zugewiesene Aktionen werden ausgelöst, wenn die definierten <b>GEO-Zonen</b> einen bestimmten Status annehmen.</p>
<b>Überwachte GEO-Zone</b>	<p>Nur für <b>Ereignistyp</b> <i>Status der GEO-Zone</i></p> <p>Wählen Sie eine konfigurierte GEO-Zone aus.</p>
<b>GEO Zone Status</b>	<p>Nur für <b>Ereignistyp</b> <i>Status der GEO-Zone</i></p> <p>Wählen Sie den <b>GEO Zone Status</b> aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Wahr</i>: Die aktuelle Position liegt innerhalb der definierten Zone.</li> <li>• <i>Falsch</i>: Die aktuelle Position liegt außerhalb der definierten Zone.</li> </ul>
<b>Überwachte Variable</b>	<p>Nur für <b>Ereignistyp</b> <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren definierter Wert als Auslöser konfiguriert werden soll. Wählen Sie zunächst das <b>System</b> aus, in dem die MIB-Variable gespeichert ist, dann die <b>MIB-Tabelle</b> und dann die <b>MIB-Variable</b> selber. Es werden nur die MIB-Tabellen und MIB-Variablen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
<b>Vergleichsbedingung</b>	<p>Nur für <b>Ereignistyp</b> <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>
<b>Vergleichswert</b>	<p>Nur für <b>Ereignistyp</b> <i>MIB/SNMP</i></p> <p>Geben Sie den Wert der MIB-Variable ein.</p>
<b>Indexvariablen</b>	<p>Nur für <b>Ereignistyp</b> <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in der <b>MIB-Tabelle</b> eindeutig zu kennzeichnen, z.B. <i>ConnIfIndex</i>. Aus der Kombination von <b>Indexvariable</b> (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und</p>

Feld	Beschreibung
	<p><b>Indexwert</b> ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere <b>Indexvariablen</b> mit <b>Hinzufügen</b> an.</p>
<b>Überwachte Schnittstelle</b>	<p>Nur für <b>Ereignistyp</b> <i>Schnittstellenstatus</i> und <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.</p>
<b>Schnittstellenstatus</b>	<p>Nur für <b>Ereignistyp</b> <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Aktiv</i> (Standardwert): Die Schnittstelle ist aktiv.</li> <li>• <i>Inaktiv</i>. Die Schnittstelle ist inaktiv.</li> </ul>
<b>Richtung des Datenverkehrs</b>	<p>Nur für <b>Ereignistyp</b> <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"> <li>• <i>RX</i> (Standardwert): Der eingehende Datenverkehr wird überwacht.</li> <li>• <i>TX</i>: Der ausgehende Datenverkehr wird überwacht.</li> </ul>
<b>Bedingung des Schnittstellenverkehrs</b>	<p>Nur für <b>Ereignistyp</b> <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>
<b>Übertragener Datenverkehr</b>	<p>Nur für <b>Ereignistyp</b> <i>Schnittstellenverkehr</i></p> <p>Geben Sie den gewünschten Wert für den Datenverkehr, mit dem verglichen werden soll, in <b>kBytes</b> ein.</p> <p>Der Standardwert ist <i>0</i>.</p>

Feld	Beschreibung
<b>Ziel-IP-Adresse</b>	<p>Nur für <b>Ereignistyp</b> <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
<b>Quell-IP-Adresse</b>	<p>Nur für <b>Ereignistyp</b> <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"> <li>• <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen.</li> <li>• <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.</li> </ul>
<b>Status</b>	<p>Nur für <b>Ereignistyp</b> <i>Ping-Test</i></p> <p>Wählen Sie aus, ob <b>Ziel-IP-Adresse</b> <i>Erreichbar</i> (Standardwert) oder <i>Nicht erreichbar</i> sein muss, um die Aktion auszulösen.</p>
<b>Intervall</b>	<p>Nur für <b>Ereignistyp</b> <i>Ping-Test</i></p> <p>Geben Sie die Zeit in <b>Sekunden</b> ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Der Standardwert ist <i>60</i> Sekunden.</p>
<b>Erfolgreiche Versuche</b>	<p>Nur für <b>Ereignistyp</b> <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>
<b>Fehlgeschlagene Ver-</b>	<p>Nur für <b>Ereignistyp</b> <i>Ping-Test</i></p>



Feld	Beschreibung
<b>suche</b>	<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>
<b>Überwachtes Zertifikat</b>	<p>Nur für <b>Ereignistyp</b> <i>Lebensdauer eines Zertifikats</i></p> <p>Wählen Sie das Zertifikat aus, dessen Gültigkeit überprüft werden soll.</p>
<b>Verbleibende Gültigkeitsdauer</b>	<p>Nur für <b>Ereignistyp</b> <i>Lebensdauer eines Zertifikats</i></p> <p>Geben Sie den gewünschten Wert für die noch verbleibende Gültigkeit des Zertifikats in Prozent ein.</p>
<b>Status der Funktionstaste</b>	<p>Nur für <b>Ereignistyp</b> <i>Funktionstaste</i></p> <p>Beim Anlegen des Auslösers können Sie über die Auswahl des <b>Status der Funktionstaste</b> 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.</p>

#### Felder im Menü Zeitintervall auswählen

Feld	Beschreibung
<b>Zeitbedingung</b>	<p>Nur für <b>Ereignistyp</b> <i>Zeit</i></p> <p>Wählen Sie zunächst die Art der Zeitangabe in <b>Bedingungstyp</b> aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Wochentag</i>: Wählen Sie in <b>Bedingungeinstellungen</b> einen</li> </ul>

Feld	Beschreibung
	<p>Wochentag aus.</p> <ul style="list-style-type: none"> <li>• <i>Perioden</i> (Standardwert): Wählen Sie in <b>Bedingungseinstellungen</b> einen bestimmten Turnus aus.</li> <li>• <i>Tag des Monats</i>: Wählen Sie in <b>Bedingungseinstellungen</b> einen bestimmten Tag im Monat aus.</li> </ul> <p>Mögliche Werte für <b>Bedingungseinstellungen</b> bei <b>Bedingungstyp</b> = <i>Wochentag</i>:</p> <p><i>Montag</i> (Standardwert) ... <i>Sonntag</i>.</p> <p>Mögliche Werte für <b>Bedingungseinstellungen</b> bei <b>Bedingungstyp</b> = <i>Perioden</i>:</p> <ul style="list-style-type: none"> <li>• <i>Täglich</i>: Der Auslöser wird täglich aktiv (Standardwert).</li> <li>• <i>Montag-Freitag</i>: Der Auslöser wird täglich von Montag bis Freitag aktiv.</li> <li>• <i>Montag-Samstag</i>: Der Auslöser wird täglich von Montag bis Samstag aktiv.</li> <li>• <i>Samstag-Sonntag</i>: Der Auslöser wird Samstag und Sonntag aktiv.</li> </ul> <p>Mögliche Werte für <b>Bedingungseinstellungen</b> bei <b>Bedingungstyp</b> = <i>Tag des Monats</i>:</p> <p>1... 31.</p>
<b>Startzeit</b>	<p>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.</p>
<b>Stoppzeit</b>	<p>Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine <b>Stoppzeit</b> eingeben oder <b>Stoppzeit</b> = <b>Startzeit</b> setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.</p>

## 19.7.2 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.

### 19.7.2.1 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
<b>Beschreibung</b>	Geben Sie eine beliebige Bezeichnung für die Aktion ein.
<b>Befehlstyp</b>	<p>Wählen Sie die gewünschte Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Neustart</i> (Standardwert): Ihr Gerät wird neu gestartet.</li> <li>• <i>MIB/SNMP</i>: Für eine MIB-Variable wird der gewünschte Wert eingetragen.</li> <li>• <i>Schnittstellenstatus</i>: Der Status einer Schnittstelle wird verändert.</li> <li>• <i>WLAN-Status</i>: Nur für Geräte mit Wireless LAN. Der Status einer WLAN-SSID wird verändert.</li> <li>• <i>Softwareaktualisierung</i>: Es wird ein Software-Update initiiert.</li> <li>• <i>Konfigurationsmanagement</i>: Eine Konfigurationsdatei wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert.</li> <li>• <i>Ping-Test</i>: Die Erreichbarkeit einer IP-Adresse wird überprüft.</li> <li>• <i>Zertifikatverwaltung</i>: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden.</li> <li>• <i>5 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt.</li> <li>• <i>5,8 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>WLC: VSS-Status</i>: Nur für Geräte mit WLAN Controller. Der Status eines Drahtlosnetzwerkes wird verändert.</li> <li>• <i>Betriebsmodus</i>: Der Betriebsmodus eines WLAN-Radiomoduls wird verändert.</li> </ul>
<b>Ereignisliste</b>	Wählen Sie die gewünschte Ereignisliste aus, die in <b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser</b> angelegt ist.
<b>Bedingung für Ereignisliste</b>	<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"> <li>• <i>Alle</i> (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten.</li> <li>• <i>Eins</i>: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt.</li> <li>• <i>Keiner</i>: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt.</li> <li>• <i>Eins nicht</i>: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.</li> </ul>
<b>Neustart des Geräts nach</b>	<p>Nur bei <b>Befehlstyp</b> = <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>
<b>Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable</b>	<p>Nur bei <b>Befehlstyp</b> = <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 <b>System</b> aus und dann die <b>MIB-Tabelle</b>. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
<b>Befehlsmodus</b>	Nur bei <b>Befehlstyp</b> = <i>MIB/SNMP</i>

Feld	Beschreibung
	<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"> <li>• <i>Vorhandenen Eintrag ändern</i> (Standardwert): Ein bestehender Eintrag soll verändert werden.</li> <li>• <i>Neuen MIB-Eintrag erstellen</i>: Ein neuer Eintrag soll angelegt werden.</li> </ul>
<b>Indexvariablen</b>	<p>Nur bei <b>Befehlstyp</b> = <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in <b>MIB-Tabelle</b> eindeutig zu kennzeichnen, z. B. <i>ConnIfIndex</i>. Aus der Kombination von <b>Indexvariable</b> (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und <b>Indexwert</b> ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere <b>Indexvariablen</b> mit <b>Hinzufügen</b> an.</p>
<b>Status des Auslösers</b>	<p>Nur bei <b>Befehlstyp</b> = <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"> <li>• <i>Aktiv</i> (Standardwert): Der Wert der MIB-Variable wird verändert, wenn der Auslöser aktiv ist.</li> <li>• <i>Inaktiv</i>: Der Wert der MIB-Variable wird verändert, wenn der Auslöser inaktiv ist.</li> <li>• <i>Beide</i>: Der Wert der MIB-Variable wird unterschiedlich verändert, wenn der Status des Auslösers sich ändert.</li> </ul>
<b>MIB-Variablen</b>	<p>Nur bei <b>Befehlstyp</b> = <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 (<b>Status des Auslösers</b> <i>Aktiv</i>), wird die MIB-Variable mit dem in <b>Aktiver Wert</b> eingetragenen Wert beschrieben.</p>

Feld	Beschreibung
	<p>Ist der Auslöser inaktiv, <b>Status des Auslösers</b> <i>Inaktiv</i>), wird die MIB-Variable mit dem in <b>Inaktiver Wert</b> eingetragenen Wert beschrieben.</p> <p>Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (<b>Status des Auslösers</b> <i>Beide</i>), wird sie mit einem aktiven Auslöser mit dem in <b>Aktiver Wert</b> eingetragenen Wert und mit einem inaktiven Auslöser mit dem in <b>Inaktiver Wert</b> eingetragenen Wert beschrieben.</p> <p>Legen Sie weitere Einträge mit <b>Hinzufügen</b> an.</p>
<b>Schnittstelle</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Schnittstellenstatus</i></p> <p>Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.</p>
<b>Schnittstellenstatus festlegen</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Aktiv</i> (Standardwert)</li> <li>• <i>Inaktiv</i></li> <li>• <i>Zurücksetzen</i></li> </ul>
<b>Lokale WLAN-SSID</b>	<p>Nur bei <b>Befehlstyp</b> = <i>WLAN-Status</i></p> <p>Wählen Sie das gewünschte Drahtlosnetzwerk aus, dessen Status verändert werden soll.</p>
<b>Status festlegen</b>	<p>Nur bei <b>Befehlstyp</b> = <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"> <li>• <i>Aktivieren</i> (Standardwert)</li> <li>• <i>Deaktivieren</i></li> </ul>
<b>Quelle</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Softwareaktualisierung</i></p>

Feld	Beschreibung
	<p>Wählen Sie die gewünschte Quelle für die Software-Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Aktuelle Software vom Update-Server</i> (Standardwert): Die aktuelle Software wird vom Update-Server geladen.</li> <li>• <i>HTTP-Server</i>: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen.</li> <li>• <i>HTTPS-Server</i>: Die aktuelle Software wird von einem HTTPS-Server geladen, den Sie über die <i>Server-URL</i> festlegen.</li> <li>• <i>TFTP-Server</i>: Die aktuelle Software wird von einem TFTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen.</li> </ul>
<b>Server-URL</b>	<p>Bei <b>Befehlstyp</b> = <i>Softwareaktualisierung</i> wenn <b>Quelle</b> nicht <i>Aktuelle Software vom Update-Server</i></p> <p>Geben Sie die URL des Servers ein, von dem die gewünschte Softwareversion geholt werden soll.</p> <p>Bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> mit <b>Aktion</b> = <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>
<b>Dateiname</b>	<p>Bei <b>Befehlstyp</b> = <i>Softwareaktualisierung</i></p> <p>Geben Sie den Dateinamen der Softwareversion ein.</p> <p>Bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> mit <b>Aktion</b> = <i>Zertifikat importieren</i></p> <p>Geben Sie den Dateinamen der Zertifikatsdatei ein.</p>
<b>Aktion</b>	<p>Bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Konfiguration importieren</i> (Standardwert)</li> <li>• <i>Konfiguration exportieren</i></li> <li>• <i>Konfiguration umbenennen</i></li> <li>• <i>Konfiguration löschen</i></li> <li>• <i>Konfiguration kopieren</i></li> </ul> <p>Bei <b>Befehlstyp</b> = <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"> <li>• <i>Zertifikat importieren</i> (Standardwert)</li> <li>• <i>Zertifikat löschen</i></li> <li>• <i>SCEP</i></li> </ul>
<b>Protokoll</b>	<p>Nur für <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <i>Konfigurationsmanagement</i> wenn <b>Aktion</b> = <i>Konfiguration importieren</i></p> <p>Wählen Sie das Protokoll für die Dateiübertragung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>HTTP</i> (Standardwert)</li> <li>• <i>HTTPS</i></li> <li>• <i>FTTP</i></li> </ul>
<b>CSV-Dateiformat</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <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>
<b>Dateiname auf Server</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i></p>



Feld	Beschreibung
	<p>Für <b>Aktion</b> = <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 <b>Aktion</b> = <i>Konfiguration exportieren</i></p> <p>Geben Sie den Namen der Datei ein, unter dem sie auf dem Server gespeichert werden soll.</p>
<b>Lokaler Dateiname</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration importieren, Konfiguration umbenennen oder Konfiguration kopieren</i></p> <p>Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.</p>
<b>Dateiname in Flash</b>	<p>Bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Datei aus, die exportiert werden soll.</p> <p>Bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration umbenennen</i></p> <p>Wählen Sie die Datei aus, die umbenannt werden soll.</p> <p>Bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration löschen</i></p> <p>Wählen Sie die Datei aus, die gelöscht werden soll.</p> <p>Bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration kopieren</i></p> <p>Wählen Sie die Datei aus, die kopiert werden soll.</p>
<b>Konfiguration enthält Zertifikate/Schlüssel</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration importieren oder Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
<b>Konfiguration verschlüsseln</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten <b>Aktion</b> verschlüsselt werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Nach Ausführung neu starten</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, ob Ihr Gerät nach der gewünschten <b>Aktion</b> neu gestartet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Versionsprüfung</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Konfigurationsmanagement</i> und <b>Aktion</b> = <i>Konfiguration importieren</i></p> <p>Wählen Sie aus, ob beim Import einer Konfigurationsdatei überprüft werden soll, ob auf dem Server eine aktuellere Version der schon geladenen Konfiguration vorhanden ist. Wenn nicht, wird der Datei-Import abgebrochen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Ziel-IP-Adresse</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
<b>Quell-IP-Adresse</b>	<p>Nur bei <b>Befehlstyp</b> = <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"> <li>• <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen.</li> <li>• <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.</li> </ul>
<b>Intervall</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Ping-Test</i></p>

Feld	Beschreibung
	<p>Geben Sie die Zeit in <b>Sekunden</b> ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Der Standardwert ist <i>1</i> Sekunde.</p>
<b>Versuche</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll.</p> <p>Der Standardwert ist <i>3</i>.</p>
<b>Serveradresse</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>Zertifikat importieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.</p>
<b>Lokale Zertifikatsbeschreibung</b>	<p>Bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <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 <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>Zertifikat löschen</i></p> <p>Wählen Sie das Zertifikat aus, das gelöscht werden soll.</p>
<b>Kennwort für geschütztes Zertifikat</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <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>
<b>Ähnliches Zertifikat überschreiben</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <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>

Feld	Beschreibung
<b>Zertifikat in Konfiguration schreiben</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <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>
<b>Zertifikatsanforderungsbeschreibung</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.</p>
<b>SCEP-Server-URL</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B. <i>http://scep.bintec-elmeg.com:8080/scep/scep.dll</i></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
<b>Subjektname</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Geben Sie einen Subjektnamen mit Attributen ein.</p> <p>Beispiel: <i>"CN=VPNServer, DC=mydomain, DC=com, c=DE"</i></p>
<b>CA-Name</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
<b>Passwort</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein</p>

Feld	Beschreibung
	<p>Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.</p>
<b>Schlüsselgröße</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind <i>1024</i> (Standardwert), <i>2048</i> und <i>4096</i>.</p>
<b>Autospeichermodus</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <i>SCEP</i></p> <p>Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>CRL verwenden</b>	<p>Nur bei <b>Befehlstyp</b> = <i>Zertifikatverwaltung</i> und <b>Aktion</b> = <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"> <li>• <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.</li> <li>• <i>Ja</i>: CRLs werden grundsätzlich überprüft.</li> <li>• <i>Nein</i>: Keine Überprüfung von CRLs.</li> </ul>
<b>WLAN-Modul auswählen</b>	<p>Nur bei <b>Befehlstyp</b> = <i>5 GHz-WLAN-Bandscan</i>, <i>5,8 GHz-WLAN-Bandscan</i> und <i>Betriebsmodus</i></p>

Feld	Beschreibung
	Wählen Sie das WLAN-Modul aus, auf dem ein Scan des Frequenzbands durchgeführt werden soll.
<b>WLC-SSID</b>	Nur bei <b>Befehlstyp</b> = <i>WLC: VSS-Status</i>  Wählen Sie das über den WLAN Controller verwaltete Drahtlosnetzwerk aus, dessen Status verändert werden soll.
<b>Betriebsmodus (Aktiv)</b>	Nur bei <b>Befehlstyp</b> = <i>Betriebsmodus</i>  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.
<b>Betriebsmodus (Inaktiv)</b>	Nur bei <b>Befehlstyp</b> = <i>Betriebsmodus</i>  Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand <i>Inaktiv</i> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.

### 19.7.3 Optionen

Im Menü **Lokale Dienste->Scheduling->Optionen** konfigurieren Sie das Schedule-Intervall.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Scheduling-Optionen

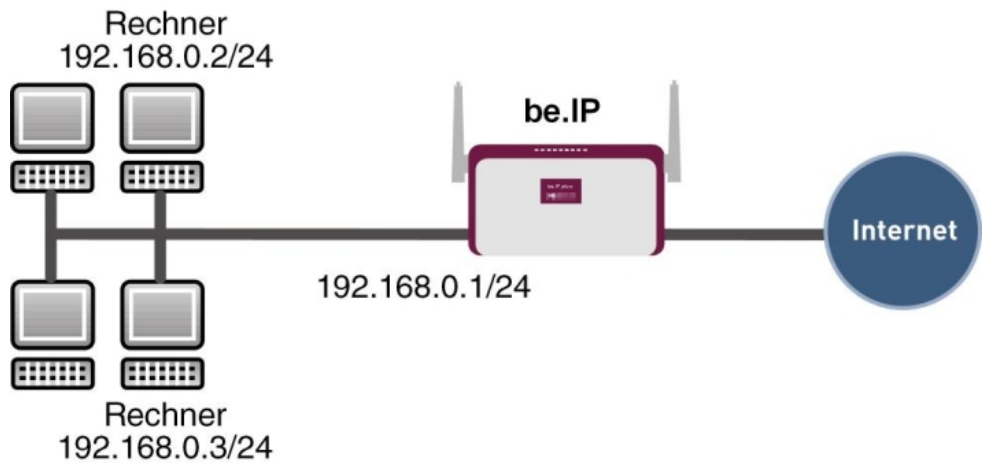
Feld	Beschreibung
<b>Schedule-Intervall</b>	Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll.  Standardmäßig ist das Schedule-Intervall nicht aktiv.  Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind.  Möglich sind Werte zwischen 0 und 65535.  Empfohlen wird der Wert 300 (5 Minuten Genauigkeit).

## 19.7.4 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->Aus-	z. B. <i>Neustart aus-</i>

Feld	Menü	Wert
	<b>löser-&gt;Neu</b>	<i>lösen</i>
<b>Ereignistyp</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	<i>Zeit</i>
<b>Zeitbedingung</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	Bedingungstyp = <i>Perioden</i> , Bedingungseinstellungen = <i>Täglich</i>
<b>Startzeit</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	Stunde <i>02</i> Minute <i>00</i>
<b>Beschreibung</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>z. B. Neustart des Geräts</i>
<b>Befehlstyp</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>Neustart</i>
<b>Ereignisliste</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>Neustart auslösen</i>
<b>Bedingung für Ereignisliste</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>Alle</i>
<b>Neustart des Geräts nach</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>z. B. 60 Sekunden</i>
<b>Schedule-Intervall</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Optionen</b>	<i>Aktiviert, 55 sec</i>

#### WLAN-Schnittstelle abschalten

Feld	Menü	Wert
<b>Ereignisliste</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	<i>Neu</i>
<b>Beschreibung</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	<i>z. B. WLAN-Schnittstelle abschalten auslösen</i>
<b>Ereignistyp</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	<i>Zeit</i>
<b>Zeitbedingung</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	Bedingungstyp = <i>Perioden</i> , Bedingungseinstellungen = <i>Samstag Sonntag</i>
<b>Startzeit</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	Stunde <i>00</i> Minute <i>00</i>
<b>Stopzeit</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Auslöser-&gt;Neu</b>	Stunde <i>23</i> Minute <i>59</i>



Feld	Menü	Wert
<b>Beschreibung</b>	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>WLAN-Schnittstelle abschalten</i>
<b>Befehlstyp</b>	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Schnittstellenstatus</i>
<b>Ereignisliste</b>	Lokale Dienste->Scheduling->Aktionen->Neu	<i>WLAN-Schnittstelle abschalten auslösen</i>
<b>Bedingung für Ereignisliste</b>	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Alle</i>
<b>Schnittstelle</b>	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>vss1-0</i>
<b>Schnittstellenstatus festlegen</b>	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Inaktiv</i>
<b>Schedule-Intervall</b>	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

#### Konfiguration monatlich sichern

Feld	Menü	Wert
<b>Ereignisliste</b>	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Neu</i>
<b>Beschreibung</b>	Lokale Dienste->Scheduling->Auslöser->Neu	z. B. <i>Konfigurationssicherung auslösen</i>
<b>Ereignistyp</b>	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Zeit</i>
<b>Zeitbedingung</b>	Lokale Dienste->Scheduling->Auslöser->Neu	Bedingungstyp = <i>Tag des Monats</i> , Bedingungseinstellungen = <i>1</i>
<b>Startzeit</b>	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde <i>03</i> Minute <i>00</i>
<b>Beschreibung</b>	Lokale Dienste->Scheduling->Aktionen->Neu	Konfiguration sichern
<b>Befehlstyp</b>	Lokale Dienste->Scheduling->Aktionen->Neu	Konfigurationsmanagement
<b>Ereignisliste</b>	Lokale Dienste->Scheduling->Aktionen->Neu	Konfigurationssicherung auslösen
<b>Bedingung für Ereignis-</b>	Lokale Dienste->Scheduling->Ak-	Alle

Feld	Menü	Wert
<b>nisliste</b>	<b>tionen-&gt;Neu</b>	
<b>Aktion</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	Konfiguration exportieren
<b>Server-URL</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	z. B. <i>tftp://192.168.2.5</i>
<b>CSV-Dateiformat</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>Aktiviert</i>
<b>Dateiname auf Server</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	z. B. <i>monthly-backup.cf</i>
<b>Dateiname in Flash</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>boot</i>
<b>Konfiguration enthält Zertifikate/Schlüssel</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Aktionen-&gt;Neu</b>	<i>Aktiviert</i>
<b>Schedule-Intervall</b>	<b>Lokale Dienste-&gt;Scheduling-&gt;Optionen</b>	<i>Aktiviert, 55 sec</i>

## 19.8 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.

### 19.8.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

#### 19.8.1.1 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
<b>Gruppen-ID</b>	<p>Wenn die Erreichbarkeit einer Gruppe von Hosts bzw. des Standard-Gateways von Ihrem Gerät überwacht werden soll, wählen Sie eine ID für die Gruppe bzw. für das Standard-Gateway.</p> <p>Die Gruppen-IDs werden automatisch von 0 bis 255 angelegt. Ist noch kein Eintrag angelegt, wird durch die Option <i>Neue ID</i> eine neue Gruppe angelegt. Sind Einträge vorhanden, kann man aus den angelegten Gruppen auswählen.</p> <p>Jeder zu überwachende Host muss einer Gruppe zugeordnet werden.</p> <p>Der für die ausgewählte <b>Schnittstelle</b> konfigurierte Vorgang wird nur dann ausgeführt, wenn kein Gruppenmitglied erreicht werden kann. Darüber hinaus müssen die Gruppenmitglieder die gleiche Kombination von Aktion und Schnittstelle haben.</p>

#### Felder im Menü Trigger

Feld	Beschreibung
<b>Überwachte IP-Adresse</b>	<p>Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Standard-Gateway</i> (Standardwert): Das Standard-Gateway wird überwacht.</li> <li>• <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse des zu überwachenden Hosts ein.</li> </ul>
<b>Quell-IP-Adresse</b>	<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"> <li>• <i>Automatisch</i> (Standardwert): Die IP-Adresse wird automatisch ermittelt.</li> <li>• <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse ein.</li> </ul>


Feld	Beschreibung
<b>Intervall</b>	<p>Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p> <p>Der Standardwert ist <i>10</i>.</p> <p>Innerhalb einer Gruppe wird das kleinste <b>Intervall</b> der Gruppenmitglieder verwendet.</p>
<b>Erfolgreiche Versuche</b>	<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>
<b>Fehlgeschlagene Versuche</b>	<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>
<b>Auszuführende Aktion</b>	<p>Nicht für <b>Aktion</b> = <i>überwachen</i>.</p> <p>Wählen Sie aus, welche <b>Aktion</b> ausgeführt werden soll, wenn der Host als unzugänglich angesehen wird. Für die meisten Aktionen wählen Sie eine <b>Schnittstelle</b>, auf die sich die <b>Aktion</b> bezieht.</p> <p>Auswählbar sind alle IP-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>

Feld	Beschreibung
	<p>Die <b>Aktionen</b> <i>Aktivieren</i> und <i>Deaktivieren</i> werden ebenfalls abgebrochen, wenn die Hosts wieder als zugänglich angesehen werden.</p> <p>Mit <b>Aktion</b> = <i>Überwachen</i> können Sie die IP-Adresse überwachen, die unter <b>Überwachte IP-Adresse</b> angegeben ist. Diese Information kann für andere Funktionen genutzt werden, z. B. für die <b>IP-Adresse zur Nachverfolgung</b>, die beim IP-Lastverteilung verwendet wird.</p>

## 19.8.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

### 19.8.2.1 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
<b>Überwachte Schnittstelle</b>	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
<b>Trigger</b>	<p>Wählen Sie den Status bzw. Statusübergang von <b>Überwachte Schnittstelle</b> aus, der eine bestimmte <b>Schnittstellenaktion</b> auslösen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Schnittstelle wird aktiviert.</i> (Standardwert)</li> <li>• <i>Schnittstelle wird deaktiviert.</i></li> </ul>
<b>Schnittstellenaktion</b>	<p>Wählen Sie die Aktion aus, welche dem in <b>Trigger</b> definierten Status bzw. Statusübergang folgen soll.</p> <p>Die Aktion wird auf die in <b>Schnittstelle</b> ausgewählte(n) Schnitt-</p>

Feld	Beschreibung
	<p>stelle(n) angewendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Aktivieren</i> (Standardwert): Aktivierung der Schnittstelle(n)</li> <li>• <i>Deaktivieren</i>: Deaktivierung der Schnittstelle(n)</li> </ul>
<b>Schnittstelle</b>	<p>Wählen Sie aus, für welche Schnittstelle(n) die unter <b>Schnittstelle</b> festgelegte Aktion ausgeführt werden soll.</p> <p>Wählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle IPSec-Schnittstellen</i>.</p>

### 19.8.3 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

#### 19.8.3.1 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
<b>Ziel-IP-Adresse</b>	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
<b>Quell-IP-Adresse</b>	<p>Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Automatisch</i>: Die IP-Adresse wird automatisch ermittelt.</li> <li>• <i>Spezifisch</i> (Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.</li> </ul>

Feld	Beschreibung
<b>Intervall</b>	<p>Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in <b>Entfernte IP-Adresse</b> angegebene Adresse abgesetzt werden soll.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 10.</p>
<b>Versuche</b>	<p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden sollen.</p> <p>Der Standardwert ist 3.</p>

## 19.9 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](http://www.upnp.org).

### 19.9.1 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
<b>Schnittstelle</b>	Zeigt den Namen der Schnittstelle an, für welche die UPnP-Einstellungen vorgenommen werden. Der Eintrag kann nicht verändert werden.
<b>Auf Client-Anfrage antworten</b>	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.
<b>Schnittstelle ist UPnP-kontrolliert</b>	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.

### 19.9.2 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
<b>UPnP-Status</b>	<p>Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv. Das Gateway nimmt die UPnP-Freigaben gemäß der in der Anfrage des LAN UPnP Clients beinhalteten Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.</p>
<b>UPnP TCP Port</b>	<p>Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht.</p> <p>Mögliche Werte sind 1 bis 65535, der Standardwert ist 5678.</p>

## 19.10 Hotspot-Gateway



### Wichtig

Das Hotspot-Gateway darf nicht mit aktiviertem IPv6 betrieben werden, da IPv6-Datenverkehr vom Hotspot-Gateway nicht erfasst wird und daher nicht kontrolliert werden kann.

Die **Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen (mittels WLAN oder kabelgebundenem Ethernet). Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **Hotspot Solution** besteht aus einem vor Ort installierten bintec elmeg Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

### Ablauf der Anmeldeprozedur am Hotspot Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP auto-

matisch eine IP-Adresse zugewiesen.

- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

## Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein bintec elmeg Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung**->**Remote Authentifizierung** ->**RADIUS**->**Neu** mit **Gruppenbeschreibung** *Standardgruppe 0*)
- bintec elmeg Hotspot Hosting (Artikelnummer 5510000198 bzw. 5510000197)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

- Gehen Sie auf [www.bintec-elmeg.com](http://www.bintec-elmeg.com) zu **Service/Support** -> **Services** -> **Online Services**.

- Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

- Sie erhalten daraufhin die Login-Daten des Hotspot Servers.



### Hinweis

Die Freischaltung kann etwa 2-3 Werktage in Anspruch nehmen.

## Zugangsdaten zur Konfiguration des Gateways

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Wird von bintec elmeg GmbH festgelegt
Domain	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Network	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Server URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Terms & Condition URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt

## Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	<a href="https://hotspot.bintec-elmeg.com/">https://hotspot.bintec-elmeg.com/</a>
Username	Wird durch bintec elmeg individuell festgelegt
Password	Wird durch bintec elmeg individuell festgelegt



### Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf [www.bintec-elmeg.com](http://www.bintec-elmeg.com) zum Download zur Verfügung steht.


## 19.10.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte bintec elmeg Gateway für die **Hotspot Solution**.

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller konfigurierten Hotspot Netzwerke angezeigt.


Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktivieren.

### 19.10.1.1 Bearbeiten oder Neu

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->**  konfigurieren Sie die Hotspot Netzwerke. Wählen Sie die Schaltfläche **Neu**, um weitere Hotspot Netzwerke einzurichten.

Das Menü besteht aus folgenden Feldern:

### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Schnittstelle</b>	<p>Wählen Sie die Schnittstelle aus, an der das Hotspot LAN oder WLAN angeschlossen ist. Bei Betrieb über LAN tragen Sie hier die Ethernet-Schnittstelle ein (z. B. die en1-0). Bei Betrieb über WLAN muss die WLAN-Schnittstelle ausgewählt werden, an der der Access Point angeschlossen ist.</p> <div data-bbox="544 543 1322 958" style="background-color: #f0f0f0; padding: 10px;">  <p><b>Achtung</b></p> <p>Die Konfiguration Ihres Gerätes ist aus Sicherheitsgründen nicht über eine Schnittstelle möglich, die für den Hotspot konfiguriert ist. Wählen Sie hier daher sorgfältig die Schnittstelle aus, die Sie für den Hotspot nutzen wollen!</p> <p>Wenn Sie hier die Schnittstelle auswählen, über die die aktuelle Konfigurationssitzung stattfindet, geht die aktuelle Verbindung verloren. Sie müssen sich dann über eine erreichbare, nicht für den Hotspot konfigurierte Schnittstelle zur weiteren Konfiguration Ihres Geräts erneut anmelden.</p> </div>
<b>Domäne am Hotspot-Server</b>	<p>Geben Sie den Domänennamen ein, der bei der Einrichtung des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.</p>
<b>Walled Garden</b>	<p>Aktivieren Sie diese Funktion, wenn Sie einen abgegrenzten und kostenfreien Bereich von Webseiten (Intranet) definieren wollen.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>
<b>Walled Network / Netzmaske</b>	<p>Nur wenn <b>Walled Garden</b> aktiviert ist.</p> <p>Geben Sie die Netzadresse des <b>Walled Network</b> und die entsprechende <b>Netzmaske</b> des Intranet-Servers ein.</p> <p>Für den aus <b>Walled Network / Netzmaske</b> resultierenden Adressraum benötigen die Clients keine Authentifizierung.</p> <p>Beispiel: Geben Sie 192.168.0.0 / 255.255.255.0 ein, sind alle</p>

Feld	Beschreibung
	IP-Adressen von 192.168.0.0 bis 19.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IP-Adresse 192.168.0.1 frei.
<b>Walled Garden URL</b>	Nur wenn <b>Walled Garden</b> aktiviert ist.  Geben Sie die <b>Walled Garden URL</b> des Intranet-Servers ein. Frei zugängliche Webseiten müssen über diese Adresse erreichbar sein.
<b>Geschäftsbedingungen</b>	Nur wenn <b>Walled Garden</b> aktiviert ist.  Tragen Sie in das Eingabefeld <b>Geschäftsbedingungen</b> die Adresse der AGB's auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. <a href="http://www.webserver.de/agb.htm">http://www.webserver.de/agb.htm</a> . Die Seite muss im Adressraum des Walled Garden-Networks liegen.
<b>Zusätzliche, frei zugängliche Domänennamen</b>	Nur wenn <b>Walled Garden</b> aktiviert ist.  Fügen Sie mit <b>Hinzufügen</b> weitere URLs oder IP-Adressen hinzu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.
<b>Aufzurufende Seite nach Login</b>	Hier können Sie eine URL angeben, zu der ein Benutzer umgeleitet wrd, wenn er sich bei der Hotspot-Lösung angemeldet hat.
<b>Sprache für Anmeldefenster</b>	Hier können Sie die Sprache für die Start/Login-Seite auswählen.  Folgende Sprachen werden unterstützt: <i>English, Deutsch, Italiano, Français, Español, Português und Nederlands</i> .  Die Sprache kann auf der Start/Login-Seite selbst jederzeit umgeschaltet werden.

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

#### Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<b>Tickettyp</b>	Wählen Sie den Tickettyp aus.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Voucher</i>: Nur der Benutzername muss eingegeben werden. Definieren Sie im Eingabefeld ein Standardpasswort.</li> <li>• <i>Benutzername/Passwort</i> (Standardwert): Benutzername und Passwort müssen eingegeben werden.</li> </ul>
<b>Zulässiger Hotspot-Client</b>	<p>Hier legen Sie fest, welche Art von Benutzern sich am Hotspot anmelden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Alle</i>: Alle Clients werden zugelassen.</li> <li>• <i>DHCP-Client</i>: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.</li> </ul>
<b>Geräte pro Ticket</b>	Geben Sie die maximale Anzahl Geräte pro Ticket an.
<b>Anmeldefenster</b>	<p>Aktivieren oder deaktivieren Sie das Anmeldefenster.</p> <p>Das Anmeldefenster auf der HTML-Startseite besteht aus zwei Frames.</p> <p>Wenn die Funktion aktiviert ist, wird auf der linken Seite das Anmelde-Formular angezeigt.</p> <p>Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Pop-Up-Fenster für Statusanzeige</b>	<p>Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Standard-Timeout bei Inaktivität</b>	<p>Aktivieren oder deaktivieren Sie den <b>Standard-Timeout bei Inaktivität</b>. Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Der Standardwert ist <i>600</i> Sekunden.</p>

## 19.10.2 Optionen

Im Menü **Lokale Dienste->Hotspot-Gateway->Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

Das Menü besteht aus folgenden Feldern:

### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Host für mehrere Standorte</b>	Wenn für einen Kunden auf dem Hotspot Server mehrere Standorte (Filialen) eingerichtet wurden, geben Sie hier den Wert des NAS-Identifiers (RADIUS-Server Parameter) ein, der für diesen Standort auf dem Hotspot Server eingetragen wurde.


## 19.11 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**.

### 19.11.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

#### 19.11.1.1 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
<b>Beschreibung</b>	Geben Sie die Bezeichnung des Filters an.

Feld	Beschreibung
<b>Dienst</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>chargen</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>Der Standardwert ist <i>any</i>.</p>
<b>Protokoll</b>	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
<b>Typ</b>	<p>Nur für <b>Protokoll</b> = <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>
<b>Verbindungsstatus</b>	<p>Bei <b>Protokoll</b> = <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"> <li>• <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden.</li> <li>• <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.</li> </ul>



Feld	Beschreibung
<b>IPv4-Zieladresse/-netzmaske</b>	<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"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.</li> </ul>
<b>IPv6-Zieladresse/-länge</b>	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>
<b>Ziel-Port/Bereich</b>	<p>Nur für <b>Protokoll</b> = <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> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>-Alle-</i> (Standardwert): Der Zielport ist nicht näher spezifiziert.</li> <li>• <i>Port angeben</i>: Geben Sie einen Zielport ein.</li> <li>• <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.</li> </ul>
<b>IPv4-Quelladresse/-netzmaske</b>	<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"> <li>• <i>Beliebig</i> (Standardwert): Die Quell-IP-Adresse/Netzmaske sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>


Feld	Beschreibung
<b>IPv6-Quelladresse/-länge</b>	<p>Geben Sie die IPv6 Quell-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Länge sind nicht näher spezifiziert.</li> <li>• <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.</li> <li>• <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.</li> </ul>
<b>Quell-Port/Bereich</b>	<p>Nur für <b>Protokoll</b> = <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"> <li>• <i>-Alle-</i> (Standardwert): Der Quellport ist nicht näher spezifiziert.</li> <li>• <i>Port angeben</i>: Geben Sie einen Quellport ein.</li> <li>• <i>Portbereich angeben</i>: Geben Sie einen Quellport-Bereich ein.</li> </ul>
<b>DSCP / Traffic Class Filter (Layer 3)</b>	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt.</li> <li>• <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).</li> <li>• <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format).</li> <li>• <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format).</li> <li>• <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111.</li> <li>• <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen For-</li> </ul>

Feld	Beschreibung
	<p>mat angegeben, z. B. 63.</p> <ul style="list-style-type: none"> <li>• <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.</li> </ul>
<b>COS-Filter (802.1p/Layer 2)</b>	<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>

## 19.11.2 WOL-Regeln

Im Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln** wird eine Liste aller konfigurierbaren WOL-Regeln angezeigt.

### 19.11.2.1 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
<b>Wake-On-LAN-Regelkette</b>	<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"> <li>• <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an.</li> <li>• <i>&lt;Name der Regelkette&gt;</i>: Zeigt eine bereits angelegte Regelkette, die Sie auswählen und bearbeiten können.</li> </ul>
<b>Beschreibung</b>	<p>Nur für <b>Wake-On-LAN-Regelkette</b> = <i>Neu</i></p> <p>Geben Sie die Bezeichnung der Regelkette ein.</p>
<b>Wake-on-LAN-Filter</b>	<p>Wählen Sie ein WOL-Filter aus.</p>

Feld	Beschreibung
	<p>Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll.</p> <p>Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll.</p> <p>Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü <b>Lokale Dienste-&gt;Wake-On-LAN-&gt;WOL-Regeln</b> konfiguriert sein.</p>
<b>Aktion</b>	<p>Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>WOL aufrufen, wenn Filter zutrifft</i>: WOL ausführen, wenn der Filter zutrifft.</li> <li>• <i>Aufrufen, wenn Filter nicht zutrifft</i>: WOL ausführen, wenn der Filter nicht zutrifft.</li> <li>• <i>WOL verweigern, wenn Filter zutrifft</i>: WOL nicht ausführen, wenn der Filter zutrifft.</li> <li>• <i>WOL verweigern, wenn Filter nicht zutrifft</i>: WOL nicht ausführen, wenn der Filter nicht zutrifft.</li> <li>• <i>Regel ignorieren und zu nächster Regel springen</i>: Diese Regel wird ignoriert und die in der Kette folgende wird überprüft.</li> </ul>
<b>Typ</b>	<p>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 <b>Sende WOL-Paket über Schnittstelle</b> festgelegt wird.</p>
<b>Sende WOL-Paket über Schnittstelle</b>	<p>Wählen Sie die Schnittstelle aus, über die das Wake on LAN Magic Packet gesendet werden soll.</p>
<b>Ziel-MAC-Adresse</b>	<p>Nur für <b>Aktion</b> = <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>
<b>Passwort</b>	<p>Nur für <b>Aktion</b> = <i>WOL aufrufen, wenn Filter zutrifft</i> und <i>Aufrufen, wenn Filter nicht zutrifft</i></p>


Feld	Beschreibung
	<p><i>trifft</i></p> <p>Wenn das Netzwerkgerät, das aktiviert werden soll, die Funktion "SecureOn" unterstützt, geben Sie hier das entsprechende Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.</p>

### 19.11.3 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.

#### 19.11.3.1 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
<b>Schnittstelle</b>	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
<b>Regelkette</b>	Wählen Sie eine Regelkette aus.

## 19.12 Trace

### 19.12.1 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.

#### Felder im Menü Trace-Einstellungen

Feld	Beschreibung
<b>Schnittstellenauswahl</b>	Wählen Sie die Schnittstelle aus, deren Datenverkehr Sie aufzeichnen wollen.
<b>Trace-Modus</b>	Hier können Sie auswählen, auf welchen Ebenen der Datenverkehr der ausgewählten Schnittstelle aufgezeichnet werden soll. Zur Auswahl stehen: <ul style="list-style-type: none"> <li>• <i>Layer 2</i></li> <li>• <i>PPP</i></li> <li>• <i>Layer 3</i></li> <li>• <i>IP</i></li> </ul>

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.

### 19.12.2 VoIP/SIP-Trace

Das Menü **VoIP/SIP-Trace** gibt Ihnen die Möglichkeit, VoIP/SIP-Meldungen auf verschiedenen Leveln aufzuzeichnen und als Textdatei auf Ihrem Computer zu speichern. Sie können aus den folgenden Trace-Leveln wählen, eine Beschreibung, welche Informationen aufgezeichnet werden wird in Abhängigkeit Ihrer Auswahl angezeigt:

- **Statusinformation:** Das Gerät schreibt den aktuellen Zustand des VoIP/SIP-Subsystems in eine Datei, die Sie dann herunterladen können.
- **Ereignisse:** Das Gerät schreibt VoIP/SIP-Informationen kontinuierlich in den Trace-Speicher, sobald Sie die Schaltfläche **Start** klicken. Sobald Sie die Schaltfläche **Stop** klicken, bekommen Sie die Möglichkeit, die Datei herunterzuladen.
- **SIP:** Das Gerät schreibt (nur) alle SIP-Meldungen kontinuierlich in den Trace-Speicher, sobald Sie die Schaltfläche **Start** klicken. Sobald Sie die Schaltfläche **Stop** klicken, bekommen Sie die Möglichkeit, die Datei herunterzuladen.

## 20 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.

### 20.1 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.

#### 20.1.1 Benutzer ausloggen

In diesem Menü sehen Sie zunächst eine Auflistung aller aktiven Konfigurationsverbindungen.

##### Felder im Menü Benutzer ausloggen

Feld	Beschreibung
<b>Klasse</b>	Zeigt die Benutzerklasse an, der der angemeldete Benutzer angehört.
<b>Benutzer</b>	Zeigt den Benutzernamen an.
<b>Entfernte IP-Adresse</b>	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.
<b>Läuft ab</b>	Zeigt an, wann die Verbindung automatisch getrennt wird.
<b>Sofort ausloggen</b>	Wenn sie das Kontrollkästchen aktivieren, wird dieser Benutzer mit einem Klick auf <b>Ausloggen</b> vom System abgemeldet.

##### 20.1.1.1 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.

## 20.2 Diagnose

Im Menü **Wartung**->**Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

### 20.2.1 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
<b>Test-Ping-Modus</b>	Wählen Sie die für den Ping-Test verwendete IP-Version.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>IPv4</i></li> <li>• <i>IPv6</i></li> </ul>
<b>Ping-Befehl testweise an Adresse senden</b>	Geben Sie die zu testende IP-Adresse ein.
<b>Zu verwendende Schnittstelle</b>	Nur für <b>Test-Ping-Modus</b> = <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.

### 20.2.2 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.



### 20.2.3 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
<b>Traceroute-Modus</b>	Wählen Sie die für den Traceroute-Test verwendete IP-Version.  Mögliche Werte: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Traceroute-Adresse</b>	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.

## 20.3 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

### 20.3.1 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](http://www.bintec-elmeg.com). Hier finden Sie auch aktuelle Dokumentationen.



#### Wichtig

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörigen Release Notes. Hier sind alle Änderungen beschrieben, die mit der neuen Systemsoftware eingeführt werden.

Die Folge von unterbrochenen Update-Vorgängen (z. B. Stromausfall während des

Updates) könnte sein, dass Ihr Gerät nicht mehr bootet. Schalten Sie Ihr Gerät nicht aus, während die Aktualisierung durchgeführt wird.

In seltenen Fällen ist zusätzlich eine Aktualisierung von BOOTmonitor und/oder Logic empfohlen. In diesem Fall wird ausdrücklich in den entsprechenden Release Notes darauf hingewiesen. Führen Sie bei BOOTmonitor oder Logic nur ein Update durch, wenn bintec elmeg GmbH eine explizite Empfehlung dazu ausspricht.

## Flash

Ihr Gerät speichert seine Konfiguration in Konfigurationsdateien im Flash EEPROM (electrically erasable programmable read-only memory). Auch wenn Ihr Gerät ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

## RAM

Im Arbeitsspeicher (RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf Ihrem Gerät einstellen. Der Inhalt des RAM geht verloren, wenn Ihr Gerät ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start Ihres Geräts beibehalten wollen, müssen Sie die geänderte Konfiguration im Flash speichern: Schaltfläche **Konfiguration speichern** über dem Navigationsbereich des **GUIs**. Dadurch wird die Konfiguration in eine Datei mit dem Namen *boot* im Flash gespeichert. Beim Starten Ihres Geräts wird standardmäßig die Konfigurationsdatei *boot* verwendet.

## Aktionen

Die Dateien im Flash-Speicher können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen Ihrem Gerät und einem Host per HTTP zu transferieren.

## Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden. So können Sie mit den Aktionen "Konfiguration exportieren", "Konfiguration mit Statusinformationen exportieren" und "Konfiguration laden"

Dateien sichern bzw. einspielen. Wenn Sie mit der Aktion "Konfiguration exportieren" oder "Konfiguration mit Statusinformationen exportieren" eine Konfigurationsdatei sichern wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll.



### Achtung

Sollten Sie über die SNMP-Shell mit dem Kommando `put` eine Konfigurationsdatei in einem alten Format gesichert haben, kann ein Wiedereinspielen auf das Gerät nicht garantiert werden. Daher wird das alte Format nicht mehr empfohlen.

Das Menü **Wartung** -> **Software & Konfiguration** -> **Optionen** besteht aus folgenden Feldern:

#### Felder im Menü Aktuell Installierte Software

Feld	Beschreibung
<b>BOSS</b>	Zeigt die aktuelle Softwareversion an, die auf Ihrem Gerät geladen ist.
<b>Systemlogik</b>	Zeigt die aktuelle Systemlogik an, die auf Ihrem Gerät geladen ist.
<b>xDSL-Logik</b>	Zeigt die aktuelle Version der xDSL-Logik an, die auf Ihrem Gerät geladen ist.

#### Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
<b>Aktion</b>	<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"> <li>• <i>Keine Aktion</i> (Standardwert):</li> <li>• <i>Konfiguration exportieren</i>: Die Konfigurationsdatei <b>Aktueller Dateiname im Flash</b> wird zu Ihrem lokalen Host transferiert. Wenn Sie die <b>Los</b>-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.</li> </ul>

Feld	Beschreibung
	<ul style="list-style-type: none"> <li>• <i>Konfiguration importieren</i>: Wählen Sie in <b>Dateiname</b> eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken auf <b>Los</b> 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!</li> <li>• <i>Konfiguration kopieren</i>: Die Konfigurationsdatei im Feld <b>Name der Quelldatei</b> wird als <b>Name der Zieldatei</b> gespeichert.</li> <li>• <i>Konfiguration löschen</i>: Die Konfiguration im Feld <b>Datei auswählen</b> wird gelöscht.</li> <li>• <i>Konfiguration umbenennen</i>: Die Konfigurationsdatei im Feld <b>Datei auswählen</b> wird zu <b>Neuer Dateiname</b> umbenannt.</li> <li>• <i>Konfigurationssicherung wiederherstellen</i>: Nur, wenn unter <b>Konfiguration speichern</b> 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.</li> <li>• <i>Software/Firmware löschen</i>: Die Datei im Feld <b>Datei auswählen</b> wird gelöscht.</li> <li>• <i>Sprache importieren</i>: Sie können weitere Sprachversionen des <b>GUI</b> auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von <a href="http://www.bintec-elmeg.com">www.bintec-elmeg.com</a> auf Ihren PC herunterladen und von dort aus in Ihr Gerät einspielen.</li> <li>• <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware, der DSL-Logik und des BOOTmonitors initiieren.</li> <li>• <i>Konfiguration mit Statusinformationen exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die <b>Los</b>-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.</li> </ul> <p>Folgende Optionen erfordern, dass eine MMC/SD-Karte gesteckt ist (sofern von Ihrem Gerät unterstützt) oder dass Ihr Ge-</p>

Feld	Beschreibung
	<p>rät über einen zusätzlichen internen Speicher verfügt:</p> <ul style="list-style-type: none"> <li>• <i>Voice Mail Wave-Dateien importieren</i> (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist, sofern von Ihrem Gerät unterstützt): Wählen Sie in <b>Dateiname</b> die Datei <i>vms_wavfiles.zip</i> aus, die Sie importieren wollen.</li> <li>• <i>Zusätzliche Dateien laden (in den USB-Speicher)</i>: Sie können zusätzliche Dateien wie Voice-Mail-Ansagen oder Wartemusik als ZIP gepackt in den USB-Speicher laden. Dort wird der Inhalt entpackt und eine entsprechende Verzeichnisstruktur erstellt. Wählen Sie in <b>Dateiname</b> die Datei aus, die Sie laden möchten.</li> <li>• <i>MMC/SD-Karte formatieren</i>: Unter Umständen muss der zusätzliche interne Speicher Ihres Geräts neu formatiert werden. Bei der Formatierung wird der gesamte Inhalt des zusätzlichen internen Speichers gelöscht!</li> </ul>
<b>Aktueller Dateiname im Flash</b>	<p>Für <b>Aktion</b> = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.</p>
<b>Zertifikate und Schlüssel einschließen</b>	<p>Für <b>Aktion</b> = <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die gewählte <b>Aktion</b> 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>
<b>Verschlüsselung der Konfiguration</b>	<p>Nur für <b>Aktion</b> = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten <b>Aktion</b> 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 <b>Passwort</b> eingeben.</p>

Feld	Beschreibung
<b>Dateiname</b>	<p>Nur für <b>Aktion</b> = <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 <b>Durchsuchen...</b> über den Dateibrowser aus.</p>
<b>Name der Quelldatei</b>	<p>Nur für <b>Aktion</b> = <i>Konfiguration kopieren</i></p> <p>Wählen Sie die Quelldatei aus, die kopiert werden soll.</p>
<b>Name der Zieldatei</b>	<p>Nur für <b>Aktion</b> = <i>Konfiguration kopieren</i></p> <p>Geben Sie den Namen der Kopie ein.</p>
<b>Datei auswählen</b>	<p>Nur für <b>Aktion</b> = <i>Konfiguration löschen, Konfiguration umbenennen</i> oder <i>Software/Firmware löschen</i></p> <p>Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.</p>
<b>Neuer Dateiname</b>	<p>Nur für <b>Aktion</b> = <i>Konfiguration umbenennen</i></p> <p>Geben Sie den neuen Namen der Konfigurationsdatei ein.</p>
<b>Quelle</b>	<p>Nur für <b>Aktion</b> = <i>Systemsoftware aktualisieren</i></p> <p>Wählen Sie die Quelle der Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Lokale Datei</i> (Standardwert): Die Systemsoftware-Datei ist lokal auf Ihrem PC gespeichert.</li> <li>• <i>HTTP-Server</i>: Die Datei ist auf dem entfernten Server gespeichert, der in der <b>URL</b> angegeben wird.</li> <li>• <i>Aktuelle Software vom Update-Server</i>: Die Datei liegt auf dem offiziellen Update-Server.</li> </ul>
<b>URL</b>	<p>Nur für <b>Aktion</b> = <i>Systemsoftware aktualisieren</i> und <b>Quelle</b> = <i>HTTP-Server</i></p> <p>Geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.</p>

Im Menü **Erweiterte Einstellungen** wird die Version der aktuell installierten internen Sys-

tem- Dateien angezeigt.

## 20.4 Neustart

### 20.4.1 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.

## 20.5 Factory Reset

Im Menü **Wartung->Factory Reset** können Sie Ihr Gerät über das GUI in den Auslieferungszustand versetzen.

## 21 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.

### 21.1 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](http://www.bintec-elmeg.com)).

#### 21.1.1 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.

### 21.1.1.1 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
<b>IP-Adresse</b>	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
<b>Level</b>	<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"> <li>• <i>Notfall</i> (höchste Priorität)</li> <li>• <i>Alarm</i></li> <li>• <i>Kritisch</i></li> <li>• <i>Fehler</i></li> <li>• <i>Warnung</i></li> <li>• <i>Benachrichtigung</i></li> <li>• <i>Information</i> (Standardwert)</li> <li>• <i>Debug</i> (niedrigste Priorität)</li> </ul> <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>
<b>Facility</b>	<p>Geben Sie die Syslog Facility auf dem Host an.</p> <p>Dieses ist nur erforderlich, wenn der <b>Log Host</b> ein Unix-Rechner ist.</p> <p>Mögliche Werte: <i>local0</i> - 7 (Standardwert)</p>

Feld	Beschreibung
	<i>local0.</i>
<b>Zeitstempel</b>	<p>Wählen Sie das Format des Zeitstempels im Systemprotokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Keine Systemzeitangabe.</li> <li>• <i>Zeit</i>: Systemzeit ohne Datum.</li> <li>• <i>Datum &amp; Uhrzeit</i>: Systemzeit mit Datum.</li> </ul>
<b>Protokoll</b>	<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"> <li>• <i>UDP</i> (Standardwert)</li> <li>• <i>TCP</i></li> </ul>
<b>Nachrichtentyp</b>	<p>Wählen Sie den Nachrichtentyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>System &amp; Accounting</i> (Standardwert)</li> <li>• <i>System</i></li> <li>• <i>Accounting</i></li> </ul>

## 21.2 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.

## 21.2.1 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.

## 21.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

Protokollformat

INET: %d %t %a %c %i:%r/%f -> %l:%R/%

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

Feld	Beschreibung
%R	Zielport
%F	Ziel-Schnittstellen-Index
%p	Ausgegangene Pakete
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen:

```
INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

## 21.3 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.

### 21.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

#### 21.3.1.1 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
<b>Benachrichtigungsdienst</b>	<p>Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• E-Mail</li> <li>• SMS</li> </ul>
<b>Empfänger</b>	Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des

Feld	Beschreibung
	Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
<b>Nachrichtenkompri- mierung</b>	<p>Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse.</p> <p>Aktivieren oder deaktivieren Sie das Feld.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Betreff</b>	Sie können einen Betreff eingeben.
<b>Ereignis</b>	<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"> <li>• <i>Systemmeldung enthält Zeichenfolge</i> (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge.</li> <li>• <i>Neuer Neighbor-AP gefunden</i>: Ein neuer benachbarter AP wurde gefunden.</li> <li>• <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.</li> <li>• <i>Neuer Access Point (WTP) gefunden</i>: Eine neuer unkonfigurierter AP hat sich beim WLAN Controller gemeldet.</li> <li>• <i>Verwalteter AP offline</i>: Ein managed AP ist nicht mehr erreichbar.</li> </ul>
<b>Enthaltene Zeichenfolge</b>	<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 Sys-</p>

Feld	Beschreibung
	log-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.
<b>Schweregrad</b>	<p>Wählen Sie den Schweregrad aus, auf dem der im Feld <b>Enthaltene Zeichenfolge</b> 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>
<b>Überwachte Subsysteme</b>	<p>Wählen Sie die Subsysteme aus, die überwacht werden sollen.</p> <p>Fügen Sie mit <b>Hinzufügen</b> neue Subsysteme hinzu.</p>
<b>Timeout für Nachrichten</b>	<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>
<b>Anzahl Nachrichten</b>	<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>

### 21.3.2 Benachrichtigungseinstellungen

Das Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungseinstellungen** besteht aus folgenden Feldern:

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>Benachrichtigungsdienst</b>	Wählen Sie aus, ob der Benachrichtigungsdienst aktiviert werden soll.

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<b>Maximale E-Mails pro Minute</b>	<p>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>.</p>

#### Felder im Menü E-Mail-Parameter

Feld	Beschreibung
<b>E-Mail-Adresse des Senders</b>	Geben Sie die Mailadresse ein, die in das Absenderfeld der E-Mail eingetragen werden soll.
<b>SMTP-Server</b>	<p>Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der Mails verwendet werden soll.</p> <p>Die Eingabe ist auf 40 Zeichen begrenzt.</p>
<b>SMTP-Port</b>	<p>Verschlüsselung von E-Mails (SSL/TLS).</p> <p>Das Feld <b>SMTP-Port</b> ist Standardmäßig auf <i>25</i> voreingestellt und <b>SSL</b> Encryption aktiviert.</p>
<b>SMTP-Authentifizierung</b>	<p>Authentifizierung, die der SMTP-Server erwartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Keiner</i> (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung.</li> <li>• <i>ESMTP</i>: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt.</li> <li>• <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.</li> </ul>
<b>Benutzername</b>	<p>Nur wenn <b>SMTP-Authentifizierung</b> = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.</p>

Feld	Beschreibung
<b>Passwort</b>	Nur wenn <b>SMTP-Authentifizierung</b> = <i>ESMTP</i> oder <i>SMTP after POP</i>  Geben Sie das Passwort dieses Benutzers an.
<b>POP3-Server</b>	Nur wenn <b>SMTP-Authentifizierung</b> = <i>SMTP after POP</i>  Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.
<b>POP3-Timeout</b>	Nur wenn <b>SMTP-Authentifizierung</b> = <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
<b>SMS-Gerät</b>	Sie können sich über Systemmeldungen per SMS informieren lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
<b>Maximale SMS pro Tag</b>	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> .

## 21.4 SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll in der IP-Protokollfamilie für den Transport von Managementinformationen über Netzwerkkomponenten.

Zu den Bestandteilen eines jeden SNMP-Managementsystems zählt u. a. eine MIB. Über SNMP sind verschiedene Netzwerkkomponenten von einem System aus zu konfigurieren,



zu kontrollieren und zu überwachen. Mit Ihrem Gerät haben Sie ein solches SNMP-Werkzeug erhalten, den Konfigurationsmanager. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HPOpenView verwenden.

Weitergehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

### 21.4.1 SNMP-Trap-Optionen

Zur Überwachung des Systems wird im Fehlerfall unaufgefordert eine Nachricht gesendet, ein sogenanntes Trap-Paket.

Im Menü **Externe Berichterstellung** -> **SNMP** -> **SNMP-Trap-Optionen** können Sie das Senden von Traps konfigurieren.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>SNMP Trap Broadcasting</b>	<p>Wählen Sie aus, ob die Übertragung von SNMP-Traps aktiviert werden soll.</p> <p>Ihr Gerät sendet SNMP-Traps dann an die Broadcast-Adresse des LANs.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>SNMP-Trap-UDP-Port</b>	<p>Nur wenn <b>SNMP Trap Broadcasting</b> aktiviert ist.</p> <p>Geben Sie die Nummer des UDP-Ports ein, zu dem Ihr Gerät SNMP-Traps senden soll.</p> <p>Möglich ist jeder ganzzahlige Wert.</p> <p>Der Standardwert ist <i>162</i>.</p>
<b>SNMP-</b>	<p>Nur wenn <b>SNMP Trap Broadcasting</b> aktiviert ist.</p>

Feld	Beschreibung
<b>Trap-Community</b>	<p>Geben Sie eine SNMP-Kennung ein. Diese muss vom SNMP-Manager mit jeder SNMP-Anforderung übergeben werden, damit sie von Ihrem Gerät akzeptiert wird.</p> <p>Möglich ist eine Zeichenkette mit 0 bis 255 Zeichen.</p> <p>Der Standardwert ist <i>snmp-Trap</i>.</p>

## 21.4.2 SNMP-Trap-Hosts

In diesem Menü geben Sie an, an welche IP-Adressen Ihr Gerät die SNMP-Traps schicken soll.

Im Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts** wird eine Liste aller konfigurierten SNMP-Trap-Hosts angezeigt.

### 21.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

Das Menü **Externe Berichterstellung**->**SNMP**->**SNMP-Trap-Hosts**->**Neu** besteht aus folgenden Feldern:

#### Felder im Menü Basisparameter

Feld	Beschreibung
<b>IP-Adresse</b>	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

## 21.5 SIA

### 21.5.1 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.

## 22 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.

### 22.1 Internes Protokoll

#### 22.1.1 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
<b>Nr.</b>	Zeigt die laufende Nummer der System-Meldung an.
<b>Datum</b>	Zeigt das Datum der Aufzeichnung an.
<b>Zeit</b>	Zeigt die Uhrzeit der Aufzeichnung an.
<b>Level</b>	Zeigt die hierarchische Einstufung der Meldung an.
<b>Subsystem</b>	Zeigt an, welches Subsystem Ihres Geräts die Meldung generiert hat.
<b>Nachricht</b>	Zeigt den Meldungstext an.

### 22.2 IPsec



#### 22.2.1 IPsec-Tunnel


Im Menü **Monitoring->IPsec->IPsec-Tunnel** wird eine Liste aller konfigurierten IPsec-Tunnel angezeigt.

##### Werte in der Liste IPsec-Tunnel

Feld	Beschreibung
<b>Beschreibung</b>	Zeigt den Namen der IPsec-Verbindung an.

Feld	Beschreibung
<b>Entfernte IP-Adresse</b>	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
<b>Entfernte Netzwerke</b>	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
<b>Sicherheitsalgorithmus</b>	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
<b>Status</b>	Zeigt den Betriebszustand der IPSec-Verbindung an.
<b>Aktion</b>	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
<b>Details</b>	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
<b>Beschreibung</b>	Zeigt die Beschreibung des Peers an.
<b>Lokale IP-Adresse</b>	Zeigt die WAN-IP-Adresse Ihres Geräts an.
<b>Entfernte IP-Adresse</b>	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
<b>Lokale ID</b>	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
<b>Entfernte ID</b>	Zeigt die ID des Peers an.
<b>Aushandlungsmodus</b>	Zeigt den Aushandlungsmodus an.
<b>Authentifizierungsmethode</b>	Zeigt die Authentifizierungsmethode an.
<b>MTU</b>	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
<b>Erreichbarkeitsprüfung</b>	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
<b>NAT-Erkennung</b>	Zeigt die NAT-Erkennungsmethode an.
<b>Lokaler Port</b>	Zeigt den lokalen Port an.
<b>Entfernter Port</b>	Zeigt den entfernten Port an.
<b>Pakete</b>	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
<b>Bytes</b>	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
<b>Fehler</b>	Zeigt die Anzahl der Fehler an.
<b>IKE (Phase-1) SAs (x)</b>	Zeigt die Parameter der IKE (Phase 1) SAs an.

Feld	Beschreibung
<b>Rolle / Algorithmus / Verbleibende Lebensdauer / Status</b>	
<b>IPSec (Phase-2) SAs (x)</b>	Zeigt die Parameter der IPSec (Phase 2) SAs an.
<b>Rolle / Algorithmus / Verbleibende Lebensdauer / Status</b>	
<b>Nachrichten</b>	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

## 22.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

Das Menü besteht aus folgenden Feldern:

### Feld im Menü Lizenzen

Feld	Beschreibung
<b>IPSec-Tunnel</b>	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen ( <b>In Verwendung</b> ) und die Anzahl der maximal verwendbaren Lizenzen ( <b>Maximal</b> ) an.

### Feld im Menü Peers

Feld	Beschreibung
<b>Status</b>	<p>Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an.</p> <ul style="list-style-type: none"> <li>• <b>Aktiv:</b> Aktuell aktive IPSec-Verbindungen.</li> <li>• <b>Aktivieren:</b> IPSec-Verbindungen, die sich aktuell in der Tunnelaufbau-Phase befinden.</li> <li>• <b>Blockiert:</b> IPSec-Verbindungen, die geblockt sind.</li> <li>• <b>Ruhend:</b> Aktuell inaktive IPSec-Verbindungen.</li> <li>• <b>Konfiguriert:</b> Konfigurierte IPSec-Verbindungen.</li> </ul>

### Felder im Menü SAs

Feld	Beschreibung
<b>IKE (Phase-1)</b>	Zeigt die Anzahl der aktiven Phase-1-SAs ( <b>Hergestellt</b> ) zur Gesamtzahl der Phase-1-SAs ( <b>Gesamt</b> ) an.
<b>IPSec (Phase-2)</b>	Zeigt die Anzahl der aktiven Phase-2-SAs ( <b>Hergestellt</b> ) zur Gesamtzahl der Phase-2-SAs ( <b>Gesamt</b> ) an.

#### Felder im Menü Paketstatistiken



Feld	Beschreibung
<b>Gesamt</b>	Zeigt die Anzahl aller verarbeiteten eingehenden ( <b>Eingehend</b> ) bzw. ausgehenden ( <b>Ausgehend</b> ) Pakete an.
<b>Weitergeleitet</b>	Zeigt die Anzahl der eingehenden ( <b>Eingehend</b> ) bzw. ausgehenden ( <b>Ausgehend</b> ) Pakete an, die im Klartext weitergeleitet wurden.
<b>Verworfen</b>	Zeigt die Anzahl der verworfenen eingehenden ( <b>Eingehend</b> ) bzw. ausgehenden ( <b>Ausgehend</b> ) Pakete an.
<b>Verschlüsselt</b>	Zeigt die Anzahl der durch IPSec geschützten eingehenden ( <b>Eingehend</b> ) bzw. ausgehenden ( <b>Ausgehend</b> ) Pakete an.
<b>Fehler</b>	Zeigt die Anzahl der eingehenden ( <b>Eingehend</b> ) bzw. ausgehenden ( <b>Ausgehend</b> ) Pakete an, bei deren Behandlung es zu Fehlern gekommen ist.

## 22.3 Schnittstellen

### 22.3.1 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
<b>Nr.</b>	Zeigt die laufende Nummer der Schnittstelle an.
<b>Beschreibung</b>	Zeigt den Namen der Schnittstelle an.

Feld	Beschreibung
<b>Typ</b>	Zeigt den Schnittstellentyp an.
<b>Tx-Pakete</b>	Zeigt die Gesamtzahl der gesendeten Pakete an.
<b>Tx-Bytes</b>	Zeigt die Gesamtzahl der gesendeten Oktetts an.
<b>Tx-Fehler</b>	Zeigt die Gesamtzahl der gesendeten Fehler an.
<b>Rx-Pakete</b>	Zeigt die Gesamtzahl der erhaltenen Pakete an.
<b>Rx-Bytes</b>	Zeigt die Gesamtzahl der erhaltenen Bytes an.
<b>Rx-Fehler</b>	Zeigt die Gesamtzahl der erhaltenen Fehler an.
<b>Status</b>	Zeigt den Betriebszustand der gewählten Schnittstelle an.
<b>Nicht geändert seit</b>	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
<b>Aktion</b>	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
<b>Beschreibung</b>	Zeigt den Namen der Schnittstelle an.
<b>MAC-Adresse</b>	Zeigt die MAC-Adresse an.
<b>IP-Adresse/Netzmaske</b>	Zeigt die IP-Adresse und die Netzmaske an.
<b>NAT</b>	Zeigt an, ob NAT für diese Schnittstelle aktiviert ist.
<b>Tx-Pakete</b>	Zeigt die Gesamtzahl der gesendeten Pakete an.
<b>Tx-Bytes</b>	Zeigt die Gesamtzahl der gesendeten Oktetts an.
<b>Rx-Pakete</b>	Zeigt die Gesamtzahl der erhaltenen Pakete an.
<b>Rx-Bytes</b>	Zeigt die Gesamtzahl der erhaltenen Bytes an.

#### Feld im Menü TCP-Verbindungen

Feld	Beschreibung
<b>Status</b>	Zeigt den Status einer aktiven TCP-Verbindung an.
<b>Lokale Adresse</b>	Zeigt die lokale IP-Adresse der Schnittstelle für eine aktive TCP-Verbindung an.
<b>Lokaler Port</b>	Zeigt den lokalen Port der IP-Adresse für eine aktive TCP-Verbindung an.
<b>Remote-Adresse</b>	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.

Feld	Beschreibung
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

## 22.3.2 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.

## 22.4 Bridges

### 22.4.1 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.

## 22.5 Hotspot-Gateway

### 22.5.1 Hotspot-Gateway

Im Menü **Monitoring->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

Werte in der Liste **Hotspot-Gateway**

Feld	Beschreibung
Benutzername	Zeigt den Namen des Benutzers an.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Physische Adresse	Zeigt die Physische Adresse des Benutzers an.



Feld	Beschreibung
<b>Anmeldung</b>	Zeigt den Zeitpunkt der Anmeldung an.
<b>Schnittstelle</b>	Zeigt die verwendete Schnittstelle an.

## 22.6 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

### 22.6.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

#### Werte in der Liste QoS

Feld	Beschreibung
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
<b>QoS-Queue</b>	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
<b>Senden</b>	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
<b>Verworfen</b>	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
<b>Queued</b>	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

## 23 Benutzerzugang

Der Administrator des Systems kann den Benutzern einen individuellen Oberflächen-Konfigurationszugang einrichten. So können Sie sich als Benutzer die wichtigsten persönlichen Einstellungen anzeigen lassen und bestimmte individuell anpassen.

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

Nach erfolgreichem Anmelden wird die **Status**-Seite angezeigt. Diese enthält eine Übersicht über Ihre wichtigsten Einstellungen.

Im Menü **Telefonbuch** können Sie das **System-Telefonbuch** einsehen und Einträge in einem benutzerspezifischen Telefonbuch anlegen, bearbeiten sowie löschen.

Im Menü **Verbindungsdaten** erhalten Sie eine detaillierte Übersicht über die von Ihnen geführten und angenommenen Gespräche.

Das Menü **Einstellungen** enthält eine Übersicht über die aktuellen Einstellungen der Leistungsmerkmale **Direktruf**, **Anrufweitschaltung (AWS)** und **Parallelruf**. Diese können Sie hier individuell anpassen. Weiterhin können Sie allgemeine Einstellungen einsehen und Zugangs- und Kontaktdaten anpassen.

### 23.1 Status

Im Menü **Benutzerzugang->Status** werden die wichtigsten Einstellungen angezeigt, die vom Administrator des Systems für Sie vorgenommen wurden.

Das Menü besteht aus folgenden Feldern:

#### Werte in der Liste Benutzerdaten

Feld	Beschreibung
<b>Name, Vorname</b>	Zeigt den konfigurierten Namen und ggf. Vornamen Ihres Benutzers an.
<b>Beschreibung</b>	Zeigt die konfigurierte zusätzliche Beschreibung für Ihren Benutzer an.

#### Werte in der Liste Interne Rufnummern & Verbindungskosten

Feld	Beschreibung
<Interne Rufnummer>	Zeigt die Verbindungskosten für die internen Rufnummern an,

Feld	Beschreibung
	die Ihrem Benutzer zugeordnet wurden.

#### Werte in der Liste Weitere Einstellungen

Feld	Beschreibung
<b>Aktuelle Berechtigungsklasse</b>	Zeigt den Namen der Berechtigungsklasse an, zu der Ihr Benutzer zugeordnet ist.
<b>Wahlberechtigung</b>	<p>Zeigt die Wahlberechtigung Ihrer Telefone an. Diese leitet sich ab aus der Einstellung für die entsprechende Benutzerklasse.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>International</i>: Die Telefone haben uneingeschränkte Berechtigungen für die Wahl und können alle Verbindungen selbst einleiten.</li> <li>• <i>National</i>: Die Telefone können außer internationalen Gesprächen alle Gespräche selbst einleiten. Beginnt eine Rufnummer mit der Kennziffer für internationale Wahl, kann diese Rufnummer nicht gewählt werden.</li> <li>• <i>Kommand</i>: Die Telefone sind kommand für externe Gespräche erreichbar, können aber selbst keine externen Gespräche einleiten. Interne Gespräche sind möglich.</li> <li>• <i>Region</i>: Die Telefone können keine nationalen und internationalen Gespräche führen. Für diese Wahlberechtigung sind 10 Ausnahmerufnummern konfigurierbar, über die eine nationale oder internationale Wahl ermöglicht werden kann. Eine Ausnahmerufnummer kann aus vollständigen Rufnummern oder Teilen einer Rufnummer (z. B. die ersten Ziffern) bestehen.</li> <li>• <i>Ort</i>: Die Telefone können Ortsgespräche führen. Nationale und internationale Gespräche sind nicht möglich.</li> <li>• <i>Intern</i>: Die Telefone sind kommand und gehend nicht für externe Gespräche berechtigt. Es können nur interne Gespräche geführt werden.</li> </ul>
<b>Manuelle Bündelbelegung zulassen</b>	Zeigt an, ob Ihr Benutzer einer Berechtigungsklasse zugeordnet ist, für die die manuelle Bündelbelegung erlaubt wurde. Wenn ja, werden die zulässigen Bündel bzw. externen Anschlüsse angezeigt.

Feld	Beschreibung
	<p>Neben der allgemeinen Amtsbelegung kann ein Telefon auch gezielt ein Bündel belegen. Hierbei wird eine externe Verbindung mit der entsprechenden Kennziffer zur gezielten Belegung des Bündels eingeleitet und nicht durch die Wahl der Amtskennziffer.</p> <p>Um eine gezielte Bündelbelegung durchführen zu können, muss die Berechtigungsklasse die Berechtigung dafür besitzen. Diese Berechtigung kann auch Bündel umfassen, die die Berechtigungsklasse sonst nicht belegen kann. Hat ein Telefon nicht die Berechtigung zur gezielten Bündelbelegung oder ist das gewählte Bündel belegt, hört es nach Wahl der Kennziffer den Besetztton. Ist für eine Berechtigungsklasse die <b>Automatische Amtsholung</b> eingerichtet, müssen Benutzer dieser Berechtigungsklasse vor einer gezielten Bündelbelegung die Stern-Taste betätigen und anschließend die externe Wahl durch die Kennziffer zur Bündelbelegung einleiten.</p>
<b>Pick-Up-Gruppe</b>	Zeigt die Nummer der Gruppe an, in der Rufe herangeholt werden dürfen.

## 23.2 Telefonbuch

Im Menü **Telefonbuch** werden die Telefonbucheinträge getrennt nach **System-Telefonbuch** und **Benutzertelefonbuch** angezeigt. Im **Benutzertelefonbuch** kann der Benutzer bis zu 50 eigene Einträge anlegen, ändern oder löschen. Diese Einträge können ausschließlich vom jeweiligen Benutzer eingesehen werden. Die Pflege dieser Einträge erfolgt über das **GUI**.

### 23.2.1 System-Telefonbuch

Im **System-Telefonbuch** werden die Einträge des Gesamtsystems angezeigt, die vom Administrator angelegt wurden. Sie können sie nicht ändern.

#### Werte in der Liste Systemtelefonbuch


Feld	Beschreibung
<b>Beschreibung</b>	Zeigt eine Beschreibung des Teilnehmers an. Das <b>System-Telefonbuch</b> ist nach diesen Einträgen sortiert.
<b>Telefonnummer</b>	Zeigt die Telefonnummer an.

Feld	Beschreibung
<b>Kurzwahl</b>	Zeigt die Kurzwahl an.
<b>Call Through</b>	Zeigt, ob die Telefonnummer für die Funktion <b>Call Through</b> freigegeben ist.

## 23.2.2 Benutzertelefonbuch

Im **Benutzertelefonbuch** werden Ihre Benutzereinträge angezeigt. Sie können Einträge hinzufügen, bearbeiten oder löschen.

### 23.2.2.1 Bearbeiten oder Neu

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

Das Menü **Benutzerzugang->Telefonbuch->Benutzertelefonbuch->Neu** besteht aus folgenden Feldern:

#### Felder im Menü Telefonbucheintrag

Feld	Beschreibung
<b>Beschreibung</b>	Geben Sie eine Beschreibung für den Eintrag ein. Die Sortierung im <b>Benutzertelefonbuch</b> erfolgt nach den ersten Buchstaben der Einträge.
<b>Telefonnummer</b>	Geben Sie die Telefonnummer ein (intern oder extern).

## 23.3 Verbindungsdaten

im Menü **Verbindungsdaten** werden die bisher erfassten ausgehenden und eingehenden Verbindungen Ihres Benutzers angezeigt.

### 23.3.1 Gehend

Das Menü **Verbindungsdaten->Gehend** besteht aus folgenden Feldern:

#### Werte in der Liste Gehend

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.

Feld	Beschreibung
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Dauer</b>	Zeigt die Dauer der Verbindung an.
<b>Benutzer</b>	Zeigt den Benutzer an, der angerufen hat.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Angerufener Name</b>	Zeigt den Namen an, der angerufen hat.
<b>Gewählte Rufnummer</b>	Zeigt die gewählte Rufnummer an.
<b>Projektnummer</b>	Zeigt ggf. die Projektnummer des Gesprächs an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung nach Extern geleitet wurde.
<b>Kosten</b>	Zeigt die Kosten der Verbindung an, jedoch nur, wenn der Provider die entsprechenden Informationen übermittelt.

### 23.3.2 Kommend

Das Menü **Verbindungsdaten->Kommend** besteht aus folgenden Feldern:

#### Werte in der Liste Kommend

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Dauer</b>	Zeigt die Dauer der Verbindung an.
<b>Benutzer</b>	Zeigt den Benutzer an, der angerufen wurde.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Angerufener Name</b>	Zeigt den Namen an, der angerufen hat.
<b>Externe Rufnummer</b>	Zeigt die Rufnummer des Anrufers an.
<b>Projektnummer</b>	Zeigt ggf. die Projektnummer des Gesprächs an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung von Extern

Feld	Beschreibung
	eingegangen ist.

## 23.4 Anrufliste

Im Menü **Anwendungen**->**Anrufliste** können Sie Details eingehender und ausgehender Rufe einsehen.

### 23.4.1 Kommend

Im Menü **Anwendungen**->**Anrufliste**->**Kommend** enthält Informationen, die das Überwachen der kommenden Aktivitäten ermöglichen.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Kommend

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Typ</b>	Zeigt den Typ der Verbindung an.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Anrufernummer</b>	Zeigt die Nummer des Anrufers an.
<b>Anschlussrufnummer</b>	Zeigt die Nummer des Anschlusses an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.
<b>Löschen</b>	Für alle angezeigten Geräte können Sie die Schaltflächen <b>Alle auswählen</b> bzw. <b>Alle deaktivieren</b> nutzen.

### 23.4.2 Gehend

Das Menü **Anwendungen**->**Anrufliste**->**Gehend** enthält Informationen, die das Überwachen der gehenden Aktivitäten ermöglichen.

Das Menü besteht aus folgenden Feldern:

**Felder im Menü Gehend**

Feld	Beschreibung
<b>Datum</b>	Zeigt das Datum der Verbindung an.
<b>Zeit</b>	Zeigt die Uhrzeit zu Beginn des Gesprächs an.
<b>Typ</b>	Zeigt den Typ der Verbindung an.
<b>Int. Rufnr.</b>	Zeigt die interne Rufnummer des Benutzers an.
<b>Gewählte Rufnummer</b>	Zeigt die gewählte Nummer an.
<b>Anschlussrufnummer</b>	Zeigt die Nummer des Anschlusses an.
<b>Schnittstelle</b>	Zeigt die Schnittstelle an, über die die Verbindung von Extern eingegangen ist.
<b>Löschen</b>	Für alle angezeigten Geräte können Sie die Schaltflächen <b>Alle auswählen</b> bzw. <b>Alle deaktivieren</b> nutzen.

## 23.5 Einstellungen

Im Menü **Einstellungen** können Sie persönliche Einstellungen zu den Leistungsmerkmalen "Direktruf", "Anrufweiterschaltung (AWS)", "Parallelruf" und "Anrufschutz" vornehmen und allgemeinen Einstellungen anpassen.

### 23.5.1 Einstellungen von Features

Im Menü **Einstellungen->Einstellungen von Features** können die Einstellungen für die Leistungsmerkmale "Direktruf", "Anrufweiterschaltung (AWS)", "Parallelruf" und "Anrufschutz" angepasst werden.

#### 23.5.1.1 Anrufweiterschaltung (AWS)


Im Menü **Einstellungen->Einstellungen von Features->Anrufweiterschaltung (AWS)** konfigurieren Sie Weiterleitungen von kommenden Rufen auf Ihre interne Rufnummer auf die eingetragene Zielrufnummer.


Sie sind vorübergehend nicht in Ihrem Büro und möchten dennoch keinen Anruf verpassen. Mit einer Anrufweiterschaltung zu einer anderen Rufnummer, z. B. Ihr Handy, können Sie ihre Anrufe auch annehmen, wenn Sie nicht am Platz sind. Sie können Anrufe für Ihre



Rufnummer zu einer beliebigen Rufnummer weiterschalten. Sie kann *Sofort*, *Bei Nichtmelden* oder *Bei Besetzt* erfolgen. Anrufweiterschaltungen *Bei Nichtmelden* und *Bei Besetzt* können gleichzeitig bestehen. Sind Sie z. B. nicht in der Nähe Ihres Telefons, wird der Anruf nach einer kurzen Zeit zu einer anderen Rufnummer (z. B. Ihr Handy) weitergeschaltet. Führen Sie bereits ein Telefongespräch an Ihrem Arbeitsplatz, erhalten weitere Anrufer möglicherweise Besetzt. Diese Anrufer können Sie mit einer Anrufweiterschaltung bei Besetzt z. B. zu einem Kollegen oder dem Sekretariat weiterschalten.

Die Anrufweiterschaltung kann zu internen Teilnehmer-Rufnummern, internen Team-Rufnummern oder externen Rufnummern erfolgen. Bei der Eingabe der Rufnummer, zu der die Anrufe weitergeschaltet werden sollen, prüft das System automatisch, ob es sich um eine interne oder um eine externe Rufnummer handelt.

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Wählen Sie die Schaltfläche , um Web-Konfigurator des IP1x0-Telefons zu gelangen. Dieser wird in der Bedienungsanleitung zum Telefon beschrieben.

Das Menü **Einstellungen->Einstellungen von Features->Anrufweiterschaltung (AWS)** besteht aus folgenden Feldern:

#### Felder im Menü Anrufweiterschaltung (AWS)

Feld	Beschreibung
<b>Aktive Funktion</b>	Wählen Sie aus, ob Sie für Ihr Telefon die Funktion Anrufweiterschaltung (AWS) aktivieren wollen.  Mit <i>Aktiviert</i> wird die Funktion aktiviert.  Standardmäßig ist die Funktion nicht aktiv.
<b>Typ</b>	Wählen Sie aus, wann kommende Anrufe auf die angegebene interne Rufnummer weitergeschaltet werden sollen.  Mögliche Werte: <ul style="list-style-type: none"> <li>• <i>Sofort</i></li> <li>• <i>Bei Besetzt</i></li> <li>• <i>Bei Nichtmelden</i> (Standardwert)</li> <li>• <i>Bei Besetzt / Bei Nichtmelden</i></li> </ul>
<b>Ziel bei Nichtmelden</b>	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei Nichtmelden weitergeschaltet werden sollen.
<b>Ziel bei Besetzt</b>	Geben Sie die Rufnummer ein, auf die kommende Anrufe bei Besetzt weitergeschaltet werden sollen.

Feld	Beschreibung
Ziel Sofort	Geben Sie die Rufnummer ein, auf die kommende Anrufe sofort weitergeschaltet werden sollen.

### 23.5.1.2 Parallelruf

Im Menü **Einstellungen->Einstellungen von Features->Parallelruf** konfigurieren Sie, welche Anrufe an Ihrem Endgerät signalisiert werden sollen.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Anrufschutz

Feld	Beschreibung
<b>Aktive Funktion</b>	Wählen Sie aus, ob Sie für Ihr Telefon die Funktion Parallelruf aktivieren wollen.  Mit <i>Aktiviert</i> wird die Funktion aktiviert.  Standardmäßig ist die Funktion nicht aktiv.
<b>Externe Rufnummer</b>	Geben Sie zu <i>Individuelle Rufnummer</i> die externe Telefonnummer ein, auf der ein Anruf parallel signalisiert werden soll. Sind eine Mobilnummer oder eine Rufnummer privat eingerichtet, werden diese unter <i>Konfigurierte Rufnummer privat</i> oder <i>Konfigurierte Mobilnummer</i> angezeigt und können ausgewählt werden.

### 23.5.1.3 Direktruf

Sie möchten Ihr Telefon so einrichten, dass die Verbindung zu einer bestimmten Rufnummer auch ohne die Eingabe der Rufnummer aufgebaut wird (z. B. Notruftelefon). Sie befinden sich außer Haus. Es gibt jedoch jemanden zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Haben Sie für ihr Telefon die Funktion Direktruf eingerichtet, braucht nur der Hörer des Telefons abgehoben zu werden. Nach einer in der Konfiguration eingestellten Zeit ohne weitere Eingaben wählt das System automatisch die festgelegte Direktrufnummer.

Wählen Sie nach dem Abheben des Hörers nicht innerhalb der vorgegebenen Zeit, wird die automatische Wahl eingeleitet.

Das Menü **Einstellungen->Einstellungen von Features->Direktruf** besteht aus folgenden Feldern:

#### Felder im Menü Direktruf

Feld	Beschreibung
<b>Aktive Funktion</b>	<p>Wählen Sie aus, ob Sie für Ihr Telefon die Funktion "Direktruf" aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Rufnummer (MSN)</b>	<p>Wählen Sie aus, welche Nummer Sie für den Direktruf verwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Vorkonfigurierte Nummer</i>: Wählen Sie aus der Drop-down-Liste die gewünschte Rufnummer aus, zu der der Direktruf aufgebaut werden soll.</li> <li>• <i>Individuelle Rufnummer</i>: Geben Sie in das Eingabefeld die gewünschte Rufnummer ein, zu der der Direktruf aufgebaut werden soll.</li> </ul>

### 23.5.1.4 Anrufschutz

Mit dem Leistungsmerkmal „Anrufschutz“ (Ruhe vor der Telefon) konfigurieren Sie, welche Anrufe an Ihrem Endgerät signalisiert werden sollen.

Das Menü **Einstellungen->Einstellungen von Features->Anrufschutz** besteht aus folgenden Feldern:

#### Felder im Menü Anrufschutz

Feld	Beschreibung
<b>Aktive Funktion</b>	<p>Wählen Sie aus, ob Sie für Ihr Telefon die Funktion „Anrufschutz“ aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<b>Anrufschutz</b>	<p>Mit dem Leistungsmerkmal Anrufschutz können Sie die Signalisierung von Anrufen an Ihrem Endgerät schalten. Analoge Endgeräte nutzen dafür Kennziffern des Systems.</p> <p>Wählen Sie aus, für welche Anrufe Sie das Leistungsmerkmal nutzen wollen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• <i>Kein Signal für interne Anrufe</i></li> <li>• <i>Kein Signal für externe Anrufe</i></li> <li>• <i>Keine Anrufe</i></li> </ul>

### 23.5.1.5 Einloggen/Ausloggen

Es ist lediglich mit Systemtelefonen möglich sich über die Funktionstaste **Einloggen/Ausloggen** aus einem Team auszuloggen. Bei Standardtelefonen muss diese Funktion der Team-Administrator manuell ausführen.

Das Menü **Einstellungen->Einstellungen von Features->Einloggen/Ausloggen** besteht aus folgenden Feldern:

#### Felder im Menü Einloggen/Ausloggen

Feld	Beschreibung
<b>Beschreibung</b>	Zeigt an, welchen Teams der Benutzer angehört.
<b>Status</b>	<p>Wählen Sie aus, ob das Teammitglied am Team an- oder abgemeldet sein soll.</p> <p>Mit Auswahl von <i>Angemeldet</i> ist die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

### 23.5.2 Allgemeine Einstellungen

Im Menü **Einstellungen->Allgemeine Einstellungen** werden die wichtigsten Einstellungen Ihres Benutzers aufgelistet. Die persönlichen Zugangsdaten (Konfigurationspasswort und Passwort für IP-Telefon) und Mobil- und Home-Office-Nummer können angepasst werden.

Das Menü besteht aus folgenden Feldern:

#### Felder im Menü Benutzerdaten

Feld	Beschreibung
<b>Name</b>	Zeigt den Namen Ihres Benutzers an.
<b>Beschreibung</b>	Zeigt die zusätzliche Beschreibung Ihres Benutzers an.

Feld	Beschreibung
<b>Benutzername</b>	Zeit Ihren Benutzernamen für das Login zur Benutzer-Konfigurationsoberfläche an.
<b>Passwort für HTML-Konfigurationszugriff</b>	Wenn Sie Ihr Passwort für den Zugang zur Benutzer-Konfigurationsoberfläche ändern wollen, geben Sie hier ein neues Passwort ein. Zur Überprüfung können Sie das Passwort durch Klicken der Option <b>Anzeigen</b> im Klartext anzeigen lassen.
<b>Passwort für IP-Telefonregistrierung</b>	Wenn Sie Ihr Passwort für die Registrierung eines IP-Telefons ändern wollen, geben Sie hier ein neues Passwort ein. Zur Überprüfung können Sie das Passwort durch Klicken der Option <b>Anzeigen</b> im Klartext anzeigen lassen.
<b>PIN für Zugang via Telefon</b>	Wenn Sie die PIN für Ihre persönliche Voice Box ändern wollen, geben Sie hier eine neue PIN ein. Zur Überprüfung können Sie das Passwort durch Klicken der Option <b>Anzeigen</b> im Klartext anzeigen lassen.
<b>Mobilnummer</b>	Hier können Sie Ihre Mobilfunknummer, unter der Sie erreichbar sein sollen, eingeben.
<b>Home-Office-Nummer</b>	Hier können Sie Ihre Home-Office-Nummer, unter der Sie erreichbar sein sollen, eingeben.
<b>Besetzt bei Besetzt (Busy on Busy)</b>	<p>Zeigt, ob für den aktuell gewählten Benutzer das Leistungsmerkmal Busy on Busy aktiviert ist.</p> <p>Führt ein Benutzer, für den mehrere Telefonnummern eingerichtet sind, ein Gespräch, so können Sie entscheiden, ob weitere Anrufe für diesen Benutzer signalisiert werden sollen. Ist die Funktion »Busy on Busy« für diesen Benutzer eingerichtet, so erhalten weitere Anrufer <b>Besetzt</b> signalisiert, wenn der Benutzer auf einer seiner Nummern telefoniert.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

#### Felder im Menü Statusinformationen

Feld	Beschreibung
<b>Teilnehmernummern</b>	Zeigt die internen Rufnummern an, die Ihnen zugewiesen wur-

Feld	Beschreibung
	den.
<b>Aktuelle Berechtigungsklasse</b>	Zeigt die Berechtigungsklasse an, der Sie aktuell zugewiesen sind.
<b>Wahlberechtigung</b>	Zeigt Ihre Wahlberechtigung an.
<b>Manuelle Bündelbelegung zulassen</b>	Zeigt an, ob Sie manuell weitere Bündel für Leitungen nach extern belegen dürfen und welche.
<b>Pick-Up-Gruppe</b>	Zeigt die Nummer der Gruppe an, in der Rufe herangeholt werden dürfen.

## Glossar

<b>2G</b>	Siehe GSM.
<b>3DES</b>	Siehe DES.
<b>3G</b>	Siehe UMTS.
<b>4G</b>	Siehe LTE.
<b>802.11</b>	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)
<b>A-Teilnehmer</b>	Der A-Teilnehmer ist der Anrufer.
<b>a/b-Schnittstelle</b>	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.
<b>Abwurf / Abwurf-funktion</b>	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.
<b>Access Client</b>	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.
<b>Access Point</b>	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).
<b>Accounting</b>	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.



<b>Analog</b>	Analoge Signale werden zur Datenübertragung eingesetzt. Im Gegensatz zu digitalen Signalen sind sie stör anfälliger.
<b>Analoge Endgeräte</b>	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.
<b>Anklopfen</b>	Anklopfen ist ein Leistungsmerkmal. Während eines Telefonats wird ein weiterer Anrufer signalisiert.
<b>Anklopf Sperre</b>	Bei aktiviertem Anklopfschutz wird ein weiterer Anrufer nicht am Endgerät signalisiert. Der Anrufer hört den Besetztton.
<b>Anlagenanschluss</b>	Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...) Siehe auch Mehrgeräteanschluss.
<b>Anlagenanschluss-Rufnummer</b>	Siehe Anlagenanschluss.
<b>Annex A</b>	Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.
<b>Annex B</b>	Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.
<b>Annex J</b>	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.
<b>Annex L</b>	Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrate vergrößert.
<b>Annex M</b>	Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.
<b>Anrufbeantworter</b>	Analoge Anrufbeantworter werden als analoges Endgerät konfigu-

riert und über den Endgerätetyp ausgewählt. Daneben dient das Voice Mail System der TK-Anlage als Anrufbeantworter.

<b>Anruferliste</b>	In Systemtelefonen werden entgangene Anrufe in einer Anruferliste gespeichert. Dazu muss die Übermittlung der Telefonnummer des Anrufers (CLIP) aktiviert sein.
<b>Anrufschutz</b>	Bei aktiviertem Anrufschutz ist die akustische Anrufsignalisierung ausgeschaltet. Diese Funktion wird auch als Ruhe vor dem Telefon bezeichnet.
<b>Anrufvariante</b>	Die Anrufvariante legt fest, an welchen Endgeräten ein Anruf signalisiert wird. Die einzelnen Anrufvarianten können über den Kalender zeitgesteuert umgeschaltet werden.
<b>Anrufweitschaltung</b>	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.
<b>ANSI T1.413</b>	ANSI T1.413 ist eine ADSL-Variante.
<b>ARP</b>	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.
<b>ARS</b>	Mithilfe der Automatic Route Selection (ARS) bestimmt die TK-Anlage die optimale Route zum angerufenen Teilnehmer, in Abhängigkeit von Provider, Dienst, QoS, ...
<b>ATM</b>	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.
<b>Authentifikation</b>	Überprüfung der Identität des Nutzers (Authentisierung).
<b>Automatische Amtsholung</b>	Bei automatischer Amtsholung kann sofort (ohne Eingabe einer Kennziffer) die Telefonnummer eines externen Gesprächspartners gewählt werden.
<b>Automatische Wahlwiederholung</b>	Ist der Anschluss der angerufenen Seite besetzt, kann eine automatische Wahlwiederholung eingeleitet werden. Diese informiert den

Anrufer sobald die Leitung frei ist.

<b>Automatischer Rückruf bei besetzt (CCBS)</b>	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.
<b>Automatischer Rückruf bei Nichtmelden (CCNR)</b>	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.
<b>Autorisierung</b>	Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
<b>AUX</b>	AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.
<b>B-Kanal</b>	Siehe Basisanschluss und Primärmultiplexanschluss.
<b>B-Teilnehmer</b>	Der B-Teilnehmer ist der angerufene Teilnehmer.
<b>Backbone Area</b>	Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.
<b>Basisanschluss</b>	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.
<b>Beacon</b>	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.
<b>Berechtigungsklasse</b>	Siehe CoS.
<b>Besetzt bei besetzt</b>	Siehe Busy on Busy.
<b>Bit</b>	Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.

<b>Black / White List</b>	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.)
<b>Blowfish</b>	Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.
<b>BootP</b>	Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.
<b>Bps</b>	Bits pro Sekunde. Ein Maßstab für die Übertragungsrates.
<b>BRI</b>	Siehe Basisanschluss.
<b>Bridge</b>	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.
<b>Broadcast</b>	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
<b>BRRP</b>	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.
<b>Bündel</b>	Die externen Anschlüsse einer Telefonanlage können zu Bündeln zusammengefasst werden.
<b>Busy On Busy</b>	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.
<b>CA</b>	Certificate Authority. Siehe Zertifikat.
<b>Cache</b>	Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.
<b>Call Deflection (CD)</b>	Siehe Rufumleitung.

<b>Call Through</b>	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.
<b>Callcenter</b>	Ein Callcenter bietet Beratung, Informationsaustausch und Verkauf über das Telefon.
<b>Called Party's Number</b>	Rufnummer des angerufenen Teilnehmers.
<b>Calling Party's Number</b>	Rufnummer des Anrufers.
<b>CAPI</b>	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.
<b>CAPWAP</b>	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.
<b>CAST</b>	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.
<b>CFB</b>	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).
<b>CFNR</b>	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).
<b>CHAP</b>	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.

<b>Cipher</b>	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.
<b>CLID</b>	Calling Line Identification (CLID), auch Caller ID, wird zur Authentifizierung verwendet. Ein Anrufer wird anhand seiner ISDN-Rufnummer erkannt, bevor die Verbindung aufgebaut wird.
<b>Client</b>	Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.
<b>CLIP</b>	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).
<b>CLIP no Screening</b>	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.
<b>CLIP off Hook</b>	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).
<b>CLIR</b>	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR).
<b>COLP</b>	Siehe Telefonnummer des Angerufenen anzeigen (COLP / COLR).
<b>COLP no Screening</b>	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.
<b>COLR</b>	Siehe Telefonnummer des Angerufenen anzeigen (COLP / COLR).
<b>CoS</b>	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).
<b>CRC</b>	Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.
<b>CRL</b>	Siehe Zertifikat.
<b>D-Kanal</b>	Siehe Basisanschluss und Primärmultiplexanschluss.
<b>Daemon</b>	Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.
<b>Datagramm</b>	Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.
<b>Datenkompression</b>	Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.
<b>DDI</b>	Direct Dial In (DDI) bedeutet Durchwahl. Siehe Anlagenanschluss und Durchwahl (VoIP).
<b>Dead Peer Detection</b>	In IPsec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.
<b>DECT</b>	Digital Enhanced Cordless Telecommunications (DECT) ist ein Standard für Schnurlostelefone sowie für kabellose Telefonanlagen.
<b>Default Gateway</b>	An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.
<b>Default Route</b>	Siehe Standardroute.
<b>Diffie-Hellman</b>	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.
<b>Denial-Of-Service Attack</b>	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.
<b>DES</b>	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).

<b>DFÜ</b>	DFÜ steht für Datenfernübertragung.
<b>DHCP</b>	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.
<b>Digital</b>	Digitale Signale werden zur Datenübertragung eingesetzt. Im Gegensatz zu analogen Signalen sind sie weniger stör anfällig.
<b>DIME</b>	Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.
<b>Direktruf</b>	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.
<b>DISA</b>	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.
<b>DNS</b>	Mithilfe des Domain Name System (DNS) wird der Domänenname (z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).
<b>Domäne</b>	Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).
<b>Downstream</b>	Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.
<b>Dreierkonferenz</b>	Die Dreierkonferenz ist ein Leistungsmerkmal. Drei Teilnehmer können gleichzeitig miteinander telefonieren.
<b>DSA</b>	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).

<b>Durchwahlnummer</b>	Siehe Anlagenanschluss und Durchwahl (VoIP).
<b>Dynamische IP-Adresse</b>	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.
<b>DynDNS</b>	Mithilfe eines DynDNS-Providers kann ein Domänenname auch mit einer dynamisch wechselnden IP-Adresse verknüpft werden.
<b>Einzelrufnummer (VoIP)</b>	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).
<b>Encapsulation</b>	Enkapsulierung (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.
<b>Encryption</b>	Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.
<b>ESP</b>	Encapsulating Security Payload (ESP) ist ein Protokoll für IPSec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.
<b>Ethernet</b>	Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.
<b>Euro-ISDN</b>	In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.
<b>Eurofile-Transfer</b>	EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.
<b>Fax</b>	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.
<b>Filter</b>	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>
<b>Filterregel</b>	<p>Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.</p>
<b>Firmware</b>	<p>Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts bereitgestellt.</p>
<b>Flash-Taste</b>	<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>
<b>Follow-me</b>	<p>Follow-me ist ein Leistungsmerkmal. Mit dieser Funktion können eingehende Anrufe einer anderen Nebenstelle zum eigenen Endgerät umgeleitet werden.</p>
<b>Fragmentierung</b>	<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>
<b>Frame</b>	<p>Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells</p>
<b>Frame Relay</b>	<p>Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.</p>
<b>Freisprechen</b>	<p>Beim Freisprechen kann man bei aufgelegtem Hörer telefonieren. Dabei können weitere Personen im Raum über Mikrofon und Lautsprecher am Gespräch teilnehmen.</p>
<b>FTP</b>	<p>Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.</p>
<b>Full-Duplex</b>	<p>Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.</p>
<b>Funktionstasten</b>	<p>Funktionstasten sind spezielle Tasten bei Systemtelefonen, die mit Telefonnummern oder Funktionen belegt werden können.</p>

<b>FXO</b>	Foreign Exchange Office (FXO) bezeichnet den Anschluss am analogen Endgerät. Siehe auch FXS.
<b>FXS</b>	Foreign Exchange Station (FXS) bezeichnet den analogen Anschluss an der Anschlussdose oder der Telefonanlage. Siehe auch FXO.
<b>G.711</b>	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 $\mu$ law-Quantisierungsverfahren verwendet.
<b>G.722</b>	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).
<b>G.726</b>	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
<b>G.729</b>	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).
<b>G.991.1</b>	Datenübertragungsempfehlung für HDSL.
<b>G.991.2</b>	Datenübertragungsempfehlung für SHDSL.
<b>G.992.1</b>	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)
<b>G.992.2</b>	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)
<b>G.992.3</b>	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.

<b>G.992.4</b>	Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)
<b>G.992.5</b>	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.
<b>G.993.1</b>	Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)
<b>G.993.2</b>	Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)
<b>G.DMT</b>	Siehe F.992.1.
<b>G.Lite</b>	Siehe F.992.2.
<b>G.SHDSL</b>	Siehe G.991.2.
<b>Gateway</b>	Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.
<b>GPRS</b>	General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.
<b>GRE</b>	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.
<b>GSM</b>	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.
<b>Half-Duplex</b>	Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.

<b>Halten</b>	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.
<b>Hash</b>	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).
<b>HDSL</b>	High Data Rate Digital Subscriber Line. Siehe DSL.
<b>Heartbeat</b>	Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.
<b>Heranholen von Rufen</b>	Siehe Pick-Up
<b>Hop</b>	Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.
<b>Host</b>	Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.
<b>Host-Name</b>	Domänenname eines Host. Siehe DNS.
<b>Hostroute</b>	Eine Hostroute bezeichnet die Route zu einem einzelnen Host.
<b>Hotspot</b>	Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.
<b>HSDPA</b>	High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.
<b>HTTP</b>	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.

<b>HTTPS</b>	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.
<b>Hyperchannel</b>	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.
<b>IAE</b>	IAE bezeichnet die standardisierte Steckdose (ISDN-Anschlusseinheit), an der ISDN-Endgeräte angeschlossen werden.
<b>ICMP</b>	Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.
<b>IGMP</b>	Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.
<b>IKE</b>	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.
<b>Impulswahlverfahren</b>	Das Impulswahlverfahren (IWW) ist ein Signalisierungsverfahren zur automatischen Telefonvermittlung. Tastatureingaben werden durch eine definierte Anzahl von Gleichstromimpulsen dargestellt. Siehe auch Mehrfrequenzwahlverfahren (MFV).
<b>Infrastruktur-Netzwerk</b>	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.
<b>Interne Telefonnummern</b>	Die internen Telefonnummern werden für Gespräche innerhalb der Telefonanlage verwendet.
<b>Internrufton</b>	Der Internrufton dient als besondere Signalisierung in Telefonanlagen zur Unterscheidung von Intern- und Externanrufen.

<b>IP</b>	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).
<b>IP-Adresse</b>	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 $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ 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.
<b>IPCP</b>	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.
<b>IPSec</b>	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.
<b>IPv6</b>	Siehe IP.
<b>ISDN</b>	Integrated Services Digital Network (ISDN) ist ein Datenübertragungsstandard, der Telefonie, Telefax und Datenübertragung umfasst. Es existieren zwei ISDN-Anschluss-Varianten: Basisanschluss und Primärmultiplexanschluss.
<b>ISDN-Adresse</b>	Die ISDN-Adresse eines ISDN-Geräts setzt sich zusammen aus einer ISDN-Nummer gefolgt von weiteren Ziffern, die sich auf das spezifische Endgerät beziehen.
<b>ISDN-BRI</b>	Siehe BRI.
<b>ISDN-Intern-/Extern</b>	Alternative Bezeichnung für den S0-Bus.



<b>ISDN-Login</b>	Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.
<b>ISDN-Nummer</b>	Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.
<b>ISDN-PRI</b>	Siehe PRI.
<b>ISDN-Router</b>	Siehe Router.
<b>ISP</b>	Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.
<b>ITU</b>	Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.
<b>IWV</b>	Siehe Impulswahlverfahren.
<b>Kanal</b>	Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.
<b>Kanalbündelung</b>	Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.
<b>Keepalive</b>	Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.
<b>Keepalive</b>	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.
<b>Kennzifferprozedur</b>	Über die Telefontastatur kann man eine Sequenz (Kennzifferprozedur) eingeben (bestehend aus 0 - 9, *, # und R), um Funktionen der Telefonanlage aufzurufen.
<b>Keypad</b>	Das Keypad-Protokoll (Netz-Direkt) wird zum Aufruf und zur Steuerung von Leistungsmerkmalen, die von der Vermittlungsstelle bereitgestellt werden, verwendet.
<b>Konferenzschaltung</b>	Bei einer Konferenzschaltung können mehrere interne Gesprächsteilnehmer gleichzeitig miteinander telefonieren.
<b>Konfiguration</b>	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.
<b>Lease Time</b>	Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.
<b>Leased Line</b>	Siehe Standleitung.
<b>LLC</b>	Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.
<b>LNS</b>	Siehe L2TP.
<b>Loopback</b>	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
<b>LTE</b>	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
<b>MAC-Adresse</b>	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
<b>Main Mode</b>	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.
<b>Makeln</b>	Makeln erlaubt es, zwischen zwei Gesprächspartnern hin und her zu schalten, ohne dass der wartende Teilnehmer mithören kann.
<b>Man-in-the-Middle Attack</b>	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.
<b>MD5</b>	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
<b>Media Gateway</b>	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.
<b>Mehrfachrufnummer (MSN)</b>	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
<b>Mehrfrequenzwahl-</b>	Das Mehrfrequenzwahlverfahren, auch als Tonwahlverfahren, MFV,

<b>verfahren</b>	MFC oder DTMF bezeichnet, ist ein Signalisierungsverfahren zur automatischen Telefonvermittlung. Tastatureingaben werden durch überlagerte, sinusförmige Signale dargestellt. Siehe auch Impulswahlverfahren (MFV).
<b>Mehrgeräteanschluss</b>	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.
<b>Metrik</b>	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).
<b>MFC</b>	Siehe Mehrfrequenzwahlverfahren.
<b>MFV</b>	Siehe Mehrfrequenzwahlverfahren.
<b>MIB</b>	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.
<b>MLP</b>	Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.
<b>Mobiler Teilnehmer</b>	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.
<b>Modem</b>	Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.
<b>MOH</b>	Siehe Music On Hold.
<b>MPDU</b>	Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.
<b>MPPC</b>	Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.

<b>MPPE</b>	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.
<b>MS-CHAP</b>	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).
<b>MSDU</b>	Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.
<b>MSN</b>	Siehe Mehrfachrufnummer.
<b>MSS</b>	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.
<b>MSS Clamping</b>	Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.
<b>MTU</b>	Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.
<b>Multicast</b>	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.
<b>Multilink</b>	Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, ...) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.
<b>Music On Hold</b>	Der Begriff Music On Hold (MOH) steht für automatische Ansagen oder Wartemusik über die Telefonanlage.
<b>MWI</b>	Über den Message Waiting Indicator (MWI) wird das Vorhandensein einer neuen Nachricht signalisiert.
<b>NAPT</b>	Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.

<b>NAT</b>	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.
<b>NBNS</b>	NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.
<b>Nebenstelle</b>	Eine Nebenstelle bezeichnet bei Telefonanlagen das mit der Anlage verbundene Endgerät.
<b>Netz-Direkt</b>	Siehe Keypad.
<b>Netzabschluss</b>	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.
<b>Netzmaske</b>	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.
<b>Netzwerkadresse</b>	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
<b>Netzwerkroute</b>	Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.
<b>NT</b>	Siehe Netzabschluss.
<b>NTBA</b>	Siehe Netzabschluss.
<b>NTP</b>	Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.
<b>NTPMGF</b>	Siehe Netzabschluss.
<b>Nutzkanal</b>	Siehe B-Kanal.

<b>OAM</b>	OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.
<b>Offene Rückfrage</b>	Bei der offenen Rückfrage wird ein Gespräch in einen Wartezustand versetzt und kann von jedem Teilnehmer wieder angenommen werden.
<b>OSI-Modell</b>	Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.
<b>OSPF</b>	OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.
<b>PABX</b>	Private Automatic Branch Exchange (PABX) ist eine andere Bezeichnung für eine Telefonanlage.
<b>PAP</b>	Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.
<b>Parallelruf</b>	Siehe Mobiler Teilnehmer.
<b>Parken</b>	Beim Parken wird eine Telefonverbindung gehalten, selbst wenn beim beteiligten Endgerät der Hörer aufgelegt oder die Kabelverbindung getrennt ist.
<b>PAT</b>	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.
<b>PBX</b>	Private Branch Exchange (PBX) ist eine andere Bezeichnung für eine Telefonanlage.
<b>Peer</b>	Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.
<b>Phase-1/2</b>	Siehe IKE.
<b>Pick-Up</b>	Bei Pick-Up werden Anrufe über Kennzifferprozeduren an einem internen Endgerät entgegengenommen, das sich nicht in der aktiven Rufverteilung befindet.
<b>PIM</b>	Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.

<b>PIN</b>	Mithilfe einer persönlichen Identifikationsnummer (PIN) kann man sich am Gerät authentisieren und dadurch Funktionen des Geräts nutzen.
<b>Ping</b>	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.
<b>PKCS</b>	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.
<b>PKI</b>	Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.
<b>PMTU</b>	Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.
<b>Point-to-Multipoint</b>	Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).
<b>Point-to-Point</b>	Siehe Anlagenanschluss und Durchwahl (VoIP).
<b>Pool</b>	Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.
<b>POP3</b>	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.
<b>Port</b>	Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, ...) ein ankommendes Datenpaket weitergeleitet wird.
<b>POTS</b>	Plain Old Telephone System (POTS) bezeichnet das analoge Telefonnetz.
<b>PPP</b>	Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.



<b>PPPoA</b>	Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.
<b>PPPoE</b>	Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.
<b>PPTP</b>	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.
<b>Präfix</b>	Siehe Netzwerkadresse.
<b>Präfixdelegation</b>	In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.
<b>Präfixlänge</b>	Siehe Netzmaske.
<b>Preshared Key</b>	Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.
<b>PRI</b>	Siehe Primärmultiplexanschluss.
<b>Primärmultiplexanschluss</b>	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.
<b>Proposal</b>	Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.
<b>Protokoll</b>	Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP

<b>Proxy</b>	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.
<b>PVID</b>	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.
<b>Q-SIG</b>	Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.
<b>QoS</b>	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.
<b>Queue</b>	In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.
<b>RADIUS</b>	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+.
<b>Raumüberwachung</b>	Die Raumüberwachung ist ein Leistungsmerkmal. Die Geräusche eines Zimmers können mitgehört werden.
<b>RE-ADSL2</b>	Siehe G.992.5.
<b>Real Time Jitter Control</b>	Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.
<b>Regelkette</b>	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.
<b>Registrar</b>	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.

<b>Repeater</b>	Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.
<b>Reset</b>	Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.
<b>RFC</b>	Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.
<b>Rijndael</b>	Siehe AES.
<b>RIP</b>	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.
<b>RipeMD 160</b>	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
<b>RJ45</b>	RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.
<b>Roaming</b>	Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.
<b>Router</b>	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.
<b>Router Advertisement</b>	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.
<b>Routing</b>	Routing bezeichnet das Festlegen von Wegen für die Nachrichtenübermittlung.
<b>RSA</b>	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.
<b>RTP</b>	Mit dem Real-Time Transport Protocol (RTP) werden Audio- und Video-Daten (Streams) über IP-basierte Netzwerke übertragen.
<b>RTS Threshold</b>	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.
<b>RTSP</b>	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.
<b>Rückfrage</b>	Bei der Rückfrage wird das Telefongespräch mit dem ersten Gesprächspartner gehalten, während man ein zweites Gespräch führt.
<b>Rückruf bei besetzt</b>	Siehe automatischer Rückruf bei besetzt (CCBS).
<b>Rückruf bei Nicht-melden</b>	Siehe automatischer Rückruf bei Nichtmelden (CCNR).
<b>Rufnummernband</b>	Siehe Rufnummernblock beim Anlagenanschluss.
<b>Rufnummernblock</b>	Siehe Anlagenanschluss und Durchwahl (VoIP).
<b>Rufumleitung</b>	Rufumleitung (Call Deflection, CD) ist ein Leistungsmerkmal. Ein Anruf kann weitergeleitet werden, ohne ihn vorher angenommen zu haben.
<b>Rufverteilung</b>	Bei der Rufverteilung in der Telefonanlage werden eingehende Telefongespräche bestimmten Rufnummern oder Anwendungen (Fernzugang, ISDN-Login, ...) zugeordnet.
<b>Ruhe vor dem Telefon</b>	Siehe Anrufschutz.
<b>S0-Bus</b>	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.
<b>S2M-Anschluss</b>	Siehe Primärmultiplexanschluss.
<b>SA</b>	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.

<b>Shorthold</b>	Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.
<b>SIF</b>	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.
<b>SIP</b>	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.
<b>SIP-Provider</b>	Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.
<b>SMTP</b>	Das Simple Mail Transfer Protocol (SMTP) wird zum Austausch von E-Mails eingesetzt.
<b>SNMP</b>	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.
<b>SNTP</b>	Das Simple Network Time Protocol (SNTP) wird zur Zeitübertragung und Synchronisation zwischen Server und Client eingesetzt.
<b>Softkey</b>	Als Softkey bezeichnet man eine Taste, deren Funktion von der zugehörigen Bildschirmanzeige bestimmt wird.
<b>Spatial Streams</b>	Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der Übertragungsrates.
<b>SPD</b>	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.
<b>STUN-Server</b>	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.
<b>Subadressierung</b>	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.
<b>Subnetz</b>	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).
<b>Switch</b>	Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerkkomponenten miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells betrieben werden. Das dem Switch vergleichbare Gerät der Bitübertragungsschicht wird als Hub bezeichnet.
<b>SWYX</b>	SwyxWare ist eine softwarebasierte Kommunikationslösung für VoIP.
<b>Syslog</b>	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.
<b>Systemtelefon</b>	Ein Systemtelefon ist mit mehreren Funktions- und Sondertasten ausgestattet und kann die Leistungsmerkmale einer Telefonanlage nutzen.
<b>T.38</b>	T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.



<b>TA</b>	Siehe Terminaladapter.
<b>TACACS+</b>	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.
<b>TAE</b>	Siehe Netzabschluss. Man unterscheidet zwischen F-codierten Steckverbindern für Telefone und N-codierten Steckverbindern für Faxgeräte, Modems und Anrufbeantworter.
<b>TAPI</b>	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.
<b>TCP</b>	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.
<b>TCP-ACK-Paket</b>	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.
<b>TE</b>	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.
<b>TEI</b>	Der Terminal Endpoint Identifier (TEI) ist gemäß ISDN-Protokoll DSS1 eine Kennung zur Identifizierung der Endgeräte.
<b>Telefax</b>	Siehe Fax.
<b>Telefonnummer des Angerufenen anzeigen</b>	Mithilfe von Connected Line Identification Presentation (COLP) wird die Telefonnummer des Angerufenen (B-Telefonnummer) zum An-

<b>gen (COLP / COLR)</b>	rufers übertragen. Mithilfe von Connected Line Identification Restriction (COLR) wird die Übertragung der Telefonnummer des Angerufenen zum Anrufer unterdrückt.
<b>Telefonnummer des Anrufers anzeigen (CLIP / CLIR)</b>	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.
<b>Telefonnummer unterdrücken</b>	Siehe Telefonnummer des Anrufers anzeigen (CLIP / CLIR) und Telefonnummer des Angerufenen anzeigen (COLP / COLR).
<b>Telnet</b>	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
<b>Terminaladapter</b>	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.
<b>TFE</b>	Eine Türfreisprecheinrichtung (TFE) ist an Eingängen montiert und ein Teil eines Türsprechsystems, z. B. einer Telefonanlage.
<b>TFTP</b>	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.
<b>Tiger 192</b>	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
<b>Time Service</b>	Mithilfe des Time Protocol (time) wird Datum und Uhrzeit synchronisiert. Das Protokoll verwendet den Port 37 über TCP und UDP.
<b>TK-Anlage</b>	TK-Anlage ist eine andere Bezeichnung für eine Telefonanlage.
<b>TLS</b>	Siehe SSL.
<b>Tonwahl</b>	Siehe Mehrfrequenzwahlverfahren.
<b>TOS</b>	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
<b>Traceroute</b>	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpa-

kete bis zum abgefragten Ziel-Host vermittelt werden.

<b>Trigger</b>	Unter Trigger versteht man einen Auslöseimpuls.
<b>Triple DES</b>	Siehe DES.
<b>Trunk</b>	Ein Trunk sind gebündelte Anschlüsse bzw. Übertragungskanäle. Siehe auch Bündel.
<b>TTL</b>	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.
<b>Twofish</b>	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128,192 oder 256 Bit.
<b>U-ADSL</b>	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.
<b>Überprüfung der Rückroute</b>	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.
<b>UDP</b>	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.
<b>ULA</b>	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.
<b>UMTS</b>	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+.

<b>Unicast</b>	Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertragen.
<b>UP0</b>	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.
<b>UPnP</b>	Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.
<b>Upstream</b>	Das Gateway leitet die Daten des eigenen Netzwerks weiter.
<b>URL</b>	Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: <a href="http://www.example.org/index.htm">http://www.example.org/index.htm</a> (Web-Seite im Internet)
<b>UUS</b>	Bei User to User Signalling (USS) können Textnachrichten mit anderen Teilnehmern ausgetauscht werden.
<b>V.110</b>	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.
<b>VDSL</b>	Very High Speed Digital Subscriber Line. Siehe DSL.
<b>VID</b>	Siehe VLAN.
<b>VLAN</b>	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.
<b>Voice Mail Box</b>	Eine Voice Mail Box ist der persönliche Anrufbeantworter eines Benutzers in einem Voice Mail System.
<b>Voice Mail System</b>	Ein Voice Mail System ermöglicht das Speichern, Abrufen und Weiterleiten von Sprachmitteilungen ähnlich wie ein Anrufbeantworter, jedoch mit weitaus mehr Optionen.
<b>VoIP</b>	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.

<b>VPN</b>	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.
<b>VSS</b>	Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.
<b>Wahlberechtigung</b>	Siehe Amtsberechtigung.
<b>Wahlkontrolle</b>	Siehe Black / White List.
<b>Wahlregeln</b>	Mithilfe der Wahlregeln können Anrufe abhängig von der gewählten Rufnummer (Zone) über festgelegte Provider bzw. Bündel geleitet werden.
<b>Wählverbindung</b>	Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.
<b>Wahlvorbereitung</b>	Die Wahlvorbereitung beschreibt die Eingabe der Telefonnummer vor dem Einleiten des Gesprächs, z. B. durch Abheben des Hörers.
<b>Walled Garden</b>	Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.
<b>WAN</b>	Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausge dehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.
<b>Wartemusik</b>	Siehe Music On Hold.
<b>WDS</b>	Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.
<b>Web-Server</b>	Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.
<b>Wechselsprechen</b>	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.

<b>WEP</b>	Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.
<b>WINS</b>	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.
<b>WLAN</b>	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.
<b>WMM</b>	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.
<b>WPA</b>	Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.
<b>WPA - Enterprise</b>	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.
<b>WPA - PSK</b>	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.
<b>WPA 2</b>	Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.
<b>X.25</b>	X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.
<b>X.31</b>	Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.
<b>X.500</b>	Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.
<b>X.509</b>	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

- EID Präfix aus dem Adressbaum ausschließen 330
- MTU der LISP-Schnittstelle 332
- Abfrage Intervall 243
- Address assignment 391
- Admin-Status 212
- Administrative FQDNs 394
- Administrativer Status 288 , 367
- Adressbereich 354
- Adresse/Präfix 354
- Adresse/Subnetz 354
- Adressen 107
- Adressmodus 129 , 276
- Adresstyp 354
- AFTR 258
- Ähnliches Zertifikat überschreiben 405
- Airtime Fairness 161
- Aktion 199 , 237 , 346 , 348 , 405 , 437
- Aktive Funktion 475 , 476 , 476 , 477
- Aktiver Allgemeiner Präfix 195
- Aktives Funkmodulprofil 158
- Aktives Funkmodulprofil 155
- Aktualisierung aktivieren 375
- Aktualisierungsintervall 378
- Aktualisierungspfad 378
- Alle Multicast-Gruppen 246
- Allgemeiner Name 81
- Allgemeiner Präfix 133 , 254 , 268
- Ankommende Rufnummer 303
- Ankündigen 133
- Anmeldefenster 431
- Anmeldung eines Proxys erlauben 98
- Anrufschutz 477
- Anschlussart 95
- Antwort 369
- Antwortintervall (Letztes Mitglied) 243
- Anzahl der zulässigen gleichzeitigen Gespräche 98
- Anzahl der Spatial Streams 161
- Anzahl erlaubter Verbindungen 296
- Anzahl Nachrichten 454
- APN 383
- Art der Anrufweitschaltung 116
- Art der Einrichtung 133 , 254 , 268
- Art des Datenverkehrs 198
- ATM PVC 264
- ATM-Dienstkategorie 279
- ATM-Schnittstelle 274
- Aufzurufende Seite nach Login 430
- Ausgehende Rufnummer 303
- Ausgehende Schnittstelle 228
- Ausstehende Ende-  
zu-Ende-Anforderungen 282
- Ausstehende Segment-Anforderungen 282
- Auswahl 355
- Auswahl des Client-Bands 171
- Auszuführende Aktion 421
- Authentifizierung 256 , 262 , 270 , 339
- Authentifizierungs-ID 95
- Authentifizierungsmethode 288 , 305
- Authentifizierungstyp 71
- Automatische Subnetzerstellung 133 , 254 , 268
- Autonomous Flag 135
- Autospeichermodus 82
- Autospeichermodus 405
- Bandbreite 161
- Bandbreitenbegrenzung Downstream 107
- Bandbreitenbegrenzung Upstream 107
- Basierend auf Ethernet-Schnittstelle 128
- Basisnetz (SSID) 167
- Beacon Period 163
- Bedingung des Schnittstellenverkehrs 398
- Bedingung für Ereignisliste 405
- Befehlsmodus 405
- Befehlstyp 405
- Beinhalteter Standort (Parent) 107



- Benachrichtigungsdienst 454
- Benutzer 319
- Benutzerdefiniert 81
- Benutzerdefinierte DHCP-Optionen 384
- Benutzerdefinierter Kanalplan 163
- Benutzername 95 , 249 , 259 , 264 , 337 , 375 , 396
- Benutzter Präfix/Länge 195
- Berichtsmethode 239
- Berücksichtigen 208
- Beschreibung 76 , 85 , 95 , 107 , 110 , 155 , 158 , 160 , 187 , 198 , 212 , 218 , 221 , 228 , 233 , 237 , 249 , 258 , 259 , 264 , 274 , 288 , 295 , 305 , 313 , 319 , 332 , 334 , 337 , 352 , 353 , 354 , 355 , 356 , 358 , 367 , 381 , 386 , 398 , 405 , 433 , 437 , 471 , 478
- Beschreibung 190
- Betreff 454
- Betreibermodus 71
- Betriebsmodus 155
- Betriebsmodus 158 , 160
- Bevorzugte Gültigkeitsdauer 135
- Blockieren nach Verbindungsfehler für 256 , 262 , 270 , 339
- Blockzeit 310
- Burst-Größe 228
- Burst-Mode 161
- CA-Name 405
- CA-Zertifikat 78
- CA-Zertifikate 310
- CAPWAP-Verschlüsselung 158
- Client FQDN akzeptieren 394
- Client-Typ 278
- Code 356
- Codec-Profil 98 , 105
- Codec-Reihenfolge 110
- Continuity Check (CC) Ende-zu-Ende 283
- Continuity Check (CC) Segment 283
- COS-Filter (802.1p/Layer 2) 218 , 233 , 433
- CRL verwenden 405
- CSV-Dateiformat 405
- Dateikodierung 83 , 84
- Dateiname 405
- Dateiname auf Server 405
- Dateiname in Flash 405
- DH-Gruppe 305
- DHCP Broadcast Flag 136
- DHCP-Client 130
- DHCP-Client 252 , 266
- DHCP-Hostname 136 , 276
- DHCP-MAC-Adresse 136 , 276
- DHCP-Modus 137
- DHCP-Optionen 382
- DHCP-Server 130 , 151
- Dienst 199 , 212 , 218 , 233 , 346 , 348 , 433
- DNS-Aushandlung 256 , 262 , 270 , 341
- DNS-Domänen-Suchliste 392
- DNS-Hostname 369
- DNS-Propagation 137
- DNS-Server 272 , 320 , 380 , 392
- Domäne 371
- Domäne / Realm 95
- Domäne am Hotspot-Server 430
- Drahtloser Modus 161
- Dropping-Algorithmus 230
- DSCP / Traffic Class Filter (Layer 3) 218 , 233 , 433
- DSCP/TOS-Wert 187
- DSCP-Einstellungen für RTP-Daten 108
- DSCP/Traffic-Class-Filter setzen (Layer 3) 221
- DTIM Period 163
- DTMF 110
- DUID 394
- Durchsatz 177
- Durchsatz/Client 177
- Dynamische Black List 172
- E-Mail 81
- EAP-Vorabauthentifizierung 167
- Early-Media-Unterstützung 98

- EID-Präfix (IP-Adresse / Länge) 331
- EID-Prefix (IP-Adresse / Länge) 330
- Eigene IP-Adresse per ISDN/GSM übertragen 303
- Eintrag aktiv 71
- Empfänger 454
- Ende-zu-Ende-Sendeintervall 282
- Enkapsulierung 274
- Entfernte PPTP-IP-Adresse 262
- Entfernte IP-Adresse 335
- Entfernter Hostname 334
- Entferntes IPv6-Netzwerk 293
- Enthaltene Zeichenfolge 454
- Ereignis 454
- Ereignisliste 398 , 405
- Ereignistyp 398
- Erfolgreiche Versuche 398 , 421
- Erlaubte Adressen 172
- Erreichbarkeitsprüfung 73 , 310 , 316
- Ersetzen des Präfix der eingehenden Nummer 98
- Ersetzen des internationalen Präfix durch "+" 98
- Erzeugungsmethode 134 , 255 , 269
- Externe Rufnummer 476
- Externer Dateiname 83 , 84
- Facility 451
- Fallback-Proxy-Schnittstelle 1 244
- Fallback-Proxy-Schnittstelle 2 244
- Fehlgeschlagene Versuche 398 , 421
- Fehlversuche per Zeitraum 172
- Feste Rufnummer für ausgehende Gespräche anzeigen 96
- Filter 221
- Fragmentation Threshold 163
- Freigegebene Rufnummer 118
- Frequenzband 160
- From Domain 98
- G.711 aLaw 110
- G.711 uLaw 110
- G.722 110
- G.726 Codec-Einstellungen 110
- G.726 (16 Kbit/s) 110
- G.726 (24 Kbit/s) 110
- G.726 (32 Kbit/s) 110
- G.726 (40 Kbit/s) 110
- G.729 110
- Gateway 382
- Gateway-Adresse 190
- Gateway-IP-Adresse 186
- Gehende Rufnummer 96
- GEO Zone Status 398
- Gerät 158
- Geräte pro Ticket 431
- Geschäftsbedingungen 430
- Geschwindigkeitsprofil im 2,4-GHz-Band 174
- Geschwindigkeitsprofil im 5-GHz-Band 174
- Gespernte Rufnummer 118
- Gewichtung 228
- Globale Rufnummer für CLIP-No-Screening 96
- Größe des Protokoll-Headers unterhalb Layer 3 224
- Gruppen-ID 421
- Gruppenbeschreibung 71 , 208 , 209
- Gültigkeitsdauer 135
- Halten im System 98
- Hello-Intervall 336
- Hersteller auswählen 383 , 384
- Hersteller-ID 383 , 384
- Herstellerbeschreibung 383 , 384
- Herstellerspezifische Informationen 383
- Herstellerspezifische Informationen (DHCP-Option 43) 382
- High-Priority-Klasse 221
- Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable 405
- HMAC Truncation 328
- Host 371
- Hostname 375
- ID 331
- IGMP Proxy 244
- IGMP Snooping 166
- IKE (Internet Key Exchange) 288
- Immer aktiv 249 , 259 , 264 , 337

- Indexvariablen 398 , 405
- Instanz-ID 330 , 332
- Internationale Rufnummer erzeugen 98
- Interne Rufnummer 116
- Intervall 398 , 405 , 421 , 424
- Intra-cell Repeating 166
- IP-Adressbereich 151 , 272 , 320 , 380
- IP-Adresse 276 , 277 , 386 , 451 , 460
- IP-Adresse / Netzmaske 129
- IP-Adresse des Map-Server 327
- IP-Adresse des Routing Locator (RLOC) 330
- IP-Adresse zur Nachverfolgung 209
- IP-Adresse/Netzmaske 151 , 155
- IP-Adressmodus 251 , 260 , 265 , 338
- IP-Komprimierung 316
- IP-Poolname 272 , 320 , 380 , 381
- IP-Version 355
- IP-Version 367
- IP-Version des Tunnelnetzwerks 288
- IP-Zuordnungspool 290
- IP-Zuordnungspool (IPCP) 338
- IPv4 354
- IPv4 Proxy ARP 298
- IPv4-Adresse 369
- IPv4-Adressvergabe 290
- IPv4-Quelladresse/-netzmaske 218 , 233 , 433
- IPv4-Zieladresse/-netzmaske 218 , 233 , 433
- IPv6 130 , 252 , 266 , 354
- IPv6-Adresse 369
- IPv6-Adressen 130 , 252 , 266
- IPv6-Modus 130 , 252 , 266
- IPv6-Quelladresse/-länge 218 , 233 , 433
- IPv6-Schnittstelle 258
- IPv6-Zieladresse/-länge 218 , 233 , 433
- Kanal 158
- Kanalplan 163
- Kennung der statischen Schnittstelle 394
- Kennwort für geschütztes Zertifikat 405
- Klassen-ID 221 , 228
- Klassenplan 221
- Konfiguration verschlüsseln 405
- Konfiguration enthält Zertifikate/Schlüssel 405
- Konfigurationsmodus 290
- Kontrollmodus 224 , 285
- Land 81
- Layer 4-Protokoll 187
- LCP-Erreichbarkeitsprüfung 256 , 262 , 270 , 339
- LDAP-URL-Pfad 85
- Lease Time 382
- Lebensdauer 305 , 313
- Lebensdauer des Datenbankeintrags (in Min.) 330
- Level 451
- Link-Präfix 133 , 254 , 268
- Lizenzschlüssel 55
- Lizenzseriennummer 55
- Lokale Zertifikatsbeschreibung 83 , 84 , 405
- Lokale ID 288
- Lokale IP-Adresse 186 , 251 , 260 , 265 , 290 , 336 , 338
- Lokale PPTP-IP-Adresse 262
- Lokale WLAN-SSID 405
- Lokaler Dateiname 405
- Lokaler Hostname 334
- Lokaler ID-Typ 288 , 305
- Lokaler ID-Wert 305
- Lokales IPv6-Netzwerk 293
- Lokales Zertifikat 305
- Long Retry Limit 163
- Loopback Ende-zu-Ende 282
- Loopback-Segment 282
- MAC-Adresse 128 , 155 , 276 , 386
- Mail-Exchanger (MX) 377
- Map-Register-Dauer (in Sek.) 328
- Max. Anzahl ausstehender Map-

- Requests 329
- Max. Anzahl Clients - Hard Limit 171
- Max. Anzahl Clients - Soft Limit 171
- Max. Queue-Größe 230
- Max. Übertragungsrate 163
- Max. Verzögerung vor dem Umschalten zum nächster 329
- Maximale Downstream-Bandbreite 107
- Maximale Upload-Geschwindigkeit 224 , 228 , 285
- Maximale Upstream-Bandbreite 107
- Maximale Antwortzeit 243
- Maximale Anzahl der erneuten Einwählversuche 256 , 262 , 270
- Maximale Anzahl Wiederholungen 336
- Maximale Anzahl der IGMP-Statusmeldungen 243
- Maximale Anzahl der EID/RLOC-Einträge im Cache 332
- Maximale Anzahl von RLOC-Adressen pro EID/RLOC-Eintrag 332
- Maximale Burst-Größe (MBS) 279
- Maximale Zeit zwischen Versuchen 336
- Metrik 186 , 190 , 290
- MIB-Variablen 405
- Min. Queue-Größe 230
- Minimale Map-Request-Dauer (in Sek.) 329
- Minimale Zeit zwischen Versuchen 336
- Mitglieder 352 , 353 , 358
- MobiKE 298
- Modus 78 , 187 , 243 , 303 , 305 , 319
- Modus des D-Kanals 303
- Monitored GEO Zone 398
- MTU 258
- Multicast-Gruppen-Adresse 246
- Nach Ausführung neu starten 405
- Nachrichtenkompromierung 454
- Nachrichtentyp 451
- Name 158 , 195 , 319 , 391
- NAT-Eintrag erstellen 251 , 260 , 265 , 338
- NAT-Methode 198
- NAT-Traversal 310
- Nationale Rufnummer erzeugen 98
- Netzmaske 276 , 277
- Netzwerkname (SSID) 166
- Neue Quell-IP-Adresse/Netzmaske 203
- Neue Ziel-IP-Adresse/Netzmaske 203
- Neuer Quell-Port 203
- Neuer Ziel-Port 203
- Neustart des Geräts nach 405
- Nummernunterdrückung deaktivieren 98
- OAM-Fluss-Level 281
- Öffentliche IPv4-Quelladresse 298
- Öffentliche IPv6-Quelladresse 298
- Öffentliche Schnittstelle 298
- Öffentlicher Schnittstellenmodus 298
- On Link Flag 135
- Organisation 81
- Organisationseinheit 81
- Original Quell-Port/Bereich 199
- Original Ziel-IP-Adresse/Netzmaske 199
- Original Ziel-Port/Bereich 199
- Originale Quell-IP-Adresse/Netzmaske 199
- Ort 81
- OSPF-Modus 341
- Passwort 78 , 83 , 84 , 95 , 249 , 259 , 264 , 319 , 334 , 337 , 375 , 396 , 405 , 437
- Peak Cell Rate (PCR) 279
- Peer-Adresse 288
- Peer-ID 288
- PFS-Gruppe verwenden 313
- Phase-1-Profil 296
- Phase-2-Profil 296
- PIN 383
- PMTU propagieren 316
- Pool-Verwendung 381

- Pop-Up-Fenster für Statusanzeige 431
- Port 378
- Port Proxy 98
- Port Registrar 96
- Port-STUN-Server 97
- PPPoE-Ethernet-Schnittstelle 249
- PPPoE-Modus 249
- PPPoE-Schnittstelle für Mehrfachlink 249
- PPTP-Adressmodus 262
- PPTP-Ethernet-Schnittstelle 259
- Preshared Key 167 , 288
- Primärer IPv4-DNS-Server 367
- Primärer IPv6-DNS-Server 367
- Primärer DNS-Server (IPv4/IPv6) 371
- Priorisierungsalgorithmus 224
- Priorität 71 , 228 , 367
- Priority Queueing 228
- Privaten Schlüssel generieren 78
- Proposals 305 , 313
- Protokoll 199 , 212 , 218 , 233 , 295 , 356 , 378 , 405 , 433 , 451
- Provider 274 , 375
- Provider ohne Registrierung 98
- Provider-Status 95
- Providename 378
- Provisioning-Server 384
- Proxy 98
- Proxy ARP 136
- Proxy-ARP-Modus 341
- Proxy-ETR-RLOC 332
- Proxy-Schnittstelle 244
- Quell-IP-Adresse 398 , 405
- Quell-IP-Adresse 421 , 424
- Quell-IP-Adresse/Netzmaske 187 , 199 , 212 , 295
- Quell-Port 187 , 295
- Quell-Port/Bereich 199 , 212 , 218 , 233 , 433
- Quelladresse/Länge 190
- Quelle 346 , 348 , 405
- Quellportbereich 356
- Quellschnittstelle 187 , 212 , 246 , 371
- Queues/Richtlinien 227
- RA-Signierungszertifikat 78
- RA-Verschlüsselungszertifikat 78
- RADIUS-Dialout 73
- RADIUS-Passwort 71
- RADIUS-Server 167
- RADIUS-Server Gruppen-ID 319
- Real Time Jitter Control 224
- Regelkette 237 , 239 , 439
- Registrar 96
- Registrierungstimer 97
- Richtlinie 73
- Richtung 221
- Richtung des Datenverkehrs 398
- Robustheit 243
- Rolle 319
- Route aktiv 190
- Routeneinträge 251 , 260 , 265 , 290 , 338
- Routenklasse 184
- Routenselektor 209
- Routentyp 184 , 190
- Router Advertisement annehmen 130 , 252 , 266
- Router-Gültigkeitsdauer 137
- Router-Präferenz 137
- RSSI-Schwellwert 175
- RTS Threshold 163
- RTT-Modus (Realtime-Traffic-Modus) 228
- Rufnummer (MSN) 476
- Rufnummer des entfernten Gesprächspartners anzeigen 96
- Rx Shaping 174
- SCEP-Server-URL 405
- SCEP-URL 78
- Schlüssel zur Authentisierung 327
- Schlüsselgröße 405
- Schlüsseltyp (HMAC-Algorithmus) 327
- Schnittstelle 61 , 61 , 64 , 184 , 198 , 209 , 224 , 239 , 243 , 285 , 367 , 375 , 381 , 391 , 405 , 423 , 430 ,

- 439
- Schnittstellen 107 , 221
- Schnittstellenaktion 423
- Schnittstellenbindung 330
- Schnittstellenmodus 128 , 367
- Schnittstellenstatus 398
- Schnittstellenstatus festlegen 405
- Schweregrad 454
- Segment-Sendeintervall 282
- Sekundärer IPv4-DNS-Server 367
- Sekundärer IPv6-DNS-Server 367
- Sekundärer DNS-Server (IPv4/IPv6)  
371
- Sende WOL-Paket über Schnittstelle  
437
- Sendeleistung 158
- Sequenznummern der Datenpakete  
336
- Server 378
- Server Timeout 73
- Server-IP-Adresse 71
- Server-URL 405
- Serveradresse 405
- Setze COS Wert (802.1p/Layer 2)  
221
- Short Guard Interval 163
- Short Retry Limit 163
- Sicherheitsmodus 167
- Sicherheitsrichtlinie 129 , 130 , 251 ,  
252 , 260 , 265 , 266 , 290 , 293
- SIP Update senden 98
- SIP-Bindungen nach Neustart löschen  
98
- SNTP-Server 392
- Special Handling Timer 212
- Sperrzeit für Black List 172
- Sprache für Anmeldefenster 430
- SRTP 105
- Staat/Provinz 81
- Standard TTL eines EID/  
RLOC-Eintragsim Cache (in Min.)  
332
- Standard TTL-Modus 332
- Standard-Benutzerpasswort 71
- Standard-Ethernet für PPPoE-  
Schnittstellen 276
- Standard-Timeout bei Inaktivität 431
- Standardroute 258
- Standardroute 251 , 260 , 265 , 290 ,  
338
- Standardroute erstellen 136
- Standort 98 , 155 , 158
- Startmodus 296
- Startzeit 403
- Statische Adressen 134 , 255 , 269
- Status 398 , 478
- Status der Funktionstaste 398
- Status des Auslösers 405
- Status festlegen 405
- Stoppzeit 403
- STUN-Server 97
- Subjektnamen 405
- Subnetz-ID 133 , 254 , 268
- Sustained Cell Rate (SCR) 279
- T.38 FAX Unterstützung 98
- TCP-ACK-Pakete priorisieren 256 ,  
262 , 270 , 277 , 339
- TCP-MSS-Clamping 136
- Telefonnummer 471
- Tickettyp 431
- Timeout bei Inaktivität 249 , 259 , 264  
, 337
- Timeout für Nachrichten 454
- Toleranzzeit 175
- Traffic Shaping 228
- Traffic Shaping 224
- Transparente MAC-Adresse 61
- Transportprotokoll 96 , 98
- Trigger 423
- Tunnelprofil 337
- Tx Shaping 174
- Typ 107 , 195 , 218 , 233 , 274 , 356 ,  
433 , 437 , 475
- U-APSD 166
- Überbuchen zugelassen 228
- Überprüfung anhand einer Zertifi-  
katsperlliste (CRL) 76
- Überprüfung der IPv4-Rückroute 298

- Übertragener Datenverkehr 398
- Übertragungsmodus 303
- Übertragungsschlüssel 167
- Überwachte Schnittstelle 398
- Überwachte Subsysteme 454
- Überwachte Variable 398
- Überwachte IP-Adresse 421
- Überwachte Schnittstelle 423
- Überwachtes Zertifikat 398
- UDP-Port 73
- UDP-Quellport 335
- UDP-Zielpport 335
- Unveränderliche Parameter 214
- Verbindungsstatus 218 , 233 , 433
- Verbindungstyp 337
- Verbleibende Gültigkeitsdauer 398
- Verbundene Clients 177
- Vergleichsbedingung 398
- Vergleichswert 398
- Vermeidung von Datenstau (RED) 230
- Verschlüsselung 339
- Verschlüsselungsmethode 224
- Versionsprüfung 405
- Versuche 405 , 424
- Verteilungsmodus 208
- Verteilungsrichtlinie 208 , 209
- Verteilungsverhältnis 209
- Vertrauenswürdigkeit des Zertifikats erzwingen 76
- Verwendeter Kanal 158
- Verwerfen ohne Rückmeldung 239
- Video 105
- Virtual Channel Connection (VCC) 279 , 281
- Virtual Channel Identifier (VCI) 274
- Virtual Path Connection (VPC) 281
- Virtual Path Identifier (VPI) 274
- VLAN 173 , 249
- VLAN Identifier 140
- VLAN-ID 128 , 151 , 173 , 249
- VLAN-Mitglieder 140
- VLAN-Name 140
- Von Schnittstelle 195
- Vorgeschaltetes Gerät mit NAT 98
- Wahlendeüberwachungstimer 98
- Wake-on-LAN-Filter 437
- Wake-On-LAN-Regelkette 437
- Walled Garden 430
- Walled Garden URL 430
- Weiterleiten 371
- Weiterleiten an 371
- Wiederholungen 73
- Wiederkehrender Hintergrund-Scan 161
- Wildcard 377
- Wildcard-MAC-Adresse 61
- Wildcard-Modus 61
- WLAN-Modul auswählen 405
- WLC-SSID 405
- WPA Cipher 167
- WPA-Modus 167
- WPA2 Cipher 167
- XAUTH-Profil 296
- Zeitbedingung 403
- Zeitstempel 451
- Zertifikat in Konfiguration schreiben 405
- Zertifikat ist ein CA-Zertifikat 76
- Zertifikatsanforderungsbeschreibung 78 , 405
- Ziel 346 , 348
- Ziel bei Besetzt 475
- Ziel bei Nichtmelden 475
- Ziel Sofort 475
- Ziel-IP-Adresse 398 , 405 , 424
- Ziel-IP-Adresse/Netzmaske 186 , 199 , 212 , 295
- Ziel-MAC-Adresse 437
- Ziel-Port/Bereich 199 , 212 , 218 , 233 , 433
- Zieladresse/Länge 190
- Zielpport 187 , 295
- Zielpportbereich 356
- Zielrufnummer "Sofort" 116
- Zielrufnummer "Bei besetzt" 116
- Zielrufnummer "Bei Nichtmelden" 116
- Zielschnittstelle 246 , 371

- Zielschnittstelle 190
- Zugewiesene Drahtlosnetzwerke (VSS) 158
- Zugewiesene Drahtlosnetzwerke (VSS) 155
- Zugriff 396
- Zugriffsfiler 237
- Zugriffskontrolle 172
- Zulässiger Hotspot-Client 431
- Zusammenfassend 81
- Zusätzliche, frei zugängliche Domänen-  
namen 430
- Zusätzlicher Filter des  
IPv4-Datenverkehrs 293 , 295
- Abwurf auf Ansage 44
- Abwurf auf Rufnummer 40
- Access Point-LED-Modus 152
- Access Point-Standort 152
- Aktion 182 , 445 , 461 , 464
- Aktuelle Berechtigungsklasse 479
- Aktuelle Ortszeit 48
- Aktueller Dateiname im Flash 445
- Als DHCP-Server 366
- Als IPCP-Server 366
- Alternative Schnittstelle, um DNS-Ser-  
ver zu erhalten 365
- Amtskennziffer 57
- Andere Inaktivität 351
- Angegriffener Access Point 180
- Angenommene Anrufe erfassen 124
- Angerufener Name 471 , 472
- Anmeldung 466
- Anrufe erfassen 124
- Anrufernummer 123 , 473 , 473
- Anrufschutz 477
- Anrufweitschaltung (AWS) 474
- Anschlussrufnummer 474
- AP gefunden 176
- AP offline 176
- AP verwaltet 176
- Art des Angriffs 180
- Auf Client-Anfrage antworten 426
- Aus 156
- Aushandlungsmodus 462
- Ausloggen 441
- Authentifizierung für PPP-Einwahl 75
- Authentifizierungsmethode 462
- Benachrichtigungsdienst 456
- Benutzer 119 , 120 , 123 , 441 , 471 ,  
472
- Benutzername 457 , 466 , 478
- Benutzername für Webzugang 121
- Beschreibung 461 , 462 , 464 , 465 ,  
470 , 478
- Besetzt bei Besetzt (Busy on Busy)  
478
- BOSS 445
- Bytes 462
- Cache-Größe 365
- Cache-Treffer 373
- Cache-Trefferrate (%) 373
- Call Through 470
- Client Subscription Timer 112
- CPU-Last [%] 176
- CRLs senden 323
- Datei auswählen 445
- Dateiname 445
- Datum 119 , 120 , 123 , 123 , 461 ,  
471 , 472 , 473 , 474
- Datum einstellen 49
- Dauer 119 , 120 , 123 , 471 , 472
- Delete the complete WLAN Controller  
configuration 152
- Details 461
- DHCP-Server 152
- Direktruf 52 , 476
- DNS-Anfragen 373
- DNS-Domänen-Suchliste 393
- DNS-Server 393
- Domänenname 365
- Dritter Zeitserver 49
- DSCP-Einstellungen für SIP-Daten  
112
- DSL-Logik 445
- Durchsatz 178
- Dynamische RADIUS-Authentifizierung  
322
- E-Mail-Adresse 457



- ECDSA-Schlüsselstatus 65
- ED25519-Schlüsselstatus 65
- Einloggen/Ausloggen 478
- Empfangene DNS-Pakete 373
- Endgeräte-Registrierungstimer 112
- Entfernte IP-Adresse 441
- Entfernte ID 462
- Entfernte IP-Adresse 461 , 462
- Entfernte Netzwerke 461
- Entfernter Port 462 , 465
- Erfolgreich beantwortete Anfragen 373
- Erreichbarkeitsprüfung 462
- Erster Zeitserver 49
- Erweiterte Route 192
- Externe TFE-Verbindung 52
- Externe Rufnummer 120 , 123 , 472
- Externe Verbindungen zusammenschalten 40
- Faxkopfzeile 396
- Fehler 182 , 462 , 464
- Fernzugang (z. B. Follow me, Raumüberwachung) 46
- Fertig 182
- Firewall auf Werkseinstellungen zurücksetzen 352
- Frames ohne Tag verwerfen 141
- Gateway 192
- Gebühreninformationen (S0/Upn-Erweiterung) 43
- Gefunden 156
- Gehende Verbindungen speichern 121
- Gesamt 464
- Gesprächsweitergabe ohne Melden (UbA) 53
- Gewählte Rufnummer 119 , 471 , 474
- Globaler Abwurf 44 , 44
- Größe der Zero Cookies 322
- Hashing-Algorithmen 65
- Herstellernamen anzeigen 38
- Home-Office-Nummer 478
- Host für mehrere Standorte 433
- HTTPS-TCP-Port 374
- IGMP-Status 245
- IKE (Phase-1) 463
- IKE (Phase-1) SAs 462
- Image bereits vorhanden. 182
- Importieren 83 , 84
- Individueller Teilnehmer Abwurf 44
- Initial Contact Message senden 322
- Initialisiere 156
- Int. Rufnr. 119 , 120 , 123 , 123 , 471 , 472 , 473 , 474
- Interface selection 439
- Internationaler Präfix / Länderkennzahl 42
- IP-Adressbereich 152
- IP-Adresse 466
- IP-Adresse/Netzmaske 465
- IPSec (Phase-2) 463
- IPSec (Phase-2) SAs 462
- IPSec aktivieren 321
- IPSec über TCP 322
- IPSec-Debug-Level 321
- IPSec-Tunnel 463
- ISDN-Zeitserver 49
- Keine Lizenz vorhanden 156
- Key Hash Payloads senden 323
- Klasse 441
- Kommende Verbindungen speichern 121
- Komprimierung 67
- Konfigurationsschnittstelle 60
- Kontakt 38
- Kosten 119 , 471
- Kurzwahl 57 , 470
- Ländereinstellung 42
- Läuft ab 441
- Level 461
- Lokale Adresse 465
- Lokale ID 462
- Lokale IP-Adresse 462
- Lokaler Port 462 , 465
- Lokales Zertifikat 114 , 374
- Loopback aktiv 197
- Löschen 123 , 123 , 180 , 192 , 473 , 474

- MAC-Adresse 465 , 466
- MAC-Adresse des Rogue Clients 180
- Managed 156
- Manuelle Auswahl der Bündel 57
- Manuelle Bündelbelegung zulassen 479
- Max. Anruferlisteneinträge für Benutzer 124
- Max. Anruferlisteneinträge für Systemru- fe 124
- Maximale Anzahl der Accounting- Protokolleinträge 38
- Maximale Anzahl gleichzeitiger Verbin- dungen 64
- Maximale Anzahl der IGMP- Statusmeldungen 245
- Maximale Anzahl der Syslog- Protokolleinträge 38
- Maximale E-Mails pro Minute 456
- Maximale Gruppen 245
- Maximale Quellen 245
- Maximale SMS pro Tag 458
- Maximale TTL für negative Cacheeinträ- ge 365
- Maximale TTL für positive Cacheeinträ- ge 365
- Maximales Nachrichtenlevel von Sy- stemprotokolleinträgen 38
- Meldeeingang 44
- Metrik 192 , 193
- Mobilnummer 478
- Modus 193 , 245
- Modus / Bridge-Gruppe 60
- MTU 462
- Multicast-Routing 242
- Nachricht 461
- Nachrichten 462
- Name 478
- Name der Quelldatei 445
- Name der Zieldatei 445
- NAT 465
- NAT aktiv 197
- NAT-Erkennung 462
- Nationaler Präfix / Ortsnetzkennzahl 42
- Negativer Cache 365
- Netzmaske 192
- Netzwerkname (SSID) 180
- Neuer Dateiname 445
- Nicht geändert seit 464
- Nicht-Mitglieder verwerfen 141
- Nr. 193 , 461 , 464
- Offene Rückfrage 53 , 57
- Pakete 462
- Parallelruf 476
- Passwort 457
- Passwort für HTML-Konfi- gurationszugriff 478
- Passwort für IP-Telefonregistrierung 478
- Passwort für Webzugang 121
- Passwörter und Schlüssel als Klartext anzeigen 47
- Physische Adresse 466
- Pick-Up Gezielt 57
- Pick-Up Gruppe 57
- Pick-Up-Gruppe 479
- PIN für Zugang via Telefon 478
- PIN1 46
- PIN2 46
- Ping-Befehl testweise an Adresse sen- den 442
- POP3-Server 457
- POP3-Timeout 457
- Port 466
- Port-STUN-Server 350
- Portweiterleitungen 197
- Positiver Cache 365
- PPTP-Inaktivität 351
- PPTP-Passthrough 197
- Primärer DHCP-Server 386
- Projektnummer 119 , 120 , 123 , 471 , 472
- Protokoll 192 , 193
- Protokollformat 453
- Protokollierte Aktionen 350
- Protokollierungslevel 67
- PVID 141

- QoS-Queue 467
- Quelle 182 , 445
- Queued 467
- Region 152
- Remote-Adresse 465
- Route 193
- Routentyp 192
- RSA-Schlüsselstatus 65
- RTP-Port 112
- Rufnummernverkürzung 121
- Rufweiterleitung (CFNR) 52
- Rx-Bytes 464 , 465
- Rx-Fehler 464
- Rx-Pakete 464 , 465
- SAs mit dem Status der ISP-  
Schnittstelle synchronisieren 322
- Schedule-Intervall 416
- Schnittstelle 119 , 120 , 123 , 123 ,  
141 , 152 , 192 , 193 , 193 , 426 ,  
466 , 467 , 471 , 472 , 473 , 474
- Schnittstelle ist UPnP-kontrolliert 426
- Schnittstellenbeschreibung 60
- Sekundärer DHCP-Server 386
- Senden 467
- Server aktivieren 396
- Server-Priorität 393
- Serverfehler 373
- Sicherheitsalgorithmus 461
- Signal 178
- Signal dBm 180
- Signalisierung der Übergabe 40
- SIP Port 112
- SMS-Gerät 458
- SMTP-Authentifizierung 457
- SMTP-Port 457
- SMTP-Server 457
- SNMP multicast discovery 68
- SNMP Read Community 47
- SNMP Trap Broadcasting 459
- SNMP Write Community 47
- SNMP-Listen-UDP-Port 68
- SNMP-Trap-Community 459
- SNMP-Trap-UDP-Port 459
- SNMP-Version 68
- SNTP-Server 393
- Sofort ausloggen 441
- Speicherverbrauch [%] 176
- SSH-Dienst aktiv 64
- SSH-Port 64
- SSID 180
- Standardeinstellungen wiederherstellen  
63
- Standardverhalten 106
- Standort 38
- Statische Black List 180
- Status 152 , 461 , 463 , 464 , 465
- Status der IPv4-Firewall 350
- STUN Handler 350
- Subsystem 461
- System als Zeitserver 49
- Systemadministrator-Kennwort 45
- Systemadministrator-Kennwort bestäti-  
gen 45
- Systemlogik 445
- Systemname 38
- Tarifeinheitenfaktor 43
- TCP-Inaktivität 351
- TCP-Keepalives 67
- TCP-Port des CAPI-Servers 396
- Team-Signalisierung 44
- Teilnehmernummern 479
- Telefonnummer 470
- Test-Ping-Modus 442
- TFE-Signalisierung 44
- Toleranzzeit beim Login 67
- Trace mode 439
- Traceroute-Adresse 443
- Traceroute-Modus 443
- Tx-Bytes 464 , 465
- Tx-Fehler 464
- Tx-Pakete 464 , 465
- Typ 123 , 123 , 464 , 473 , 474
- Übergabe auf besetzten Teilnehmer  
40 , 53
- Überprüfung der Rückroute 193
- Übersicht 177
- UDP-Inaktivität 351
- UDP-Quellportauswahl 342

- UDP-Zielport 342
- Ungültige DNS-Pakete 373
- UPnP TCP Port 426
- UPnP-Status 426
- URL 182 , 445
- Verbindungsdaten exportieren 122
- Verbindungsdaten löschen 122
- Verbindungsdaten über Serial 2 ausge-  
ben 121
- Verbundene Clients/VSS 176
- Vergabe von Projektnummern 57
- Verschlüsselt 464
- Verschlüsselung der Konfiguration  
445
- Verschlüsselungsalgorithmen 65
- Verwerfen ohne Rückmeldung 197
- Verworfen 464 , 467
- VLAN aktivieren 142
- Vollständige IPSec-Konfiguration lö-  
schen 321
- Vollständige IPv4-Filterung 350
- Wahlberechtigung 479
- Währung 43
- Weitergeleitet 464
- Weitergeleitete Anfragen 373
- WINS-Server 365
- Wird ausgeführt 182
- WLAN Controller: VSS-Durchsatz 176
- Zeit 119 , 120 , 123 , 123 , 461 , 471 ,  
472 , 473 , 474
- Zeit einstellen 49
- Zeitaktualisierungsintervall 49
- Zeitaktualisierungsrichtlinie 49
- Zeitzone 48
- Zero Cookies verwenden 322
- Zertifikate und Schlüssel einschließen  
445
- Zertifikatsanforderung 78
- Zertifikatsanforderungs-Payloads sen-  
den 323
- Zertifikatsanforderungs-Payloads nicht  
beachten 323
- Zertifikatsketten senden 323
- Ziel-IP-Adresse 192
- Zu verwendende Schnittstelle 442
- Zuerst gesehen 180
- Zuletzt gesehen 180
- Zweiter Zeitserver 49
- Access Points 177
- Access Points 156
- Adressliste 353
- Aktionen 405
- Aktive Clients 177
- Aktive IPSec-Tunnel 36
- Aktive Sitzungen (SIF, RTP, etc... )  
36
- Aktuelle Berechtigungsklasse 469
- Allgemein 121 , 124 , 152 , 426
- Allgemeine Einstellungen 478
- Änderbare Kennziffern 56
- Anrufweiterschaltung (AWS) 115
- Arbeitsspeichernutzung 36
- Auslöser 398
- Autoprofil für Access Points 155
- Benachbarte APs 179
- Benachrichtigungseinstellungen 456
- Benachrichtigungsempfänger 454
- Benutzer 337 , 396
- Benutzer ausloggen 441
- Benutzertelefonbuch 471
- Beschreibung 468
- Cache 373
- Client-Verwaltung 178
- Codec-Profil 109
- CPU-Nutzung 36
- CRLs 83
- Datum 47
- DHCP-Konfiguration 380
- DHCP-Relay-Einstellungen 386
- Dienstliste 356
- Dienstkategorien 278
- DNS-Server 367
- DNS-Test 442
- Domänenweiterleitung 371
- Drahtlosnetzwerke (VSS) 166 , 178
- Dynamische Hosts 373
- DynDNS-Aktualisierung 375
- DynDNS-Provider 377

- Einstellungen von Features 474
- Firmware-Wartung 181
- Funkmodulprofile 160
- Gehend 119 , 123 , 471 , 473
- Globale DHCPv6-Optionen 393
- Globale Einstellungen 365
- Gruppen 355 , 358
- Hosts 420
- Hotspot-Gateway 429
- HTTP 63
- HTTPS 63
- HTTPS-Server 374
- IP Pools 272 , 320
- IP-Pool-Konfiguration 380
- IP/MAC-Bindung 385
- IPSec-Peers 287
- IPSec-Statistiken 463
- IPSec-Tunnel 461
- IPv4-Filterregeln 345
- IPv4-Gruppen 352
- IPv4-Routing-Tabelle 192
- IPv4/IPv6-Filter 217
- IPv6-Routenkonfiguration 190
- IPv6-Routingtabelle 193
- ISDN-Login 63
- Kommend 120 , 122 , 472 , 473
- Konfiguration eines Allgemeinen Präfixes 195
- Konfiguration von IPv4-Routen 184
- Konfiguration von zustandsbehafteten Clients 394
- Lastverteilungsgruppen 207
- Manuelle Bündelbelegung zulassen 469
- Name, Vorname 468
- NAT-Konfiguration 198
- NAT-Schnittstellen 196
- Netzwerk-Status 466
- OAM-Regelung 280
- Optionen 75 , 112 , 193 , 245 , 321 , 342 , 350 , 396 , 416 , 433 , 443 , 453
- Passwörter 45
- Phase-1-Profile 305
- Phase-2-Profile 313
- Pick-Up-Gruppe 469
- Ping 63
- Ping-Generator 424
- Ping-Test 442
- Portkonfiguration 141
- PPPoA 264
- PPPoE 249
- PPTP 259
- Profile 274
- QoS-Klassifizierung 221
- QoS-Schnittstellen/Richtlinien 224
- RADIUS 69
- Regelketten 237
- Regulierte Schnittstellen 285
- Rogue APs 180
- Rogue Clients 180
- Schnittstellen 60 , 126 , 423 , 426 , 453
- Schnittstellenzuweisung 238 , 439
- SIP-Provider 94
- SNMP 63 , 68
- SNMP-Trap-Hosts 460
- SNMP-Trap-Optionen 459
- Special Session Handling 211
- SSH 63 , 64
- Standorte 106
- Statische Hosts 369
- Statistik 373 , 464
- Sync-Anschluss 91
- Syslog-Server 450
- System 38
- System-Telefonbuch 470
- Systemlizenzen 54
- Systemmeldungen 461
- Systemneustart 449
- Telnet 63
- Timer 51
- Trace-Schnittstelle 439
- Traceroute-Test 443
- Tunnelprofile 334
- Verwaltung 142
- VLANs 140
- Wahlberechtigung 469

- Wahlkontrolle 117
- Wake-on-LAN-Filter 433
- WLAN Controller 176
- WOL-Regeln 437
- XAUTH-Profilen 318
- Zeit 47
- Zertifikatsliste 76
- Zertifikatsserver 84
- Zugriffsfiler 233
- Zustandsbehaftete Clients 391
- Zustandsbehaftete Clients 394
- Adressen 353
- Allgemein 242
- Allgemeine IPv6-Präfixe 194
- Anrufliste 122 , 473
- AP-Konfiguration 156
- ATM 273
- Benachrichtigungsdienst 454
- Benutzer ausloggen 441
- Bridges 466
- CAPI-Server 395
- Controller-Konfiguration 152
- DHCP-Server 379
- DHCPv6-Server 389
- Diagnose 442
- Dienste 355
- DNS 363
- DynDNS-Client 375
- Einstellungen 94 , 474
- Factory Reset 449
- Globale Einstellungen 38
- Hotspot-Gateway 427 , 466
- HTTPS 374
- IGMP 242
- Internes Protokoll 461
- IP-Accounting 452
- IP-Konfiguration 126
- IPSec 286 , 461
- Kennziffern 56
- L2TP 333
- Lastverteilung 207
- Monitoring 176
- NAT 196
- Neustart 449
- QoS 217 , 467
- Real Time Jitter Control 284
- Richtlinien 345
- Routen 184
- Scheduling 397
- Schnittstellen 352 , 464
- Schnittstellenmodus / Bridge-Gruppen 58
- SIA 460
- SNMP 458
- Software & Konfiguration 443
- Systemprotokoll 450
- Telefonbuch 470
- Trace 439
- Überwachung 420
- Umgebungs-Monitoring 179
- UPnP 425
- Verbindungsdaten 119 , 471
- VLAN 140
- Wake-On-LAN 433
- Wartung 181
- Weiterleiten 246
- Wizard 144
- Zertifikate 75
- Zugriffsregeln 231
- Benutzerzugang 468
- Firewall 343
- LAN 126
- VoIP 94
- Wireless LAN Controller 143
- DHCP-Client (Konfigurationsbeispiel) 387
- DHCP-Relay-Server (Konfigurationsbeispiel) 387
- DHCP-Server (Konfigurationsbeispiel) 387
- NAT (Konfigurationsbeispiel) 204
- SIF (Konfigurationsbeispiel) 358
- #
- #1#2, #3 82
- <

<Interne Rufnummer> 468

## A

ACCESS\_ACCEPT 70  
 ACCESS\_REJECT 70  
 ACCESS\_REQUEST 70  
 ACCOUNTING\_START 70  
 ACCOUNTING\_STOP 70  
 Administrativer Zugriff 63  
 Aktuelle Geschwindigkeit / Aktueller Mo-  
 dus 87  
 Angerufener Name 119  
 Anrufername 120  
 Anrufkontrolle 115  
 Anschlussart 37, 90  
 Anwendungen 119  
 Assistent für Netzwerkeinstellung 19  
 Assistenten 34  
 Ausgehende Dienste 115

## B

Bedienelemente 24  
 Benutzerzugang 20  
 Beschreibung 37  
 Beschreibung - Verbindungsinformation  
 - Link 37  
 Betriebsmodus (Aktiv) 405  
 Betriebsmodus (Inaktiv) 405  
 Bohrschablone 10  
 BOSS-Version 36

## D

Downstream 92  
 DSL-Chipsatz 91  
 DSL-Konfiguration 91  
 DSL-Leitungsprofil 93  
 DSL-Modem 91  
 DSL-Modus 92  
 DSP-Kanäle 36

## E

Ethernet-Ports 86

Ethernet-Schnittstellenauswahl 87  
 Externe Berichterstellung 450

## F

Flusskontrolle 87  
 Funkmodul1 177  
 Funktion 90

## G

Grundkonfiguration 15

## H

Homepage 378  
 HTTPS/SSL 375

## I

Interner ISDN-Anschluss 10  
 Internet + Einwählen 248  
 IP-Adresse 16  
 IP-Version 375  
 ISDN Intern 89  
 ISDN-Ports 89

## K

Konfiguration 23  
 Konfiguration der automatischen Spei-  
 cherung 38  
 Konfigurationsbeispiel - DHCP-Client  
 387  
 Konfigurationsbeispiel - DHCP-Re-  
 lay-Server 387  
 Konfigurationsbeispiel - DHCP-Server  
 387  
 Konfigurationsbeispiel -  
 Lastverteilung 214  
 Konfigurationsbeispiel - NAT 204  
 Konfigurationsbeispiel - Scheduling  
 417  
 Konfigurationsbeispiel - SIF 358  
 Konfigurationsbeispiel - Zeitgesteuerte  
 Aufgaben 417

- Konfigurationsdaten sammeln 16
- Konfigurationsoberfläche aufrufen 24
- Konfigurierte Geschwindigkeit / Konfigu-  
rierter Modus 87
- L**
- Lastverteilung (Konfigurationsbeispiel  
) 214
- Letzte gespeicherte Konfiguration 36
- Lokale Dienste 363
- M**
- Map-Resolver IP Address 329
- Maximale Upstream-Bandbreite 92
- MediaSec 105
- Monitoring 461
- Multicast 240
- N**
- Name 90
- Netzmaske 16
- Netzwerk 184
- Netzwerkeinstellung 19
- Nr. 37
- P**
- PC einrichten 17
- Physikalische Verbindung 91
- Physikalische Schnittstellen 86
- Pin-Belegungen 11
- Portkonfiguration 87
- R**
- Rauschabstand 92
- Registrar 37
- Remote Authentifizierung 69
- Reset 8
- Reset-Taster 10
- S**
- Scheduling (Konfigurationsbeispiel)  
417
- Schnittstelle - Verbindungsinformation -  
Link 37
- Seriennummer 36
- Server IPv6 378
- SIP-Header-Feld: FROM Display 98
- SIP-Header-Feld: FROM User 98
- SIP-Header-Feld: P-Asserted 98
- SIP-Header-Feld: P-Preferred 98
- Softwareaktualisierung 21
- Standard-MSN 90
- Status 35 , 37 , 90
- Status Nachtbetrieb 36
- Support 9
- Supports SSL 378
- Switch-Port 87
- System-Voraussetzungen 15
- Systemdatum 36
- Systemsoftware 15
- Systemverwaltung 35
- T**
- Transmit Shaping 92
- U**
- Upstream 92
- Uptime 36
- V**
- Vorbereitungen 15
- VPN 286
- W**
- Walled Network / Netzmaske 430
- WAN 248
- Wandmontage 10
- Wartung 441
- WEP-Schlüssel 1-4 167
- Z**
- Zeitgesteuerte Aufgaben



(Konfigurationsbeispiel) 417  
Zugang über LAN 23