



Benutzerhandbuch bintec WLAN-Geräte

Referenz

Copyright© Version 10.2.7 RC (SVN 8981) 11/2019 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.

Inhaltsverzeichnis

Kapitel 1	Inbetriebnahme	1
1.1	bintec W1001n und bintec W1003n	1
1.1.1	Aufstellen und Anschließen	1
1.1.2	Anschlüsse	3
1.1.3	LEDs	4
1.1.4	Lieferumfang	6
1.1.5	Allgemeine Produktmerkmale	6
1.1.6	Reset	7
1.2	bintec WI1003n.	8
1.2.1	Aufstellen und Anschließen	8
1.2.2	Anschlüsse	10
1.2.3	LEDs	11
1.2.4	Lieferumfang	12
1.2.5	Allgemeine Produktmerkmale	12
1.2.6	Reset	13
1.3	bintec W2003ac und bintec W2003ac-ext	14
1.3.1	Aufstellen und Anschließen	14
1.3.2	Anschlüsse	17
1.3.3	LEDs	18
1.3.4	Lieferumfang	19
1.3.5	Allgemeine Produktmerkmale	19
1.3.6	Reset	21
1.4	bintec WO1003ac und bintec WO2003ac	21
1.4.1	Aufstellen und Anschließen	21
1.4.2	Anschlüsse	24
1.4.3	LEDs	25
1.4.4	Lieferumfang	27
1.4.5	Allgemeine Produktmerkmale	27
1.4.6	Reset	28

1.5	Reinigen	29
1.6	Pin-Belegung	29
1.6.1	Ethernet-Schnittstelle	29
1.6.2	Stromversorgung	30
1.7	Frequenzen und Kanäle	30
1.8	Support Information	30
Kapitel 2	Grundkonfiguration	31
2.1	Voreinstellungen	31
2.1.1	Vorkonfigurierte Daten	31
2.1.2	Software-Update	32
2.2	System-Voraussetzungen	33
2.3	Vorbereitung	33
2.3.1	Daten sammeln	33
2.3.2	PC einrichten	34
2.4	IP-Konfiguration	36
2.5	Systempasswort ändern	37
2.6	Drahtlosnetzwerk einrichten	38
2.7	Softwareaktualisierung	39
Kapitel 3	Zugang und Konfiguration	41
3.1	Zugangsmöglichkeiten	41
3.1.1	Zugang über LAN	41
3.2	Anmelden	45
3.2.1	Benutzernamen und Passwörter im Auslieferungszustand	45
3.2.2	Anmelden zur Konfiguration	46
3.3	Konfigurationsmöglichkeiten	46

3.3.1	GUI (Graphical User Interface) für Fortgeschrittene	47
3.3.2	SNMP-Shell	57
Kapitel 4	Assistenten	58
Kapitel 5	Systemverwaltung	59
5.1	Status	59
5.2	Globale Einstellungen	61
5.2.1	System	61
5.2.2	Passwörter	64
5.2.3	Datum und Uhrzeit	65
5.2.4	Systemlizenzen	70
5.3	Schnittstellenmodus / Bridge-Gruppen	72
5.3.1	Schnittstellen	74
5.4	Administrativer Zugriff	77
5.4.1	Zugriff	77
5.4.2	SSH	78
5.4.3	SNMP	82
5.5	Remote Authentifizierung	83
5.5.1	RADIUS	83
5.5.2	TACACS+	89
5.5.3	Optionen	91
5.6	Konfigurationszugriff	92
5.6.1	Zugriffsprofile	92
5.6.2	Benutzer	95
5.7	Zertifikate	96
5.7.1	Zertifikatsliste	97
5.7.2	CRLs	104
5.7.3	Zertifikatsserver	105

Kapitel 6	Physikalische Schnittstellen	107
6.1	Ethernet-Ports	107
6.1.1	Portkonfiguration	107
Kapitel 7	LAN	109
7.1	IP-Konfiguration	109
7.1.1	Schnittstellen	109
7.2	VLAN	123
7.2.1	VLANs	123
7.2.2	Portkonfiguration	124
7.2.3	Verwaltung	125
Kapitel 8	Wireless LAN	126
8.1	WLAN	126
8.1.1	Einstellungen Funkmodul	126
8.1.2	Drahtlosnetzwerke (VSS)	135
8.1.3	Client Link	145
8.1.4	Bridge-Links	148
8.2	Verwaltung	150
8.2.1	Grundeinstellungen	150
Kapitel 9	Wireless LAN Controller	151
9.1	Wizard	152
9.1.1	Wireless LAN Controller Wizard	153
9.1.2	Wireless LAN Controller VLAN Konfiguration	159
9.2	Controller-Konfiguration	160
9.2.1	Allgemein	160
9.2.2	Slave-AP-Autoprofil	162

9.3	Slave-AP-Konfiguration	164
9.3.1	Slave Access Points	164
9.3.2	Funkmodulprofile	167
9.3.3	Drahtlosnetzwerke (VSS)	173
9.4	Monitoring	182
9.4.1	WLAN Controller	182
9.4.2	Slave Access Points	183
9.4.3	Aktive Clients	183
9.4.4	Drahtlosnetzwerke (VSS)	184
9.4.5	Client-Verwaltung	184
9.5	Umgebungs-Monitoring	184
9.5.1	Benachbarte APs	185
9.5.2	Rogue APs	185
9.5.3	Rogue Clients	186
9.6	Wartung	187
9.6.1	Firmware-Wartung	187
Kapitel 10	Netzwerk	189
10.1	Routen	189
10.1.1	Konfiguration von IPv4-Routen	189
10.1.2	Konfiguration von IPv6-Routen	195
10.1.3	IPv4-Routing-Tabelle	197
10.1.4	IPv6-Routing-Tabelle	198
10.1.5	Optionen	198
10.2	Allgemeine IPv6-Präfixe	199
10.2.1	Konfiguration eines Allgemeinen Präfixes	200
10.3	NAT	201
10.3.1	NAT-Schnittstellen	201
10.3.2	NAT-Konfiguration	202
10.3.3	NAT - Konfigurationsbeispiel	209

10.4	Lastverteilung	212
10.4.1	Lastverteilungsgruppen	212
10.4.2	Special Session Handling	216
10.4.3	Lastverteilung - Konfigurationsbeispiel.	219
10.5	QoS	222
10.5.1	IPv4/IPv6-Filter	222
10.5.2	QoS-Klassifizierung	226
10.5.3	QoS-Schnittstellen/Richtlinien	228
10.6	Zugriffsregeln	236
10.6.1	Zugriffsfiler	238
10.6.2	Regelketten	242
10.6.3	Schnittstellenzuweisung	243
10.7	Drop-In	244
10.7.1	Drop-In-Gruppen	244
Kapitel 11	Routing-Protokolle	247
11.1	RIP	247
11.1.1	RIP-Schnittstellen	247
11.1.2	RIP-Filter	249
11.1.3	RIP-Optionen	251
Kapitel 12	Multicast	254
12.1	Allgemein	256
12.1.1	Allgemein	256
12.2	IGMP	256
12.2.1	IGMP	257
12.2.2	Optionen	259
12.3	Weiterleiten	260
12.3.1	Weiterleiten	260

12.4	PIM	261
12.4.1	PIM-Schnittstellen	262
12.4.2	PIM-Rendezvous-Punkte	264
12.4.3	PIM-Optionen	266
Kapitel 13	WAN.	267
13.1	Internet + Einwählen	267
13.1.1	PPPoE	269
13.1.2	Dual Stack Lite (DS-Lite)	278
13.1.3	PPTP	279
13.1.4	IP Pools	284
13.2	Real Time Jitter Control	285
13.2.1	Regulierte Schnittstellen	285
Kapitel 14	VPN	287
14.1	IPSec	287
14.1.1	IPSec-Peers	288
14.1.2	Phase-1-Profile	306
14.1.3	Phase-2-Profile	314
14.1.4	XAUTH-Profile	319
14.1.5	IP Pools	321
14.1.6	Optionen	322
14.2	L2TP	326
14.2.1	Tunnelprofile	326
14.2.2	Benutzer	329
14.2.3	Optionen	334
14.3	PPTP	335
14.3.1	PPTP-Tunnel	335
14.3.2	Optionen	342
14.3.3	IP Pools	342

14.4	GRE	343
14.4.1	GRE-Tunnel	344
Kapitel 15	Firewall	346
15.1	Richtlinien	348
15.1.1	IPv4-Filterregeln	348
15.1.2	IPv6-Filterregeln	350
15.1.3	Optionen	353
15.2	Schnittstellen	355
15.2.1	IPv4-Gruppen	355
15.2.2	IPv6-Gruppen	356
15.3	Adressen	356
15.3.1	Adressliste	356
15.3.2	Gruppen	358
15.4	Dienste	358
15.4.1	Dienstliste	359
15.4.2	Gruppen	361
15.5	Konfiguration.	361
15.5.1	SIF - Konfigurationsbeispiel	361
Kapitel 16	Lokale Dienste	366
16.1	DNS	366
16.1.1	Globale Einstellungen	368
16.1.2	DNS-Server	370
16.1.3	Statische Hosts	372
16.1.4	Domänenweiterleitung	373
16.1.5	Dynamische Hosts	375
16.1.6	Cache	375
16.1.7	Statistik	376

16.2	HTTPS	376
16.2.1	HTTPS-Server	377
16.3	DynDNS-Client	377
16.3.1	DynDNS-Aktualisierung	378
16.3.2	DynDNS-Provider	380
16.4	DHCP-Server	382
16.4.1	IP-Pool-Konfiguration	382
16.4.2	DHCP-Konfiguration	383
16.4.3	IP/MAC-Bindung	388
16.4.4	DHCP-Relay-Einstellungen	389
16.4.5	DHCP - Konfigurationsbeispiel	389
16.5	DHCPv6-Server	392
16.5.1	DHCPv6-Server	393
16.5.2	Globale DHCPv6-Optionen	395
16.5.3	Zustandsbehaftete Clients	397
16.5.4	Konfiguration von zustandsbehafteten Clients	397
16.6	Scheduling	398
16.6.1	Auslöser	399
16.6.2	Aktionen	405
16.6.3	Optionen	417
16.6.4	Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling)	417
16.7	Überwachung	421
16.7.1	Hosts	421
16.7.2	Schnittstellen	424
16.7.3	Ping-Generator	425
16.8	Hotspot-Gateway	426
16.8.1	Hotspot-Gateway	428
16.8.2	Optionen	431
16.9	Wake-On-LAN	432
16.9.1	Wake-on-LAN-Filter	432

16.9.2	WOL-Regeln	436
16.9.3	Schnittstellenzuweisung	437
16.10	Trace	438
16.10.1	Trace-Schnittstelle	438
16.10.2	VoIP/SIP-Trace	439
Kapitel 17	Wartung	440
17.1	Benutzer ausloggen	440
17.1.1	Benutzer ausloggen	440
17.2	Diagnose	441
17.2.1	Ping-Test	441
17.2.2	DNS-Test	441
17.2.3	Traceroute-Test	442
17.3	Software & Konfiguration	442
17.3.1	Optionen	442
17.4	Neustart	448
17.4.1	Systemneustart	448
17.5	Factory Reset	448
Kapitel 18	Externe Berichterstellung	449
18.1	Systemprotokoll	449
18.1.1	Syslog-Server	449
18.2	IP-Accounting	451
18.2.1	Schnittstellen	452
18.2.2	Optionen	452
18.3	Benachrichtigungsdienst	453
18.3.1	Benachrichtigungsempfänger	453
18.3.2	Benachrichtigungseinstellungen	455
18.4	SNMP	457

18.4.1	SNMP-Trap-Optionen	458
18.4.2	SNMP-Trap-Hosts	459
18.5	SIA	459
18.5.1	SIA	459
Kapitel 19	Monitoring	460
19.1	Internes Protokoll	460
19.1.1	Systemmeldungen	460
19.2	IPSec	460
19.2.1	IPSec-Tunnel	460
19.2.2	IPSec-Statistiken	462
19.3	Schnittstellen	463
19.3.1	Statistik	463
19.3.2	Netzwerk-Status	465
19.4	WLAN	465
19.4.1	WLANx	465
19.4.2	VSS	466
19.4.3	Client-Verwaltung	468
19.4.4	Bridge-Links	469
19.4.5	Client Links	470
19.5	Bridges	471
19.5.1	br<x>	471
19.6	Hotspot-Gateway	471
19.6.1	Hotspot-Gateway	471
19.7	QoS	472
19.7.1	QoS	472
19.8	PIM	472
19.8.1	Allgemeine Statusangaben	473
19.8.2	Nicht-schnittstellen-spezifischer Status	474

19.8.3	Schnittstellenspezifische Zustände	476
	Glossar	479
	Index	510

Kapitel 1 Inbetriebnahme



Hinweis

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

1.1 bintec W1001n und bintec W1003n

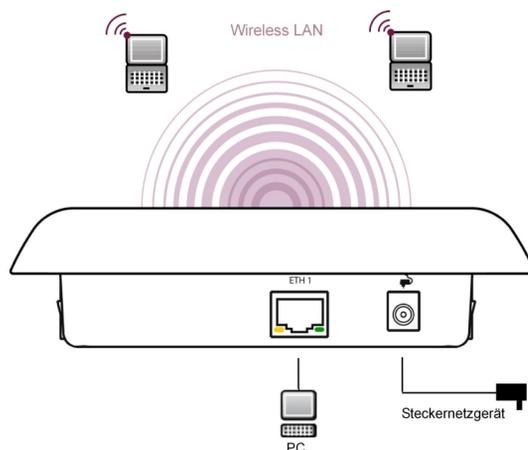
1.1.1 Aufstellen und Anschließen



Hinweis

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

Die Geräte besitzen integrierte Antennen, deren Abstrahlcharakteristik für die Deckenmontage optimiert ist.



Anschlussmöglichkeiten **bintec W1001n** und **bintec W1003n**

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

(1) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN.

Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(2) Stromanschluss



Hinweis

Die Geräte werden ohne Steckernetzteil geliefert. Das Steckernetzteil mit EU-Stecker (Artikelnummer 5500001254) ist als Zubehör erhältlich.

Schließen Sie das Gerät an eine Steckdose an. Nehmen Sie dazu das Steckernetzteil und stecken Sie es in die dafür vorgesehene Buchse Ihres Geräts. Stecken Sie nun den Netzstecker in eine Steckdose (100–240 V). Durch die Status-LED wird Ihnen signalisiert, dass Ihr Gerät korrekt an die Stromversorgung angeschlossen ist. Optional kann die Stromversorgung über ein Standard PoE-Injector (Artikelnummer 5530000082) erfolgen.

Montage

Die Access Points sind wahlweise an die Wand oder an die Decke zu montieren oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

Befestigen Sie die vier selbstklebenden Füße auf der unteren Seite des Gerätes. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wand- / Deckenmontage

Um die Geräte **bintec W1003n** an der Wand bzw. Decke zu montieren, verwenden Sie die Halterung, die im Lieferumfang enthalten ist (Artikelnummer 5500001278).

Der **bintec W1001n** ist durch Laschen an der Gehäuserückseite an die Wand zu montieren. Als Zubehör erhältlich ist eine Deckenhalterung, um das Gerät an der Decke zu montieren.

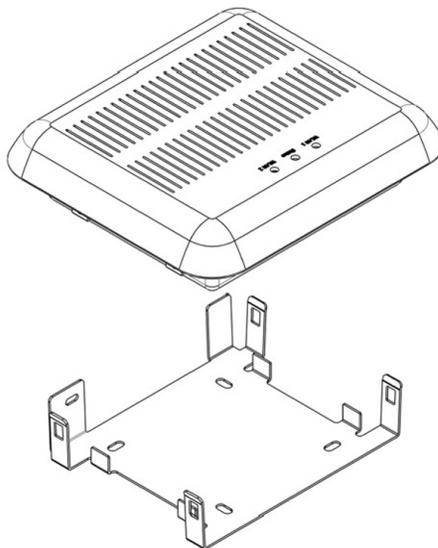
Mittels eines Kensington-Schlusses können die Geräte gegen Diebstahl gesichert werden.



Warnung

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

- Schrauben Sie die Halterung an der Wand bzw. Decke fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät ggf. mit einem Kensington-Schloss gegen Diebstahl.



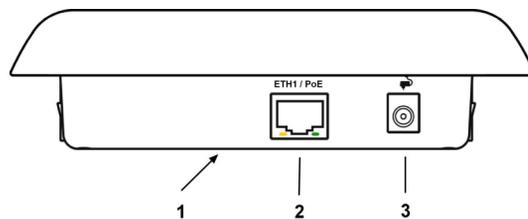
Deckenmontage

1.1.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

bintec W1001n und **bintec W1003n** verfügen über einen Ethernet-Anschluss.

Die Anschlüsse sind folgendermaßen angeordnet:



Unterseite

1	RESET	Reset-Taste führt Neustart durch (an der Bodenplatte des Geräts)
2	ETH1/PoE	10/100/1000 Base-T Ethernet-Schnittstelle

3	POWER	Buchse für Steckernetzteil
---	-------	----------------------------

1.1.3 LEDs

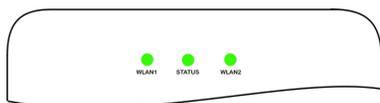
Anhand der LEDs können Sie Funkstatus und Funkaktivität Ihres Geräts erkennen.



Hinweis

Beachten Sie, dass die Anzahl der aktiven WLAN LEDs abhängig ist von der Anzahl der vorhandenen Radiomodule.

Die LEDs von **bintec W1003n** sind folgendermaßen angeordnet:



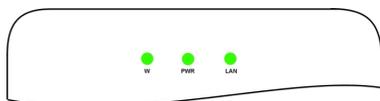
Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
Status	grün	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.
		an (statisch)	Fehler
		blinkend	Betriebsbereit
WLAN 1/2	grün	aus	Radiomodul oder alle zugeordneten VSS deaktiviert.
		langsam blinkend	VSS ist aktiv, kein Client angemeldet.
		schnell blinkend	VSS ist aktiv, mindestens 1 Client ist angemeldet.
		flackernd	VSS ist aktiv, mindestens 1 Client ist angemeldet, es besteht Datenverkehr.
ETH 1/2	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
		blinkend	Datenverkehr mit 1 Gbit/s.
	orange	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
		blinkend	Datenverkehr mit 100 Mbit/s.

LED	Farbe	Status	Information
	grün und orange	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und orange	blinkend	Datenverkehr mit 10 Mbit/s.

Die LEDs von **bintec W1001n** sind folgendermaßen angeordnet:



Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
LAN			Keine Funktion
PWR	grün	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.
		an (statisch)	Fehler
		blinkend	Betriebsbereit
W	grün	aus	Radiomodul oder alle zugeordneten VSS deaktiviert
		langsam blinkend	VSS ist aktiv, kein Client angemeldet
		schnell blinkend	VSS ist aktiv, mindestens 1 Client ist angemeldet
		flackernd	VSS ist aktiv, mindestens 1 Client ist angemeldet, es besteht Datenverkehr
ETH 1	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
	grün	blinkend	Datenverkehr mit 1 Gbit/s.
	orange	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
	orange	blinkend	Datenverkehr mit 100 Mbit/s.
	grün und orange	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und orange	blinkend	Datenverkehr mit 10 Mbit/s.

Das Leuchtverhalten der LEDs können Sie im Menü **Globale Einstellungen** und mit dem **WLAN Controller** in drei verschiedene Betriebsarten schalten.



Hinweis

Wenn Sie das LED-Verhalten über das **GUI** oder den **WLAN Controller** angepasst haben, bleibt diese Einstellung nach einem Wiederherstellen des Auslieferungszustands erhalten.

Status	Die LEDs zeigen ihr Standardverhalten.
Blinkend	Nur die Status-LED blinkt einmal in der Sekunde.
Aus	Alle LEDs sind deaktiviert.

1.1.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Dokumentation
bintec W1001n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße	Installationsposter Sicherheitshinweise
bintec W1003n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße Wand- bzw. Deckenbefestigung	Installationsposter Sicherheitshinweise

1.1.5 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	ca. 159 x 145 x 43 mm
Gewicht	ca. 1000 g (mit WLAN-Modulen)

Eigenschaft	Wert
LEDs	Für bintec W1001n : 3 (1x LAN, 1x Power, 1x WLAN) Für bintec W1003n : 3 (1x Status, 2x WLAN)
Leistungsaufnahme Gerät	bintec W1001n : max. 4,5 W bintec W1003n : max. 6,5 W
Spannungsversorgung	230 V / 9-12 V DC, 1 A (Das Steckernetzteil mit der Artikelnummer 5500001254 ist als Zubehör erhältlich) PoE an Ethernet 1 Class 0, gemäß 802.3af (max. 12,4 W), kompatibel mit 802.3at Injektor. Der Gigabit PoE Injektor mit der Artikelnummer 5530000082 ist als Zubehör erhältlich.
Umweltanforderungen:	
Lagertemperatur	-10 °C bis +70 °C
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 95 % (nicht kondensierend)
Verfügbare Schnittstellen:	
WLAN	1 Radiomodul 802.11abgn 2,4 oder 5 GHz Mimo 2x2
Ethernet IEEE 802.3 LAN	10/100/1000 MBit/s
Vorhandene Buchsen:	
Ethernet-Schnittstelle	1 RJ45-Buchse
Antennen:	
Antennenanschluss	2 interne Antennen
Sendeleistung (WLAN)	max. 100 mW (20 dBm) EIRP
Richtlinien & Normen	Directive 2014/53/EU, 2011/65/EU, 2009/125/EU, EN 60950-1; EN 62311; EN 301489-1; EN301489-17; EN 300 328; EN 301893; EN 50581; EN 60601-1-2 (Medical devices - part 1-2)
Taster	Reset-Taster für Neustart oder Reset

1.1.6 Reset

Im Falle einer Fehlkonfiguration oder bei Nichterreichbarkeit Ihres Geräts können Sie das Gerät mit dem Reset-Knopf auf der Geräteunterseite mit den Standardeinstellungen des Auslieferungszustands starten lassen.

Dabei werden alle bestehenden Konfigurationsdaten gelöscht.

- (1) Drücken Sie die **Reset**-Taste Ihres Geräts.

- (2) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt.
- (3) Achten Sie auf die LEDs:
Die Status-LED leuchtet, das Gerät durchläuft die Boot-Sequenz.
Lassen Sie **Reset**-Taste los, wenn die Status-LED wieder zu blinken beginnt.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 31 beschrieben.



Hinweis

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



Hinweis

Wenn sie das LED-Verhalten im Menü **Globale Einstellungen** oder mit dem **WLAN Controller** auf einen anderen als den Standardwert gesetzt haben, bleibt diese Einstellung beim Zurücksetzen des Geräts erhalten.

1.2 bintec WI1003n

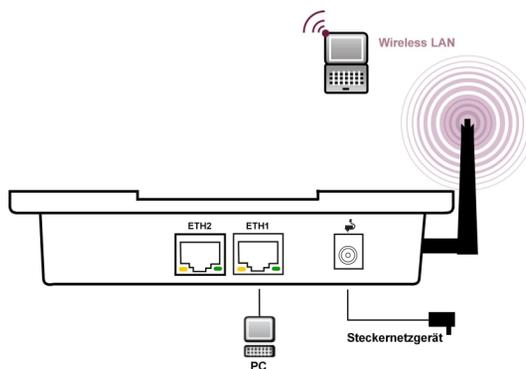
1.2.1 Aufstellen und Anschließen



Hinweis

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

Die Geräte **bintec WI1003n** verwenden externe Antennen.



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

(1) Antennen

Schrauben Sie die Standardantennen (Zubehör) auf die dafür vorgesehenen Anschlüsse. Falls Sie andere Antennen verwenden, beachten Sie, dass MIMO-Antennen an den Anschlüssen Ant 1-1 und Ant 2-2 anzuschließen sind.

(2) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

Wählen Sie hier lediglich einen der Anschlüsse **ETH1** oder **ETH2**, der zweite Anschluss dient der Kaskadierung mehrerer Geräte. Bei Verwendung beider Ethernet-Anschlüsse am selben Switch können sich Loops bilden.

Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(3) Stromanschluss



Hinweis

Die Geräte werden ohne Steckernetzteil geliefert. Das Steckernetzteil mit EU-Stecker (Artikelnummer 5500001254) ist als Zubehör erhältlich.

Schließen Sie das Gerät an eine Steckdose an. Nehmen Sie dazu das Steckernetzteil und stecken Sie es in die dafür vorgesehene Buchse Ihres Geräts. Stecken Sie nun den Netzstecker in eine Steckdose (100–240 V). Durch die Status-LED wird Ihnen signalisiert, dass Ihr Gerät korrekt an die Stromversorgung angeschlossen ist. Optional kann die Stromversorgung über ein Standard PoE-Injector (Artikelnummer 5530000082) erfolgen.

Montage

Die Access Points sind wahlweise an die Wand oder an die Decke zu montieren oder als

Tischgerät einzusetzen.

Mit dem im Lieferumfang enthaltenen DIN-Hutschienenadapter können die Access Points in einer Schalttafel montiert werden.

Verwendung als Tischgerät

Befestigen Sie die vier selbstklebenden Füße auf der unteren Seite des Gerätes. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wand- / Deckenmontage

Um die Geräte **bintec WI1003n** an der Wand bzw. Decke zu montieren, verwenden Sie die Halterung, die im Lieferumfang enthalten ist (Artikelnummer 5500001278).

Schalttafel

Für den Einbau in eine Schalttafel verwenden Sie den DIN-Hutschienenadapter der im Lieferumfang enthalten ist.



Warnung

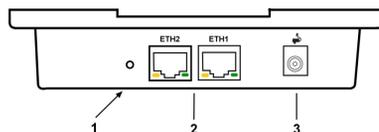
Vergewissern Sie sich vor dem Bohren, dass sich an der Bohrstelle keine Hausinstallationen befinden. Bei Beschädigung an Gas-, Strom-, Wasser- und Abwasserleitungen kann Lebensgefahr oder Sachschaden entstehen.

- Schrauben Sie die Halterung an der Wand bzw. Decke fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät ggf. mit einem Kensington-Schloss gegen Diebstahl.

1.2.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts. **bintec WI1003n** verfügt über zwei Ethernet-Anschlüsse.

Die Anschlüsse sind folgendermaßen angeordnet:



Anschlüsse bintec WI1003n

1	RESET	Reset-Taste führt Neustart durch (an der Bodenplatte des Ge-
---	-------	--

		räts)
2	ETH1/PoE und ETH2	10/100/1000 Base-T Ethernet-Schnittstelle
3	POWER	Buchse für Steckernetzteil

1.2.3 LEDs

Anhand der LEDs können Sie Funkstatus und Funkaktivität Ihres Geräts erkennen.



Hinweis

Beachten Sie, dass die Anzahl der aktiven WLAN LEDs abhängig ist von der Anzahl der vorhandenen Radiomodule.

Die LEDs von **bintec WI1003n** sind folgendermaßen angeordnet:



Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
Status	grün	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.
		an (statisch)	Fehler
		blinkend	Betriebsbereit
WLAN 1/2	grün	aus	Radiomodul oder alle zugeordneten VSS deaktiviert
		langsam blinkend	VSS ist aktiv, kein Client angemeldet
		schnell blinkend	VSS ist aktiv, mindestens 1 Client ist angemeldet
		flackernd	VSS ist aktiv, mindestens 1 Client ist angemeldet, es besteht Datenverkehr
ETH 1/2	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
		blinkend	Datenverkehr mit 1 Gbit/s.
		orange	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.

LED	Farbe	Status	Information
	orange	blinkend	Datenverkehr mit 100 Mbit/s.
	grün und orange	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und orange	blinkend	Datenverkehr mit 10 Mbit/s.

Das Leuchtverhalten der LEDs können Sie im Menü **Globale Einstellungen** und mit dem **WLAN Controller** in drei verschiedene Betriebsarten schalten.



Hinweis

Wenn Sie das LED-Verhalten über das **GUI** oder den **WLAN Controller** angepasst haben, bleibt diese Einstellung nach einem Wiederherstellen des Auslieferungszustands erhalten.

Status	Die LEDs zeigen ihr Standardverhalten.
Blinkend	Nur die Status-LED blinkt einmal in der Sekunde.
Aus	Alle LEDs sind deaktiviert.

1.2.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Dokumentation
bintec WI1003n	Ethernet-Kabel (RJ-45, STP) 2 x externe RSMA-Standardantennen Selbstklebende Füße Wand- bzw. Deckenbefestigung	Installationsposter Sicherheitshinweise

1.2.5 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	ca. 150 x 120 x 41 mm
Gewicht	ca. 750 g (mit WLAN-Modulen)
LEDs	1x Status, 2x WLAN
Leistungsaufnahme	ca. 6,5 W
Spannungsversorgung	9-12 V/1 A DC ; 100-240 V AC Steckernetzteil mit EU-Stecker (Das Steckernetzteil mit der Artikelnummer 5500001254 ist als Zubehör erhältlich) PoE an Ethernet 1 Class 0, gemäß 802.3af (max. 12,4 W). Der Gigabit PoE Injector mit der Artikelnummer 5530000082 ist als Zubehör erhältlich.
Schutzklasse	IP40 geschützt für Industrieanwendungen
Umweltanforderungen:	
Umgebungstemperatur	-20 °C bis +50 °C
Relative Luftfeuchtigkeit	10 % bis 100 %
Verfügbare Schnittstellen:	
WLAN	1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2
Ethernet IEEE 802.3 LAN	2 x 10/100/1000 MBit/s, autosensing, auto MDI/MDIX
Vorhandene Buchsen:	
Ethernet-Schnittstelle	2 RJ45-Buchsen
Antennen:	
Antennenanschluss	Zwei externe, rundstrahlende Antennen mit RSMA Anschluß. Die Antennen unterstützen 2,4 und 5 GHz. Antennengewinn ca. 2dBm.
Richtlinien & Normen	Directive 2014/53/EU, 2011/65/EU, 2009/125/EU, EN 60950-1; EN 62311; EN 301489-1; EN301489-17; EN 300 328; EN 301893; EN 50581
Taster	Reset-Taster für Neustart oder Reset

1.2.6 Reset

Im Falle einer Fehlkonfiguration oder bei Nichterreichbarkeit Ihres Geräts können Sie das Gerät mit dem Reset-Knopf auf der Geräteunterseite mit den Standardeinstellungen des Auslieferungszustands starten lassen.

Dabei werden alle bestehenden Konfigurationsdaten gelöscht.

- (1) Drücken Sie die **Reset**-Taste Ihres Geräts.
- (2) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt.
- (3) Achten Sie auf die LEDs:
Die Status-LED leuchtet, das Gerät durchläuft die Boot-Sequenz.
Lassen Sie **Reset**-Taste los, wenn die Status-LED wieder zu blinken beginnt.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 31 beschrieben.



Hinweis

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



Hinweis

Wenn sie das LED-Verhalten im Menü **Globale Einstellungen** oder mit dem **WLAN Controller** auf einen anderen als den Standardwert gesetzt haben, bleibt diese Einstellung beim Zurücksetzen des Geräts erhalten.

1.3 bintec W2003ac und bintec W2003ac-ext

1.3.1 Aufstellen und Anschließen

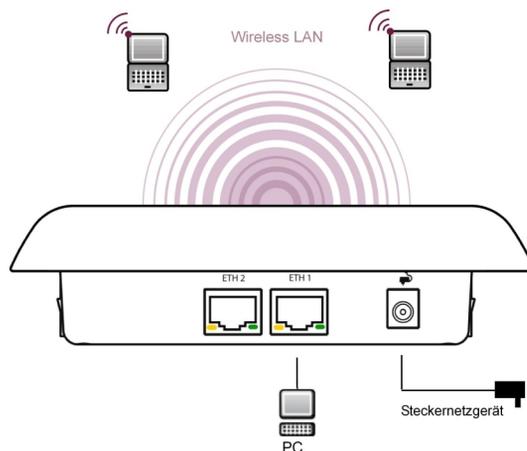


Hinweis

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

Das Gerät **bintec W2003ac** besitzen integrierte Antennen, deren Abstrahlcharakteristik für die Deckenmontage optimiert ist.

Das Gerät **bintec W2003ac-ext** verwendet externe Antennen.



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

(1) Antennen

Bei **bintec W2003ac-ext** schrauben Sie die Standardantennen (Zubehör) auf die dafür vorgesehenen Anschlüsse. Falls Sie andere Antennen verwenden, beachten Sie, dass SIMO-Antennen am Anschluss Ant1 und MIMO-Antennen an den Anschlüssen Ant1 und Ant2 anzuschließen sind.

(2) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN..

Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

Wählen Sie hier lediglich einen der Anschlüsse **ETH1** oder **ETH2**, der zweite Anschluss dient der Kaskadierung mehrerer Geräte. Bei Verwendung beider Ethernet-Anschlüsse am selben Switch können sich Loops bilden.

Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(3) Stromanschluss



Hinweis

Die Geräte werden ohne Steckernetzteil geliefert. Das Steckernetzteil mit EU-Stecker (Artikelnummer 5500001254) ist als Zubehör erhältlich.

Schließen Sie das Gerät an eine Steckdose an. Nehmen Sie dazu das Steckernetzteil und stecken Sie es in die dafür vorgesehene Buchse Ihres Geräts. Stecken Sie nun den Netzstecker in eine Steckdose (100–240 V). Durch die Status-LED wird Ihnen signalisiert, dass Ihr Gerät korrekt an die Stromversorgung angeschlossen ist. Optional kann die Stromversorgung über ein Standard PoE-Injector (Artikelnummer

5530000082) erfolgen.

Montage

Die Access Points sind wahlweise an die Wand oder an die Decke zu montieren oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

Befestigen Sie die vier selbstklebenden Füße auf der unteren Seite des Gerätes. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wand- / Deckenmontage

Um die Geräte an der Wand bzw. Decke zu montieren, verwenden Sie die Halterung, die im Lieferumfang enthalten ist (Artikelnummer 5500001278).

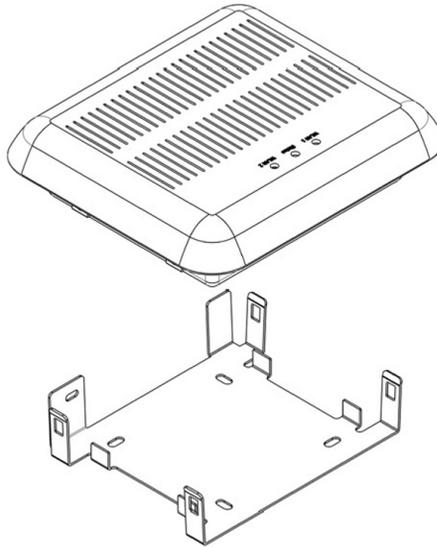
Mittels eines Kensington-Schlusses können die Geräte gegen Diebstahl gesichert werden.



Warnung

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

- Schrauben Sie die Halterung an der Wand bzw. Decke fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät ggf. mit einem Kensington-Schloss gegen Diebstahl.



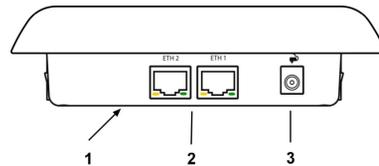
Deckenmontage

1.3.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

bintec W2003ac und **bintec W2003ac-ext** verfügen über zwei Ethernet-Anschlüsse.

Die Anschlüsse sind folgendermaßen angeordnet:



bintec W2003ac und **bintec W2003ac-ext** Unterseite

1	RESET	Reset-Taste führt Neustart durch (an der Bodenplatte des Geräts)
2	ETH1/PoE und ETH2	10/100/1000 Base-T Ethernet-Schnittstelle
3	POWER	Buchse für Steckernetzteil

1.3.3 LEDs

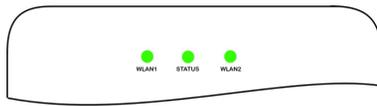
Anhand der LEDs können Sie Funkstatus und Funkaktivität Ihres Geräts erkennen.



Hinweis

Beachten Sie, dass die Anzahl der aktiven WLAN LEDs abhängig ist von der Anzahl der vorhandenen Radiomodule.

Die LEDs sind folgendermaßen angeordnet:



Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
Status	grün	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.
		an (statisch)	Fehler
		blinkend	Betriebsbereit
WLAN 1/2	grün	aus	Radiomodul oder alle zugeordneten VSS deaktiviert.
		langsam blinkend	VSS ist aktiv, kein Client angemeldet.
		schnell blinkend	VSS ist aktiv, mindestens 1 Client ist angemeldet.
		flackernd	VSS ist aktiv, mindestens 1 Client ist angemeldet, es besteht Datenverkehr.
ETH 1/2	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
		blinkend	Datenverkehr mit 1 Gbit/s.
	orange	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
		blinkend	Datenverkehr mit 100 Mbit/s.
		grün und orange	an

LED	Farbe	Status	Information
	grün und orange	blinkend	Datenverkehr mit 10 Mbit/s.

Das Leuchtverhalten der LEDs können Sie im Menü **Globale Einstellungen** und mit dem **WLAN Controller** in drei verschiedene Betriebsarten schalten.



Hinweis

Wenn Sie das LED-Verhalten über das **GUI** oder den **WLAN Controller** angepasst haben, bleibt diese Einstellung nach einem Wiederherstellen des Auslieferungszustands erhalten.

Status	Die LEDs zeigen ihr Standardverhalten.
Blinkend	Nur die Status-LED blinkt einmal in der Sekunde.
Aus	Alle LEDs sind deaktiviert.

1.3.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Dokumentation
bintec W2003ac	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße Wand- bzw. Deckenbefestigung	Installationsposter Sicherheitshinweise
bintec W2003ac-ext	Ethernet-Kabel (RJ-45, STP) 4 externe RSMA-Standardantennen Selbstklebende Füße Wand- bzw. Deckenbefestigung	Installationsposter Sicherheitshinweise

1.3.5 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	ca. 159 x 145 x 43 mm
Gewicht	ca. 1000 g (mit WLAN-Modulen)
LEDs	4 (1x Status, 2x WLAN, 2x Ethernet)
Leistungsaufnahme Gerät	max. 12,4 Watt
Spannungsversorgung	230 V / 9-12 V DC, 1 A (Das Steckernetzteil mit der Artikelnummer 5500001254 ist als Zubehör erhältlich) PoE an Ethernet 1 Class 0, gemäß 802.3af (max. 12,4 W). Der Gigabit PoE Injector mit der Artikelnummer 5530000082 ist als Zubehör erhältlich.
Umweltanforderungen:	
Lagertemperatur	-10 °C bis +70 °C
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 95 % (nichtkondensierend)
Verfügbare Schnittstellen:	
WLAN	bintec W2003ac: 1 Radiomodul 802.11bgn 2,4 GHz Mimo 2x2; 1 Radiomodul 802.11an 5 GHz Mimo 2x2 bintec W2003ac-ext: 1 Radiomodul 802.11abgn 2,4 oder 5 GHz Mimo 2x2; 1 Radiomodul 802.11abgn 2,4 oder 5 GHz Mimo 2x2
Ethernet IEEE 802.3 LAN	2 x 10/100/1000 MBit/s Ethernet Twisted Pair, autosensing, Auto MDI/MDI-X
Vorhandene Buchsen:	
Ethernet-Schnittstelle	2 RJ45-Buchsen
Antennen:	
Antennenanschluss	bintec W2003ac: 4 interne Antennen bintec W2003ac-ext: 4 externe Dualband-Antennen
Sendeleistung (WLAN)	max. 100 mW (20 dBm) EIRP
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371
Taster	Reset-Taster für Neustart oder Reset

1.3.6 Reset

Im Falle einer Fehlkonfiguration oder bei Nichterreichbarkeit Ihres Geräts können Sie das Gerät mit dem Reset-Knopf auf der Geräteunterseite mit den Standardeinstellungen des Auslieferungszustands starten lassen.

Dabei werden alle bestehenden Konfigurationsdaten gelöscht.

- (1) Drücken Sie die **Reset**-Taste Ihres Geräts.
- (2) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt.
- (3) Achten Sie auf die LEDs:
Die Status-LED leuchtet, das Gerät durchläuft die Boot-Sequenz.
Lassen Sie **Reset**-Taste los, wenn die Status-LED wieder zu blinken beginnt.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 31 beschrieben.



Hinweis

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



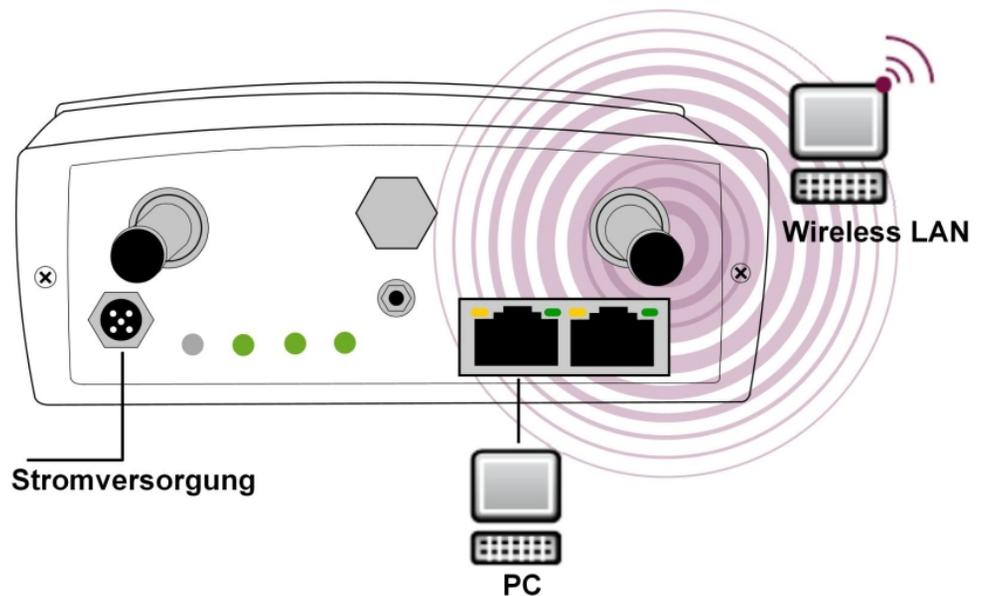
Hinweis

Wenn sie das LED-Verhalten im Menü **Globale Einstellungen** oder mit dem **WLAN Controller** auf einen anderen als den Standardwert gesetzt haben, bleibt diese Einstellung beim Zurücksetzen des Geräts erhalten.

1.4 bintec WO1003ac und bintec WO2003ac

1.4.1 Aufstellen und Anschließen

Die Geräte **bintec WO1003ac** und **bintec WO2003ac** verwenden externe Antennen.



Anschlussmöglichkeiten **bintec WO2003ac**

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

(1) Antennen

Schrauben Sie die Standardantennen (Zubehör) auf die dafür vorgesehenen Anschlüsse. Radiomodul 1 hat die Anschlüsse 1-1 und 1-2; Radiomodul 2 hat die Anschlüsse 2-1 und 2-2.

Schließen Sie die Standardantennen (MIMO) nur an einem Antennenanschluss. Beachten Sie bitte, bei der Konfiguration den zweiten Stream zu deaktivieren. Falls Sie andere Antennen verwenden, beachten Sie bitte, dass die Antennen an den Anschlüssen der entsprechenden Modulen anzuschließen sind.

(2) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN.



Hinweis

Beachten Sie, dass es zwar möglich ist einen Standard-RJ45-Stecker in den LAN-Anschluss des Gerätes zu stecken, dieser aber nur schwer wieder entfernt werden kann. Wir empfehlen die Verwendung des mitgelieferten Anschluss-Kits.

Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.

Wählen Sie hier lediglich einen der Anschlüsse **ETH1** oder **ETH2**, der zweite Anschluss dient der Kaskadierung mehrerer Geräte. Bei Verwendung beider Ethernet-

Anschlüsse am selben Switch können sich Loops bilden.

Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(3) Stromanschluss



Hinweis

Die Geräte werden ohne Steckernetzteil geliefert. Das Steckernetzteil mit EU-Stecker ist als Zubehör erhältlich. Die Geräte sind zu erden.



Warnung

Zur Leistungsbegrenzung im Fehlerfall ist der DC Versorgungsstromkreis installationsseitig mit einer externen 5 A-Sicherung abzusichern.



Warnung

Die Geräte sollen mit Blitz- und Überspannungsschutz ausgestattet sein.

Schließen Sie das Gerät an die vorgesehene Stromversorgung an. Durch die Status-LED wird Ihnen signalisiert, dass Ihr Gerät korrekt an die Stromversorgung angeschlossen ist. Optional kann die Stromversorgung über ein Standard PoE-Injector (Artikelnummer 5530000082) erfolgen.



Hinweis

Das Gerät verfügt nicht über einen Netzschalter. Um die Spannungsversorgung zu unterbrechen können Sie entweder den M12-Stecker entfernen oder die externe Sicherung entfernen bzw. anderweitig unterbrechen. Wird das Gerät mittels PoE versorgt, können Sie entweder das PoE-Kabel vom ETH1-Anschluss trennen oder die PoE-Versorgung abschalten (z. B. im Switch).

Montage

Die Access Points sind wahlweise an die Wand oder am Mast montierbar.



Wichtig

Wählen Sie den Installationsstandort sorgfältig aus. Um Schutz vor hoch wachsenden Pflanzen zu gewährleisten, muss das Gerät mindestens einen Meter über dem Boden montiert werden.

Die Umgebungstemperatur darf 60°C nicht überschreiten. Vermeiden Sie direkte Sonneneinstrahlung und achten Sie auf ausreichende Kühlung.

Für die Befestigung der Geräte an der Wand, verwenden Sie die Wandbefestigung die im Lieferumfang enthalten ist.

Für die Befestigung der Geräte am Mast, verwenden Sie den Montage Kit der als Zubehör erhältlich ist (Artikelnummer 5520000144). Optional ist auch ein Diebstahlschutz (Kensington-Schloss) erhältlich.



Warnung

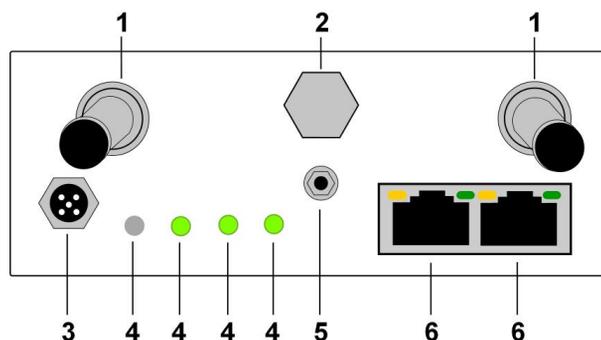
Vergewissern Sie sich vor dem Bohren, dass sich an der Bohrstelle keine Hausinstallationen befinden. Bei Beschädigung an Gas-, Strom-, Wasser- und Abwasserleitungen kann Lebensgefahr oder Sachschaden entstehen.

- Schrauben Sie die Halterung an der Wand bzw. Mast fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät ggf. mit einem Kensington-Schloss gegen Diebstahl.

1.4.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

Die Anschlüsse sind folgendermaßen angeordnet:



Anschlüsse bintec WO1003ac / bintec WO2003ac

1	Ant 1-1/1-2	Typ N Antennenanschlüsse
	Ant 2-1/2-2	Die Geräte bintec WO2003ac haben zwei weitere Anschlüsse auf der Oberseite des Gerätes.

2	Luftventil	Reguliert internen / externen Luftdruck im gesamten Temperaturbereich
3	Power	Buchse für Steckernetzteil - PoE wird an Ethernet-Port 1 unterstützt.
4	LEDs	Leuchtanzeige für Status und WLAN
5	Erdung	Anschluss für die Erdung
6	ETH1 / ETH2	10/100/1000 Base-T Ethernet-Schnittstelle; PoE wird an ETH1 unterstützt

1.4.3 LEDs

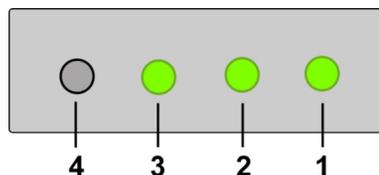
Anhand der LEDs können Sie Funkstatus und Funkaktivität Ihres Geräts erkennen.



Hinweis

Beachten Sie, dass die Anzahl der aktiven WLAN LEDs abhängig ist von der Anzahl der vorhandenen Radiomodule.

Die LEDs sind folgendermaßen angeordnet:



LEDs von **bintec WO1003ac** / **bintec WO2003ac**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Farbe	Status	Information
1 = Status	grün	an	Nach dem Einschalten: Gerät wird gestartet. Während des Betriebs: Ein Fehler ist aufgetreten.
	grün	blinkend	Das Gerät ist aktiv.
	gün	aus	Während des Betriebs: Ein Fehler ist aufgetreten.
2 = WLAN1	grün	an	WLAN-Verbindung hergestellt.

LED	Farbe	Status	Information
	grün	aus	Radiomodul oder alle zugeordneten Drahtlosnetzwerke deaktiviert.
	grün	langsam blinkend	Drahtlosnetzwerk ist aktiv, kein Client angemeldet.
	grün	schnell blinkend	Drahtlosnetzwerk ist aktiv, mindestens 1 Client ist angemeldet .
3 = WLAN2	grün	an	WLAN-Verbindung hergestellt.
	grün	aus	Radiomodul oder alle zugeordneten Drahtlosnetzwerke deaktiviert.
	grün	langsam blinkend	Drahtlosnetzwerk ist aktiv, kein Client angemeldet.
	grün	schnell blinkend	Drahtlosnetzwerk ist aktiv, mindestens 1 Client ist angemeldet .
4	inaktiv	./.	./.
ETH 1/2	grün	an	Das Gerät ist an das Ethernet angeschlossen mit 1 Gbit/s.
	grün	blinkend	Datenverkehr mit 1 Gbit/s.
	orange	an	Das Gerät ist an das Ethernet angeschlossen mit 100 Mbit/s.
	orange	blinkend	Datenverkehr mit 100 Mbit/s.
	grün und orange	an	Das Gerät ist an das Ethernet angeschlossen mit 10 Mbit/s.
	grün und orange	blinkend	Datenverkehr mit 10 Mbit/s.

Das Leuchverhalten der LEDs können Sie im Menü **Globale Einstellungen** und mit dem **WLAN Controller** in drei verschiedene Betriebsarten schalten.



Hinweis

Wenn Sie das LED-Verhalten über das **GUI** oder den **WLAN Controller** angepasst haben, bleibt diese Einstellung nach einem Wiederherstellen des Auslieferungszustandes erhalten.

Status	Die LEDs zeigen ihr Standardverhalten.
Blinkend	Nur die Status-LED blinkt einmal in der Sekunde.

Aus	Alle LEDs sind deaktiviert.
-----	-----------------------------

1.4.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Dokumentation
bintec WO1003ac / bintec WO2003ac	RJ Industrial Cat. 6a IP65-Stecker Wandbefestigung	Installationsposter Sicherheitshinweise (gedruckt)

1.4.5 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (L x B x H)	bintec WO1003ac: 173 x 176 x 72 mm bintec WO2003ac: 140 x 178 x 66 mm
Gewicht	ca. 1300 g
LEDs	1x Status, 2x WLAN
Typische Leistungsaufnahme	bintec WO1003ac: ca. 6,5 Watt bintec WO2003ac: ca. 8,7 Watt
Leistungsaufnahme in networked standby	bintec WO1003ac: 4,8 W (nach 5 Minuten Inaktivität) bintec WO2003ac: 7,3 W (nach 5 Minuten Inaktivität)
Stromversorgungsbereich (DC)	Die Geräte sind zu erden. 9-36 V max. 1,4 A mit Überspannungsschutz, galvanisch getrennt
Stromversorgung	12 - 24 Volt Stromversorgung (M12 Buchse) erforderlich oder PoE nach 802.3af oder 802.3at (Netzteil oder PoE Injektor nicht im Lieferumfang)
Umweltanforderungen:	
IP-Schutzklasse	IP65, geschützt gegen Eindringen von Staub und Wasser

Eigenschaft	Wert
Lagertemperatur	-40 °C bis +85 °C
Zulässige Umgebungstemperatur	-25 °C bis +60 °C
Relative Luftfeuchte	10 % bis 100 %
Verfügbare Schnittstellen:	
WLAN	bintec WO1003ac : 1 Radiomodul 802.11ac/abgn bintec WO2003ac : 2 Radiomodule 802.11ac/abgn
Ethernet IEEE 802.3 LAN	2 x 10/100/1000 MBit/s, autosensing, auto MDI/MDIX
Verfügbare Buchsen:	
Ethernet-Schnittstelle	Zwei wassergeschützte RJ-45 Harting Push Pull (HPP V4 RJ45 GL) Buchsen
Antennen:	
Antennenanschluss	bintec WO1003ac : 2 externe Dualband-Antennen; Zwei wassergeschützte N-Antennenbuchsen bintec WO2003ac : 4 externe Dualband-Antennen; Vier wassergeschützte N-Antennenbuchsen
Richtlinien & Normen	CE-Kennzeichnung Directive 2014/53/EU, 2011/65/EU, 2009/125/EU, EN 60950, EN 62311, EN 301489, EN 300328, EN 301893, EN 50581

1.4.6 Reset

Es gibt einen Halleffektschalter / -sensor für die Rücksetzfunktion. Führen Sie einen Magneten in der Nähe des Reset-Schalters entlang, der sich zwischen den Ethernet-Anschlüssen und den LEDs befindet, um einen Reset auszulösen. Halten Sie den Magneten solange an die entsprechende Stelle, bis die Status-LED nach ca. 30 Sekunden wieder gleichmäßig blinkt.



Hinweis

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



Hinweis

Wenn sie das LED-Verhalten auf einen anderen als den Standardwert gesetzt haben, bleibt diese Einstellung beim Zurücksetzen des Geräts erhalten.

1.5 Reinigen

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

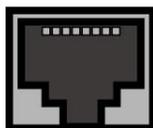
1.6 Pin-Belegung

1.6.1 Ethernet-Schnittstelle

Die Geräte **bintec W2003ac**, **bintec W2003ac-ext**, **bintec WI1003n**, **bintec WO1003ac** und **bintec WO2003ac** verfügen über zwei 10/100/1000 Ethernet-Schnittstellen, **bintec W1001n** und **bintec W1003n** haben eine 10/100/1000 Ethernet-Schnittstelle.

Der Anschluss erfolgt über eine RJ45-Buchse.

1 8



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

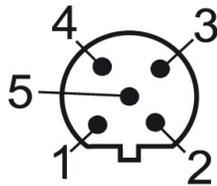
RJ45-Buchse für LAN-Anschluss

Pin	Funktion
1	Pair 0 +
2	Pair 0 -
3	Pair 1 +
4	Pair 2 +
5	Pair 2 -

Pin	Funktion
6	Pair 1 -
7	Pair 3 +
8	Pair 3 -

1.6.2 Stromversorgung

Die Geräte **bintec WO1003ac** und **bintec WO2003ac** verfügen über eine Buchse für die Stromversorgung.



Netzanschluss-Buchse

Pin	Funktion
1	TxD - Ausgehende Serielle Schnittstelle
2	VCC+ - Positive Stromversorgung
3	VCC- - Negative Stromversorgung
4	RxD - Eingehende Serielle Schnittstelle
5	GND - GND Serielle Schnittstelle

1.7 Frequenzen und Kanäle

Weltweit gelten unterschiedliche Zulassungsbestimmungen. Im Wesentlichen gelten die ETSI Vorschriften (kommt hauptsächlich in Europa zur Anwendung). Für den Betrieb in Europa lesen Sie bitte die Hinweise in der R&TTE Compliance Information.

1.8 Support Information

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

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

Kapitel 2 Grundkonfiguration

Zur Grundkonfiguration Ihres Geräts stehen das **GUI** (Einzelkonfiguration), der **Wireless LAN Controller** und der **Clou NetManager** (Konfiguration mit Konfigurationsdiensten) zur Verfügung.

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

Die Inhalte dieses Handbuches setzen die folgenden Basiskenntnisse voraus:

- Basiskenntnisse im Netzwerkaufbau,
- Kenntnisse über die grundlegende Netzwerkterminologie, wie beispielsweise Server, Client und IP-Adresse,
- Grundkenntnisse bei der Bedienung von Microsoft Windows Betriebssystemen.

Weitere nützliche Applikationen finden Sie im Internet unter www.bintec-elmeg.com.

2.1 Voreinstellungen

2.1.1 Vorkonfigurierte Daten

Sie haben drei Möglichkeiten, in Ihrem Netzwerk auf Ihr Gerät zur Konfiguration zuzugreifen:

(a) Dynamische IP-Adresse

Im Auslieferungszustand ist Ihr Gerät im DHCP-Client-Modus eingestellt, d.h. es erhält bei Anschluss an das Netzwerk automatisch eine IP-Adresse, sofern ein DHCP-Server betrieben wird. Ihr Gerät ist zur Konfiguration dann unter der vom DHCP-Server vergebenen IP-Adresse erreichbar. Zur Ermittlung der dynamisch vergebenen IP-Adresse lesen Sie bitte die Dokumentation Ihres DHCP-Servers.

(b) Fallback-IP-Adresse

Sollten Sie keinen DHCP-Server betreiben, können Sie Ihr Gerät direkt an Ihren Konfigurations-PC anschliessen und erreichen es dann unter folgender vordefinierter Fallback-IP-Konfiguration:

- **IP-Adresse:** *192.168.0.252*
- **Netzmaske:** *255.255.255.0*

Achten Sie darauf, dass der PC, von dem aus die Konfiguration durchgeführt wird,

über eine geeignete IP-Konfiguration verfügt (siehe dazu [PC einrichten](#) auf Seite 34).

(c) Feste IP-Adresse zuweisen



Hinweis

Beachten Sie bitte:

Hat Ihr Gerät bei der Erstkonfiguration dynamisch von einem in Ihrem Netzwerk betriebenen DHCP-Server eine IP-Adresse erhalten, wird die Fallback-IP-Adresse 192.168.0.252 automatisch gelöscht und Ihr Gerät ist darüber nicht mehr erreichbar.

Sollten sie dagegen bei der Erstkonfiguration eine Verbindung zum Gerät über die Fallback-IP-Adresse 192.168.0.252 aufgebaut haben, ist es nur noch über diese IP-Adresse erreichbar. Es kann nicht mehr dynamisch über DHCP eine IP-Konfiguration erhalten.

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

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



Hinweis

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

Die Vorgehensweise bei der Änderung von Passwörtern finden Sie unter [Systempasswort ändern](#) auf Seite 37.

2.1.2 Software-Update

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

Eine Beschreibung des Update-Vorgangs finden Sie unter [Softwareaktualisierung](#) auf Seite 39

.

2.2 System-Voraussetzungen

Für die Konfiguration 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)
- hohe Farbanzeige für die korrekte Darstellung der Grafiken
- Installiertes TCP/IP-Protokoll (siehe [PC einrichten](#) auf Seite 34)

2.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

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

2.3.1 Daten sammeln

Die wesentlichen Daten für die Grundkonfiguration haben Sie schnell gesammelt, denn es sind keine Informationen erforderlich, die vertiefte Netzwerkkennnisse voraussetzen. Ggf. können Sie die Beispielwerte übernehmen.

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

- IP-Konfiguration (obligatorisch sofern sich Ihr Gerät im Auslieferungszustand befindet)
- optional: Konfiguration einer drahtlosen Netzwerkverbindung im Access-Point-Modus
- optional: Konfiguration von Client Links im Client Links-Modus

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

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

Grundkonfiguration

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

IP-Konfiguration des Access Points

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Access Points	<i>192.168.0.252</i>	
Netzmaske Ihres Access Points	<i>255.255.255.0</i>	

Access-Point-Modus

Wenn Sie Ihr Gerät im Access-Point-Modus betreiben, können Sie die gewünschten Drahtlosnetzwerke einrichten. Hierzu benötigen Sie jeweils folgende Daten:

Konfiguration eines Drahtlosnetzwerks

Zugangsdaten	Beispielwert	Ihre Werte
Netzwerkname (SSID)	<i>default</i>	
Sicherheitsmodus	<i>WPA-PSK</i>	
Preshared Key	<i>supersecret</i>	

Access Client-Modus

Wenn Sie Ihr Gerät im Access Client-Modus betreiben, können Sie die gewünschten Client Links einrichten. Hierzu benötigen Sie jeweils folgende Daten:

IP-Konfiguration des Access Clients

Zugangsdaten	Beispielwert	Ihre Werte
Netzwerkname (SSID)	<i>default</i>	
Sicherheitsmodus	<i>WPA-PSK</i>	
Preshared Key	<i>supersecret</i>	

2.3.2 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.
- Wählen Sie die geeignete IP-Konfiguration für Ihren Konfigurations-PC.

Der PC, über den Sie die IP-Adresse für Ihr Gerät konfigurieren möchten, muss sich im

gleichen Netzwerk wie das zu konfigurierende Gerät befinden.

Windows TCP/IP-Protokoll prüfen

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

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

Windows TCP/IP-Protokoll installieren

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

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

PC IP-Adresse zuweisen

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

- (1) Wählen Sie **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
- (2) Wählen Sie **Folgende IP-Adresse verwenden** und geben Sie eine geeignete IP-Adresse, die passende Netzmaske, Ihr Standardgateway und Ihren bevorzugten DNS-Server ein.

Wenn Sie in Ihrem Netzwerk einen DHCP-Server betreiben, können Sie die Windows-StandardEinstellung **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** belassen.

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

2.4 IP-Konfiguration

Im Auslieferungszustand ist Ihr Gerät im DHCP-Client-Modus eingestellt und erhält somit dynamisch eine IP-Adresse, sofern Sie einen DHCP-Server in Ihrem Netzwerk betreiben. Wenn das nicht der Fall ist, schliessen Sie Ihr Gerät direkt an den Konfigurations-PC an und verwenden die Fallback-IP-Adresse `192.168.0.252`.

Konfiguration mit Konfigurationsdiensten

Wireless LAN Controller: Der WLAN Controller verfügt über einen Wizard, der Sie bei der Konfiguration Ihrer Access Points unterstützt. Die Anzahl der Access Points, die Sie mit dem Wireless LAN Controller Ihres Gateways verwalten können, sowie die Information über die notwendigen Lizenzen entnehmen Sie bitte dem Datenblatt Ihres Geräts.

Bei Aufruf des **Wizard** erhalten Sie Anweisungen und Erläuterungen auf den einzelnen Assistentenseiten (siehe [Wireless LAN Controller](#) auf Seite 151).

Cloud NetManager: Mit dem Cloud NetManager können Sie die Access Points managen. Für jeden Access Point ist eine gültige Lizenz nötig.



Hinweis

Wenn Sie auf Ihrem Gerät bereits früher eine Konfiguration mit dem **Wireless LAN Controller** realisiert haben, müssen Sie Ihr Gerät vor der Verwendung des Cloud NetManagers in den Auslieferungszustand versetzen. Die aktuelle Boot-Konfiguration wird dabei gelöscht. Vergessen Sie nicht, diese gegebenenfalls zu exportieren und auf Ihrem PC zu speichern, falls Sie sie später wieder einsetzen wollen.

Wenn Sie den Cloud NetManager verwenden, so haben Sie auf die Menüs **Wireless LAN** und **Wireless LAN Controller** keinen Zugriff. Wenn Sie den Cloud NetManager verwenden wollen, müssen Sie den **Wireless LAN Controller** vorher deaktivieren. Ansonsten hat dieser Vorrang.

Der gleichzeitige Betrieb des Cloud NetManagers und des Wireless LAN Controllers ist aktuell nicht vorgesehen.

Im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **System** ist die Option **Kommunikation mit dem NetManager** *Aktiviert*. Im Feld **IP-Adresse des NetManagers** ist die Adresse des bintec elmeg Cloud NetManagers bereits vorkonfiguriert. Sollten Sie einen eigenen Manager betreiben wollen, müssen Sie hier die Adresse Ihres Servers eintragen.

Eine anwendungsbezogene Schritt-für-Schritt-Anleitung zur Verwendung des Cloud Net-

Managers finden Sie im separaten Handbuch **Anwendungs-Workshops**, das unter www.bintec-elmeg.com unter **Lösungen** zum Download bereitsteht.

GUI aufrufen

Starten Sie die Konfigurationsoberfläche wie folgt:

- (a) Geben Sie die IP-Adresse Ihres Geräts in die Adress-Zeile Ihres Web-Browsers ein.

Mit DHCP-Server:

- die IP-Adresse, die der DHCP-Server Ihrem Gerät vergeben hat

Ohne DHCP-Server:

- Bei Direktanschluss an den Konfigurations-PC: die Fallback-IP-Adresse
192.168.0.252

- (b) Geben Sie in das Feld **User** *admin* und in das Feld **Password** *admin* ein.
- (c) Klicken Sie auf **LOGIN**, um auf die Konfigurationsoberfläche zu gelangen.

2.5 Systempasswort ändern

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

Gehen Sie dazu vor wie folgt:

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

Beachten Sie folgende Regeln zum Passwortgebrauch:

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. sollten deshalb nicht als Passwörter gewählt werden.
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl).

- Das Passwort sollte mindestens 8 Zeichen lang sein.
- Wechseln Sie regelmäßig das Passwort, z. B. alle 90 Tage.

2.6 Drahtlosnetzwerk einrichten

Gehen Sie folgendermaßen vor, um ihr Gerät als Access Point zu nutzen:

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

WLAN-Adapter unter Windows XP konfigurieren

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

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

Fahren Sie folgendermaßen fort:

- (1) Bei **Netzwerkname** geben Sie z. B. *Client-1* ein.
- (2) Unter **Netzwerkauthentifizierung** wählen Sie *WPA2-PSK*.
- (3) Bei **Datenverschlüsselung** konfigurieren Sie *AES*.
- (4) Unter **Netzwerkschlüssel** und **Netzwerkschlüssel bestätigen** geben Sie den zuvor konfigurierten Preshared Key an.
- (5) Verlassen Sie die Menüs jeweils mit **OK**.



Hinweis

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

WLAN-Adapter unter Windows 7 konfigurieren

Windows 7 erkennt vorhandene WLAN-Netzwerke automatisch. Sie müssen Ihre Verbindung nur noch konfigurieren.

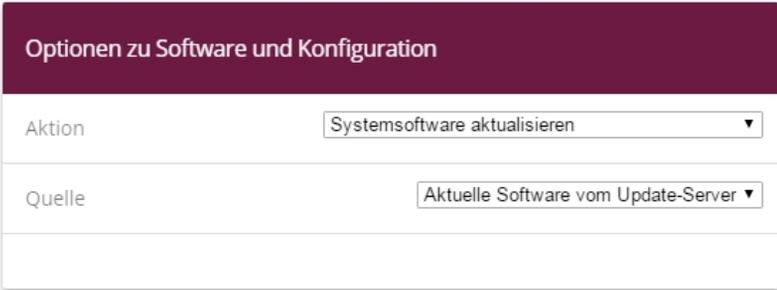
- (1) Klicken Sie zunächst auf das WLAN-Symbol im Infobereich der Taskleiste (Systemtray). Windows 7 zeigt Ihnen nun alle drahtlosen Netzwerke an, die sich in Ihrer Reichweite befinden.
- (2) Wählen Sie das WLAN-Netz Ihres Geräts aus und klicken Sie auf **Verbinden**.
- (3) Im sich anschließend öffnenden Fenster tragen Sie den zuvor konfigurierten Preshaed Key ein und bestätigen mit **OK**.

2.7 Softwareaktualisierung

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

Gehen Sie folgendermaßen vor:

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



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

START

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

en Software werden Sie zum Neustart des Geräts aufgefordert.



Achtung

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

Kapitel 3 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

3.1 Zugangsmöglichkeiten

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

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

- Über Ihr LAN

3.1.1 Zugang über LAN

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



Achtung

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

3.1.1.1 HTTP/HTTPS

Mit einem aktuellen Web-Browser können Sie die HTML-Oberflächen zur Konfiguration Ihres Geräts verwenden.

Die Konfiguration lässt sich mit dem **GUI** durchführen. Geben Sie dazu die IP-Adresse Ihres Geräts in das Adressfeld Ihres Web-Browsers ein:

Mit DHCP-Server:

- die IP-Adresse, die Ihr DHCP-Server Ihrem Gerät vergeben hat

Ohne DHCP-Server:

- Bei Direktanschluss an den Konfigurations-PC: die Fallback-IP-Adresse

192.168.0.252

3.1.1.2 Telnet

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

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

Gehen Sie folgendermaßen vor:

Windows

- (1) Klicken Sie im Windows-Startmenü auf **Ausführen...**
- (2) Geben Sie `telnet <IP-Adresse Ihres Geräts>` ein.
- (3) Klicken Sie auf **OK**.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (4) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 46.

Unix

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

- (1) Geben Sie `telnet <IP-Adresse Ihres Geräts>` in ein Terminal ein.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (2) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 46.

3.1.1.3 SSH

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

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

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

Schlüssel zur Verschlüsselung

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

- (1) Loggen Sie sich auf eine der bereits verfügbaren Arten auf Ihrem Gerät ein (z. B. über Telnet - zum Login siehe [Anmelden](#) auf Seite 45).
- (2) Am Eingabe-Prompt geben Sie `update -i` ein. Sie befinden sich auf der Flash Management Shell.
- (3) Rufen Sie eine Liste aller auf dem Gerät gespeicherten Dateien auf: `ls -al`.

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

```
Flash-Sh > ls -al

Flags Version Length Date Name...

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

Flash-Sh >
```



Hinweis

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

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

- (1) Verlassen Sie die Flash Management Shell mit `exit`.
- (2) Rufen Sie das **GUI** auf und melden Sie sich an Ihrem Gerät an (siehe [Die Konfigurationsoberfläche aufrufen](#) auf Seite 48).
- (3) Stellen Sie sicher, dass als Sprache *Deutsch* gewählt ist.
- (4) Kontrollieren Sie den Schlüsselstatus im Menü **Systemverwaltung->Administrativer Zugriff->SSH**. Wenn beide Schlüssel verfügbar sind, sehen Sie in den beiden Feldern **RSA-Schlüsselstatus** und **DSA-Schlüsselstatus** den Wert *Generiert*.
- (5) Wenn Sie in einem der beiden Felder oder in beiden Feldern den Wert *Nicht gene-*

riert sehen, so müssen Sie den entsprechenden Schlüssel erzeugen lassen. Um die Schlüssel vom Gerät erzeugen zu lassen, klicken Sie auf **Generieren**.

Das Gerät erzeugt den entsprechenden Schlüssel und speichert ihn im FlashROM. *Generiert* zeigt die erfolgreiche Generierung an.

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

Login über SSH

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

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

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

UNIX

- (1) Geben Sie `ssh <IP-Adresse des Geräts>` in einem Terminal ein.
Das Login-Prompt-Fenster wird angezeigt, sie befinden sich auf der SNMP-Shell des Geräts.
- (2) Fahren Sie mit *Anmelden* auf Seite 45 fort.

Windows

- (1) Wie eine SSH-Verbindung aufgebaut wird, hängt stark von der verwendeten Software ab. Beachten Sie die Dokumentation des von Ihnen verwendeten Programms.
Sobald Sie sich mit dem Gerät verbunden haben, wird das Login-Prompt-Fenster angezeigt. Sie befinden sich auf der SNMP-Shell des Geräts.
- (2) Fahren Sie mit *Anmelden* auf Seite 45 fort.



Hinweis

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

3.2 Anmelden

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

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

3.2.1 Benutzernamen und Passwörter im Auslieferungszustand

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

Benutzernamen und Passwörter im Auslieferungszustand

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

Um Konfigurationsänderungen vorzunehmen und zu speichern, müssen Sie sich mit dem Benutzernamen `admin` einloggen. Auch die Zugangsdaten (Benutzernamen und Passwörter) können geändert werden, wenn sich der Benutzer mit dem Benutzernamen `admin` einloggt.

Ein Sicherheitskonzept Ihres Geräts besteht darin, dass Sie mit dem Benutzernamen `read` alle anderen Konfigurationseinstellungen lesen können, nicht aber die Zugangsdaten. Es ist also nicht möglich, sich mit `read` einzuloggen, das Passwort des Benutzers `admin` auszulesen und sich dann anschließend mit `admin` einzuloggen, um Konfigurationsänderungen vorzunehmen.



Achtung

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

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

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

3.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in [Zugangsmöglichkeiten](#) auf Seite 41 beschrieben.

GUI (Graphical User Interface)

So loggen Sie sich über die HTML-Oberfläche ein:

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

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

SNMP-Shell

So loggen Sie sich auf der SNMP-Shell ein:

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

Ihr Gerät meldet sich mit dem Eingabeprompt, z. B. `w1002:>`. Das Einloggen war erfolgreich. Sie befinden sich auf der SNMP-Shell.

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

3.3 Konfigurationsmöglichkeiten

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

Sie haben folgende Möglichkeiten, Ihr Gerät zu konfigurieren:

- **GUI**

- Assistent
- SNMP-Shell-Kommandos

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

Verbindungs- und Konfigurationsarten

Verbindungsart	Mögliche Konfigurationsarten
LAN	Assistent, GUI , Shell-Kommandos



Hinweis

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

3.3.1 GUI (Graphical User Interface) für Fortgeschrittene

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

Mit dem **GUI** können Sie alle Konfigurationsaufgaben einfach und komfortabel durchführen. Es ist in Ihr Gerät integriert und steht in Englisch zur Verfügung. Weitere Sprachen können, falls erwünscht im Download-Bereich auf www.bintec-elmeg.com heruntergeladen und auf dem Gerät installiert werden.

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

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

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

Systeminformationen		Ressourceninformationen	
Uptime	2 Tag(e) 6 Stunde(n) 8 Minute(n)	CPU-Nutzung	0%
Systemdatum	Sonntag, 25 Jan 2004, 07:08:45	Arbeitsspeichernutzung	56.5/127.9 MByte (44%)
Seriennummer	RN08ELC15240005	Aktive IPSec-Tunnel	0 / 0
BOSS-Version	V.10.1.21.2 IPv6, IPSec from 2016/06/22 00:00:00		
Letzte gespeicherte Konfiguration	Freitag, 30 Jan 2004, 11:22:44		

Physikalische Schnittstellen			WAN-Schnittstellen			
Schnittstelle	Verbindungsinformation	Link	Beschreibung	Verbindungsinformation	Uptime	Link
en1-0	br0:192.168.0.110 / 255.255.255.0	✓				
en1-1	br0:192.168.0.110 / 255.255.255.0	✗				
WLAN1	Access-Point / Verwendeter Kanal - / 0 Clients / 0 WDS-Links / FW:qsdk10.2.4	✗				
WLAN2	Access-Point / Verwendeter Kanal - / 0 Clients / 0 WDS-Links / FW:qsdk10.2.4	✗				

3.3.1.1 Die Konfigurationsoberfläche aufrufen

- Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind.
- Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe [PC einrichten](#) auf Seite 34).
- Öffnen Sie einen Web-Browser.
- Geben Sie `http://192.168.0.252` (oder die von Ihrem DHCP-Server dynamisch vergebene IP-Adresse) in das Adressfeld des Web-Browsers ein.
- Geben Sie in das Feld **User** `admin` und in das Feld **Password** `admin` ein und klicken Sie auf **LOGIN**.

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

3.3.1.2 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 web interface for a bintec W2003ac device. On the left is a dark red navigation menu with the following items: Assistenten, Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Wireless LAN Controller, Netzwerk, Routing-Protokolle, Multicast, WAN, VPN, Firewall, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. At the top right is a header bar (Kopfleiste) containing the device name 'bintec W2003ac', the bintec elmeg logo, and options for 'SPRACHE Ansicht Standard' and 'KONFIGURATION SPEICHERN'. Below the header is the main configuration area (Hauptkonfigurationsfenster) with sections for 'Systempasswort' (containing fields for 'Systemadministrator-Kennwort' and 'Systemadministrator-Kennwort bestätigen'), 'SNMP-Communities' (containing fields for 'SNMP Read Community' and 'SNMP Write Community'), and 'Globale Passwortoptionen' (containing a checkbox 'Passwörter und Schlüssel als Klartext anzeigen' and an 'Anzeigen' button).

Hauptkonfigurationsfenster

Kopfleiste

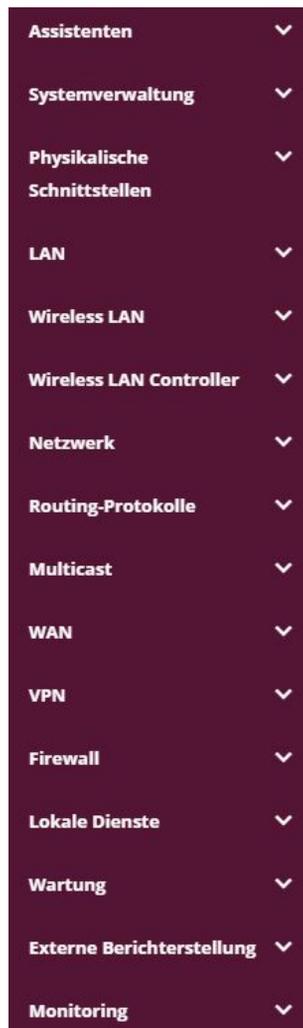
This close-up shows the header bar (Kopfleiste) of the web interface. It includes the device name 'bintec W2003ac', the bintec elmeg logo, and the text 'SPRACHE Ansicht Standard' and 'KONFIGURATION SPEICHERN'. There is also an 'Ausloggen' button with a question mark icon on the right.

Konfigurationsoberfläche Kopfleiste

Menü	Funktion
	Öffnet die Navigationsleiste, über die Sie Zugriff auf die Menüs zur Konfiguration haben.
	<p>Ausloggen: Wenn Sie die Konfiguration beenden möchten, klicken Sie auf diese Schaltfläche, um sich von Ihrem Gerät abzumelden. Es wird ein Fenster geöffnet, in dem Ihnen folgende Optionen angeboten werden:</p> <ul style="list-style-type: none"> • Konfiguration speichern, vorherige Konfiguration sichern, dann verlassen: Ihre Änderungen werden gespeichert, aber die zuvor aktive Konfiguration wird so gesichert, so dass Sie ggf. später wieder darauf zurückgreifen können. Erst dann erfolgt die Abmeldung vom Gerät. • Konfiguration speichern, dann verlassen: Ihre Änderungen werden gespeichert. Dabei wird die zuvor aktive Konfiguration ersetzt. Erst dann erfolgt die Abmeldung vom Gerät. • Ohne zu speichern verlassen: Ihre Änderungen sind zwar aktiv, werden aber nicht gespeichert. Nach einem Neustart sind

Menü	Funktion
	wieder die zuvor gültigen Einstellungen aktiv.
	Online-Hilfe: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Eine Beschreibung des Untermenüs mit den wichtigsten Informationen zu den verfügbaren Optionen wird angezeigt.
	Sprache: Wählen Sie in dem Aufklappmenü die gewünschte Sprache aus, in der die Konfigurationsoberfläche angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen <i>Deutsch</i> und <i>English</i> . Der Standardwert ist <i>Deutsch</i> .
	Ansicht: Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl steht Standard und SNMP-Browser.
	<p>Die Schaltfläche Konfiguration speichern.</p> <p>Wenn Sie Änderungen an der Konfiguration vorgenommen haben, können Sie diese auf zwei Arten speichern:</p> <ul style="list-style-type: none"> • Konfiguration speichern - Ihre Änderungen werden in die aktuelle Startkonfiguration (die Konfiguration, mit der Ihr Gerät nach jedem Start aktiv wird) übernommen und gespeichert. Die zuvor aktive Konfiguration wird dabei ersetzt. • Konfiguration speichern und vorhergehende Boot-Konfiguration sichern: Ihre Änderungen werden wie oben gespeichert, aber die zuvor aktive Konfiguration wird so gesichert, so dass Sie ggf. später wieder darauf zurückgreifen können. Es kann immer nur eine Sicherungsdatei erzeugt werden.

Navigationsleiste



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

Hauptkonfigurationsfenster

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

Konfigurationselemente

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

Schaltflächen

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

Schaltflächen für spezielle Funktionen

Schaltfläche	Funktion
IMPORTIEREN	Im Menü Systemverwaltung -> Zertifikate -> Zertifikatsliste und im Menü Systemverwaltung -> Zertifikate -> CRLs werden mit dieser Schaltfläche die Untermenüs für die Konfiguration des Zertifikate- bzw. CRL-Imports aufgerufen.
ANFORDERUNG	Im Menü Systemverwaltung -> Zertifikate -> Zertifikatsliste wird mit dieser Schaltfläche das Untermenü für die Konfiguration der Zertifikatsanforderung aufgerufen.

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

Symbole

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

Symbol	Funktion
	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 den Status "Wird aktiviert" einer Schnittstelle oder einer Verbindung.
	Kennzeichnet, dass der Datenverkehr verschlüsselt wird.
	Löst einen WLAN-Bandskan aus.
	Zeigt die nächste Seite einer Liste an.
	Zeigt die vorherige Seite einer Liste an.

In der Listenansicht haben Sie folgende Bedienfunktionen zur Auswahl:

Listenoptionen

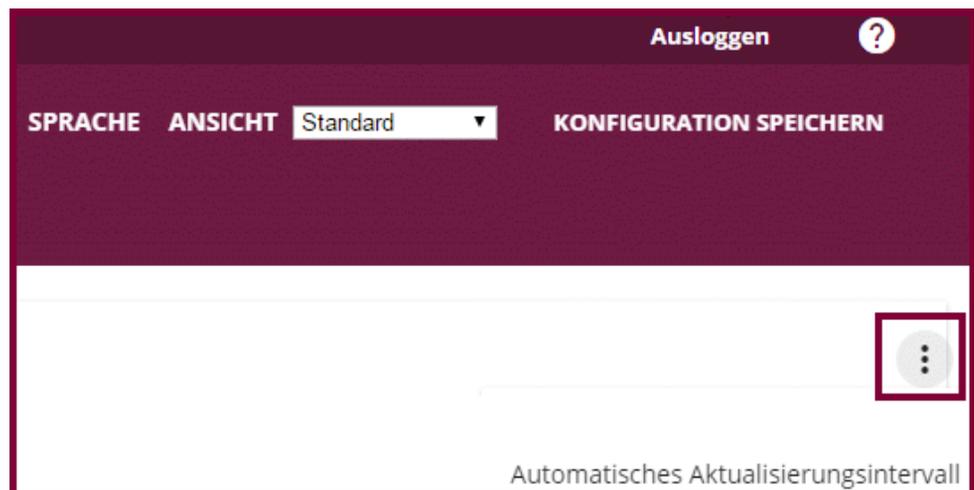
Menü	Funktion
Aktualisierungsintervall	<p>Hier können Sie das Intervall einstellen, in dem die Ansicht aktualisiert werden soll.</p> <p>Geben Sie dazu einen Zeitraum in Sekunden in das Eingabefeld ein und bestätigen Sie mit ÜBERNEHMEN.</p>

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

Ansicht 20 pro Seite   Filtern in **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**.

Automatisches Aktualisierungsintervall

60 Sekunden **ÜBERNEHMEN**

SCHLIESSEN

Konfiguration des Aktualisierungsintervalls

Struktur der Konfigurationsmenüs

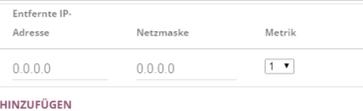
Die Menüs enthalten folgende Grundstrukturen:

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

Für die Konfiguration stehen folgende Optionen zur Verfügung:

Konfigurationselemente

Menü	Funktion
Eingabefelder	<p>z. B. leeres Textfeld</p>  <p>Textfeld mit verdeckter Eingabe</p>  <p>Geben Sie entsprechende Daten ein.</p>
Radiobuttons	<p>z. B.</p>  <p>Wählen Sie die entsprechende Option aus.</p>
Checkbox	<p>z. B. Aktivieren durch Auswahl der Checkbox</p> 
Dropdown-Menüs	<p>z. B.</p>  <p>Klicken Sie auf den Pfeil, um die Liste zu öffnen. Wählen Sie die gewünschte Option mit der Maus.</p>
Interne Listen	<p>z. B.</p>  <p>Klicken Sie auf die Schaltfläche HINZUFÜGEN. Ein neuer Listeneintrag wird angelegt. Geben Sie die entsprechenden Daten ein. Bleiben die Felder des Listeneintrags leer, wird dieser bei Bestätigen mit OK nicht gespeichert. Löschen Sie Einträge, indem Sie auf das -Symbol klicken.</p>

Darstellung von Optionen, die nicht zur Verfügung stehen

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

**Wichtig**

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

3.3.1.3 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 auf der jeweiligen Produktseite unter www.bintec-elmeg.com.

3.3.2 SNMP-Shell

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

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

Kapitel 4 Assistenten

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

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

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

Kapitel 5 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.

5.1 Status

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

Sie erhalten einen Überblick über folgende Daten:

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

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



Achtung

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

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

Felder im Menü Systeminformationen

Feld	Wert
Uptime	Zeigt die Zeit an, die vergangen ist, seit das Gerät neu gestartet wurde.
Systemdatum	Zeigt das aktuelle Systemdatum und die Systemuhrzeit an.
Seriennummer	Zeigt die Geräte-Seriennummer an.
BOSS-Version	Zeigt die aktuell geladene Version der Systemsoftware an.

Feld	Wert
Letzte gespeicherte Konfiguration	Zeigt Tag, Datum und Uhrzeit der letzten Konfigurationsspeicherung (Boot-Konfiguration im Flash) an.

Felder im Menü Ressourceninformationen

Feld	Wert
CPU-Nutzung	Zeigt die CPU-Auslastung in Prozent an.
Arbeitsspeichernutzung	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtspeicher in MByte an. Die Auslastung wird außerdem in Klammern in Prozent angezeigt.
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Felder im Menü Physikalische Schnittstellen

Feld	Wert
Schnittstelle - Verbindungsinformation - Link	<p>Hier sind alle physikalischen Schnittstellen aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle angeschlossen bzw. aktiv ist.</p> <p>Schnittstellendetails für Ethernet-Schnittstellen:</p> <ul style="list-style-type: none"> • IP-Adresse • Netzmaske <p>Schnittstellendetails für WLAN-Schnittstellen:</p> <p>Access-Point-Modus:</p> <ul style="list-style-type: none"> • Betriebsmodus: Access Point oder Aus • Der auf diesem Funkmodul verwendete Kanal • Anzahl der verbundenen Clients • Softwareversion der Funkkarte

Felder im Menü WAN-Schnittstellen

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

5.2 Globale Einstellungen

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

5.2.1 System

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

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

Feld	Wert
	<p>werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i>: Es werden nur Meldungen mit der Priorität Notfall aufgezeichnet. • <i>Alarm</i>: Es werden Meldungen mit der Priorität Notfall und Alarm aufgezeichnet. • <i>Kritisch</i>: Es werden Meldungen mit der Priorität Notfall, Alarm und Kritisch aufgezeichnet. • <i>Fehler</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch und Fehler aufgezeichnet. • <i>Warnung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler und Warnung aufgezeichnet. • <i>Benachrichtigung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung und Benachrichtigung aufgezeichnet. • <i>Information</i> (Standardwert): Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung, Benachrichtigung und Informationen aufgezeichnet. • <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.
<p>Maximale Anzahl der Accounting-Protokolleinträge</p>	<p>Geben Sie die maximale Anzahl an Einträgen an, die für Login-Vorgänge auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000</i>.</p> <p>Der Standardwert ist <i>20</i>.</p>
<p>Kommunikation mit dem Cloud NetManager</p>	<p>Nur für Geräte, die eine Verwaltung durch den Cloud NetManager unterstützen.</p> <p>Aktivieren oder deaktivieren Sie die Option Kommunikation mit dem Cloud NetManager.</p> <p>Im Auslieferungszustand ist die Option <i>Aktiviert</i>.</p>
<p>IP-Adresse des Cloud NetManagers</p>	<p>Nur für Geräte, die eine Verwaltung durch den Cloud NetManager unterstützen.</p> <p>Hier ist die Adresse des bintec elmeg Cloud NetManagers bereits vorkonfiguriert. Sollten Sie einen eigenen Manager betreiben wollen, müssen Sie hier die Adresse Ihres Servers eintra-</p>

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

5.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.



Hinweis

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

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

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

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

Felder im Menü Systempasswort

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

Felder im Menü SNMP-Communities

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

Feld im Menü Globale Passwortoptionen

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

5.2.3 Datum und Uhrzeit

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

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

ISDN/Manuell

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

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

chen Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt.

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

Zeitserver

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



Hinweis

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

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

Felder im Menü Grundeinstellungen

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

Felder im Menü Manuelle Zeiteinstellung

Feld	Beschreibung
Datum einstellen	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.

Feld	Beschreibung
Zeit einstellen	<p>Geben Sie eine neue Uhrzeit ein.</p> <p>Format:</p> <ul style="list-style-type: none"> • Stunde: hh • Minute: mm

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
ISDN-Zeitserver	<p>Nur für Geräte mit ISDN-Schnittstelle.</p> <p>Legen Sie fest, ob die Systemzeit über ISDN aktualisiert werden soll.</p> <p>Falls ein Zeitserver konfiguriert ist, wird die Zeit nur solange über ISDN ermittelt, bis ein erfolgreiches Update von diesem Zeitserver empfangen wurde. Für den Zeitraum, in dem die Zeit über einen Zeitserver ermittelt wird, wird die Aktualisierung über ISDN außer Kraft gesetzt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erster Zeitserver	<p>Geben Sie den ersten Zeitserver an, entweder mit Domänennamen oder IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitervers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zweiter Zeitserver	Geben Sie den zweiten Zeitserver an, entweder mit Domänen-

Feld	Beschreibung
	<p>namen oder IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitervers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Dritter Zeitserver	<p>Geben Sie den dritten Zeitserver an, entweder mit Domännennamen oder IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitervers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	<p>Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird.</p> <p>Der Standardwert ist <i>1440</i>.</p>
Zeitaktualisierungsrichtlinie	<p>Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Normal</i> (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen. • <i>Aggressiv</i>: Zehn Minuten lang wird versucht, den Zeitserver nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • <i>Endlos</i>: Es wird ohne zeitliche Begrenzung versucht, den Zeitserver zuerst nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. <p>Bei der Verwendung von Zertifikaten für die Verschlüsselung des Datenverkehrs in einem VPN ist es von zentraler Bedeutung, dass auf dem Gerät die korrekte Zeit eingestellt ist. Um dies sicherzustellen, wählen Sie für Zeitaktualisierungsrichtlinie den Wert <i>Endlos</i>.</p>
System als Zeitserver	<p>Wählen Sie aus, ob der interne Zeitserver verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Zeitanfragen eines Clients werden mit der aktuellen Systemzeit beantwortet. Diese wird als GMT ohne Offset angegeben.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Zeitanfragen eines Clients werden nicht beantwortet.</p>

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

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

5.2.4 Systemlizenzen

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

Es sind generell folgende Lizenztypen zu unterscheiden:

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

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

Lizenzdaten eintragen

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

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

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

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

Mögliche Werte für Status

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

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



Hinweis

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

5.2.4.1 Bearbeiten oder Neu

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

Freischalten von Zusatzlizenzen

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Grundeinstellungen

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



Hinweis

Wenn als Status *Nicht OK* angezeigt wird:

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

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

Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

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

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

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

5.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

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

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

Konventionen für die Port-/Schnittstellennamen

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

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

Beispiel: *WLAN1*

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

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

Beispiel: *ETH1*

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

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

- (c) Nummer der Schnittstelle

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

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

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

Beispiel: *br0* (erste Bridge-Gruppe)

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

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

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

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

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

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

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

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

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

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

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

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

5.3.1 Schnittstellen

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

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

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

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

Felder im Menü Schnittstellen

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

5.3.1.1 Hinzufügen

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

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

Felder im Menü Schnittstellen

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

Bearbeiten für Geräte der 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
Schnittstelle	Zeigt die Schnittstelle an, die gerade bearbeitet wird.

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

Feld	Wert
	Standardmäßig ist die Funktion nicht aktiv.

5.4 Administrativer Zugriff

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

5.4.1 Zugriff

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

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



Hinweis

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

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

Service Login (ISDN Web-Access) ist standardmäßig nicht aktiv. 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
Standardeinstellungen wiederherstellen	Erst wenn Sie Änderungen an der Konfiguration des administrativen Zugangs vornehmen, werden entsprechende Zugangsregeln eingerichtet und aktiviert. Mithilfe des Symbols  können Sie die Standardeinstellungen wiederherstellen.

5.4.1.1 Hinzufügen

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

Felder im Menü Zugriff

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

5.4.2 SSH

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

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

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

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



Hinweis

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

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

Felder im Menü SSH-Parameter (Secure Shell)

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

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

Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

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

Felder im Menü Schlüsselstatus

Feld	Wert
RSA-Schlüsselstatus	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>
ECDSA-Schlüsselstatus	<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>
ED25519-Schlüsselstatus	<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
Toleranzzeit beim Login	<p>Geben Sie die Zeit (in Sekunden) ein, die für den Verbindungsaufbau zur Verfügung steht. Wenn ein Client innerhalb dieser Zeit nicht erfolgreich authentifiziert werden kann, wird die Verbindung getrennt.</p> <p>Der Standardwert ist <i>600</i> Sekunden.</p>
Komprimierung	<p>Wählen Sie aus, ob Datenkompression verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-Keepalives	<p>Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierungslevel	<p>Wählen Sie den Syslog-Level für die vom SSH Daemon generierten Syslog-Messages aus.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Information</i> (Standardwert): Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet. • <i>Fatal</i>: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet. • <i>Fehler</i>: Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet. • <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.

5.4.3 SNMP

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

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

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

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

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

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

Felder im Menü Grundeinstellungen

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

Feld	Wert
SNMP multicast discovery	<p>Aktivieren oder deaktivieren Sie die Funktion SNMP multicast discovery.</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.

5.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

5.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete

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

Pakettyten

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.

5.5.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

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

Feld	Wert
	<p>Telecom.</p> <ul style="list-style-type: none"> • <i>bintec HotSpot Server</i>: Für Hotspot-Anwendungen.
Server-IP-Adresse	Geben Sie die IP-Adresse des RADIUS-Servers ein.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein.
Standard-Benutzerpasswort	Einige RADIUS-Server benötigen für jede RADIUS-Anfrage ein Benutzerpasswort. Geben Sie daher das Passwort hier ein, das Ihr Gerät als Standard-Benutzerpasswort in der Anfrage für die Dialout-Routen an den RADIUS-Server mitsendet.
Priorität	<p>Wenn mehrere RADIUS-Server-Einträge angelegt wurden, wird der Server mit der obersten Priorität als erstes verwendet. Wenn dieser Server nicht antwortet, wird der Server mit der nächstniedrigeren Priorität verwendet usw.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 7 (niedrigste Priorität).</p> <p>Der Standardwert ist 0.</p> <p>Siehe auch Richtlinie in den erweiterten Einstellungen.</p>
Eintrag aktiv	<p>Wählen Sie aus, ob der in diesem Eintrag konfigurierte RADIUS-Server verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Gruppenbeschreibung	<p>Definieren Sie eine neue RADIUS-Gruppenbeschreibung bzw. weisen Sie den neuen RADIUS-Eintrag einer schon definierten Gruppe zu. Die konfigurierten RADIUS-Server einer Gruppe werden gemäß der Priorität und der Richtlinie abgefragt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neu</i> (Standardwert): Tragen Sie in das Textfeld eine neue Gruppenbeschreibung ein. • <i>Standardgruppe 0</i>: Wählen Sie diesen Eintrag für spezielle Anwendungen, wie z. B. Hotspot-Server-Konfiguration, aus. • <i><Gruppenname></i>: Wählen Sie aus der Liste eine schon defi-

Feld	Wert
	nierte Gruppe aus.

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Wert
Richtlinie	<p>Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Verbindlich</i> (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. • <i>Nicht verbindlich</i>: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS-Server wird angefragt, bis Ihr Gerät eine Antwort von einem als autoritativ konfigurierten Server erhält.
UDP-Port	<p>Geben Sie den zu verwendenden UDP-Port für RADIUS-Daten ein.</p> <p>Gemäß RFC 2138 sind die Standard-Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Gebührenerfassung (1646 in älteren RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist.</p> <p>Der Standardwert ist <i>1812</i>.</p>
Server Timeout	<p>Geben Sie die maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden ein.</p> <p>Nach Ablauf dieser Zeit wird die Anfrage gemäß Wiederholungen wiederholt bzw. der nächste konfigurierte RADIUS-Server angefragt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>50</i> und <i>50000</i>.</p> <p>Der Standardwert ist <i>1000</i> (1 Sekunde).</p>
Erreichbarkeitsprüfung	<p>Wählen Sie eine Überprüfung der Erreichbarkeit eines RADIUS-Servers im Status <i>Inaktiv</i>.</p> <p>Es wird regelmäßig (alle 20 Sekunden) ein Alive-Check 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 Status wieder auf <i>aktiv</i> gesetzt. Wenn der RADIUS-Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit <i>inaktiv</i> ist.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Wiederholungen	<p>Geben Sie die Anzahl der Wiederholungen für den Fall ein, dass eine Anfrage nicht beantwortet wird. Falls nach diesen Versuchen dennoch keine Antwort erhalten wurde, wird der Status auf <i>inaktiv</i> gesetzt. bei Erreichbarkeitsprüfung = <i>Aktiviert</i> versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird Status wieder auf <i>aktiv</i> zurückgesetzt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 10.</p> <p>Der Standardwert ist 1. Um zu verhindern, dass Status auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf 0.</p>
RADIUS-Dialout	<p>Nur für Authentifizierungstyp = <i>PPP-Authentifizierung</i> und <i>IPSec-Authentifizierung</i>.</p> <p>Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiv ist, können Sie folgende Optionen eingeben:</p> <ul style="list-style-type: none"> • <i>Neulade-Intervall</i>: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. <p>Standardmäßig ist hier 0 eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>

5.5.2 TACACS+

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

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

Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:

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

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

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

5.5.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Authentifizierungstyp	<p>Zeigt an, welche TACACS+-Funktion genutzt werden soll. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Login-Authentifizierung</i>: Hier können Sie festlegen, ob der aktuelle TACACS+-Server für die Login-Authentifizierung zu Ihrem Gerät benutzt werden soll.
Server-IP-Adresse	Geben Sie die IP-Adresse des TACACS+-Servers ein, der für eine Login-Authentifizierung abgefragt werden soll.
TACACS+-Passwort	Geben Sie das Passwort ein, welches benutzt werden soll, um den Datenaustausch zwischen dem TACACS+-Server und dem

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

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

Felder im Menü Erweiterte Einstellungen

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

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

5.5.3 Optionen

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

Das Menü **Systemverwaltung** -> **Remote Authentifizierung** -> **Optionen** besteht aus fol-

genden Feldern:

Felder im Menü Globale RADIUS-Optionen

Feld	Beschreibung
Authentifizierung für PPP-Einwahl	<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"> • <i>Inband</i>: Nur Inband-RADIUS-Anfragen (PAP, CHAP, MS-CHAP V1 & V2) (d. h. PPP-Anfragen ohne Rufnummernidentifizierung) werden zum in Server-IP-Adresse definierten RADIUS-Server geschickt. • <i>Outband (CLID)</i>: Nur Outband-RADIUS-Anfragen (d. h. Anfragen zur Rufnummernidentifizierung) werden zum RADIUS-Server geschickt (CLID = Calling Line Identification). <p>Standardmäßig ist <i>Inband</i> aktiviert, <i>Outband (CLID)</i> deaktiviert.</p>

5.6 Konfigurationszugriff

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

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

5.6.1 Zugriffsprofile

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

Für Telefonanlagen sind standardmäßig die Zugriffsprofile *Mini-Callcenter*, *Kosten*, *Telefonbuch*, *Benutzerzugang zur Telefonanlage*, *Schnellstart*, *Experte*, *Benutzer* bereits angelegt. Diese können Sie mithilfe des Symbols  ändern sowie über das Symbol  auf die Standardeinstellungen zurücksetzen.

5.6.1.1 Bearbeiten oder Neu

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

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

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

Felder im Menü Grundeinstellungen

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

Felder im Menü Schaltflächen

Feld	Beschreibung
Konfiguration speichern	<p>Wenn Sie die Schaltfläche Konfiguration speichern aktivieren, darf der Benutzer Konfigurationen speichern.</p> <div data-bbox="539 1050 621 1101" style="display: inline-block; vertical-align: middle;">  </div> <p>Hinweis</p> <p>Beachten Sie, dass die Passwörter in der gespeicherten Datei im Klartext eingesehen werden können.</p> <p>Aktivieren oder deaktivieren Sie Konfiguration speichern.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zum SNMP Browser wechseln	Wenn Sie die Schaltfläche Zum SNMP Browser wechseln aktivieren, kann der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und alle dort angezeigten Einstellungen ändern.

Feld	Beschreibung
	<div data-bbox="539 211 619 297" style="text-align: center;"> </div> <p>Achtung</p> <p>Beachten Sie, dass die Berechtigung für Zum SNMP Browser wechseln bedeutet, dass der Benutzer auf die gesamte MIB zugreifen kann, da in dieser Ansicht kein individuelles Zugangsprofil angelegt werden kann. Mit der Berechtigung für Konfiguration speichern kann er die geänderte MIB speichern.</p> <p>Mit der Berechtigung für Zum SNMP Browser wechseln heben Sie die konfigurierten GUI- Einschränkungen auf der MIB-Ebene wieder auf.</p> <p>Aktivieren oder deaktivieren Sie Zum SNMP Browser wechseln.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Navigationseinträge

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Alle zulassen</i>: Das Menü und alle untergeordneten Menüs sind freigegeben. <p>Sie können in der entsprechenden Zeile <i>Zulassen</i> bzw. <i>Alle zulassen</i> wählen, um dem aktuellen Zugriffsprofil Elemente zuzuweisen.</p> <p>Elemente, die dem aktuellen Zugriffsprofil zugewiesen sind, sind mit dem Symbol  gekennzeichnet.</p> <p> kennzeichnet ein Menü, das gesperrt ist, das aber mindestens über ein freigegebenes Untermenü verfügt.</p>

5.6.2 Benutzer

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

Es sind keine Benutzer vorkonfiguriert.

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

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

5.6.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Benutzer	Geben Sie eine eindeutige Bezeichnung für den Benutzer ein.
Passwort	Geben Sie ein Passwort für den Benutzer ein.
Benutzer muss das	Mit der Option Benutzer muss das Passwort ändern kann der

Feld	Beschreibung
Passwort ändern	<p>Administrator bestimmen, dass der Benutzer beim ersten Login ein eigenes Passwort vergeben muss. Dazu muss die Option Konfiguration speichern im Menü Zugriffsprofile aktiv sein. Ist diese Option nicht aktiv, so wird ein Warnhinweis angezeigt.</p> <p>Aktivieren oder deaktivieren Sie Benutzer muss das Passwort ändern.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zugangs-Level	<p>Mit Hinzufügen weisen Sie dem Benutzer mindestens ein Zugriffsprofil zu. Mit der Auswahl von Nur lesen wird festgelegt, dass der Benutzer die Parameter des Zugriffsprofils ansehen, aber nicht ändern kann. Die Auswahl Nur lesen ist nur möglich, wenn die Option Zum SNMP Browser wechseln im Menü Zugriffsprofile nicht aktiv ist.</p> <p>Ist die Option Zum SNMP Browser wechseln aktiv, so wird ein Warnhinweis angezeigt, weil der Benutzer zur SNMP-Browser-Ansicht wechseln, auf die Parameter zugreifen und beliebige Änderungen vornehmen kann. Die Option Nur lesen ist in der SNMP-Browser-Ansicht nicht verfügbar.</p> <p>Werden einem Benutzer sich überschneidende Zugriffsprofile zugeordnet, so hat Lesen und Schreiben eine höhere Priorität als Nur lesen. Schaltflächen können nicht auf die Einstellung Nur lesen gesetzt werden.</p>

5.7 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.

5.7.1 Zertifikatsliste

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

5.7.1.1 Bearbeiten

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

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

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

Felder im Menü Parameter bearbeiten

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.

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



Achtung

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

5.7.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

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

Felder im Menü Zertifikatsanforderung

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Manuell</i> (Standardwert): Ihr Gerät erzeugt für den Schlüssel eine PKCS#10-Datei, die direkt im Browser hochgeladen oder im  -Menü über das Feld Details anzeigen kopiert werden kann. Diese Datei muss der CA zugestellt und das erhaltene Zertifikat anschließend manuell auf Ihr Gerät importiert werden. • <i>SCEP</i>: Der Schlüssel wird mittels des Simple Certificate Enrollment Protocols bei einer CA beantragt.
Privaten Schlüssel generieren	<p>Nur für Modus = <i>Manuell</i></p> <p>Wählen Sie einen Algorithmus für die Schlüsselerstellung aus.</p> <p>Zur Verfügung stehen <i>RSA</i> (Standardwert) und <i>DSA</i>.</p> <p>Wählen Sie weiterhin die Länge des zu erzeugenden Schlüssels aus.</p> <p>Mögliche Werte: <i>512, 768, 1024, 1536, 2048, 4096</i>.</p> <p>Beachten Sie, dass ein Schlüssel mit der Länge 512 Bit als unsicher eingestuft werden könnte, während ein Schlüssel mit 4096 Bit nicht nur viel Zeit zur Erzeugung erfordert, sondern während der IPSec-Verarbeitung einen wesentlichen Teil der Ressourcen belegt. Ein Wert von 768 oder mehr wird jedoch empfohlen, als Standardwert ist 1024 Bit vorgegeben.</p>
SCEP-URL	<p>Nur für Modus = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B. http://scep.beispiel.com:8080/scep/scep.dll</p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
CA-Zertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Wählen Sie das CA-Zertifikat aus.</p> <ul style="list-style-type: none"> • <i>-- Download --</i>: Geben Sie in CA-Name den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.

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 Zertifikatsanforderung generieren zurück.</p> <p>Falls das CA-Zertifikat keine CRL-Verteilstelle (Certificate Revocation List, CRL) enthält und auf Ihrem Gerät kein Zertifikatsserver konfiguriert ist, werden Zertifikate von dieser CA nicht auf ihre Gültigkeit überprüft.</p> <ul style="list-style-type: none"> • <Name eines vorhandenen Zertifikats>: Sind alle notwendigen Zertifikate bereits auf dem System vorhanden, wählen Sie diese manuell aus.
RA-Signierungszertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Nur für CA-Zertifikat nicht = <i>-- Download --</i></p> <p>Wählen Sie ein Zertifikat für die Signierung der SCEP-Kommunikation aus.</p> <p>Der Standardwert ist <i>-- CA-Zertifikat verwenden --</i>, d. h. es wird das CA-Zertifikat verwendet.</p>
RA-Verschlüsselungszertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Nur wenn RA-Signierungszertifikat nicht = <i>-- CA-Zertifikat verwenden --</i></p> <p>Wenn Sie ein eigenes Zertifikat zur Signierung der 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>
Passwort	<p>Nur für Modus = <i>SCEP</i></p> <p>Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.</p>

Felder im Menü Subjektname

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

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

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

Felder im Menü **Subjekt-Alternativnamen**

Feld	Beschreibung
#1, #2, #3	<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"> • <i>Keiner</i> (Standardwert): Es wird kein zusätzlicher Name eingegeben. • <i>IP</i>: Es wird eine IP-Adresse eingetragen. • <i>DNS</i>: Es wird ein DNS-Name eingetragen. • <i>E-Mail</i>: Es wird eine E-Mail-Adresse eingetragen. • <i>URI</i>: Es wird ein Uniform Resource Identifier eingetragen. • <i>DN</i>: Es wird ein Distinguished Name (DN) eingetragen. • <i>RID</i>: Es wird eine Registered Identity (RID) eingetragen.

Feld im Menü **Optionen**

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

5.7.1.3 Importieren

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

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

Felder im Menü Importieren

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

5.7.2 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.

5.7.2.1 Importieren

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

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

Felder im Menü CRL-Import

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

5.7.3 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.

5.7.3.1 Neu

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

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

Felder im Menü Basisparameter

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

Kapitel 6 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.

6.1 Ethernet-Ports

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



Hinweis

Die Ethernet-Ports ETH1 und ETH2 sind im Auslieferungszustand der Standard-Bridge-Gruppe *br0* zugeordnet, die als DHCP-Client und mit der Fallback-**IP-Adresse** *192.168.0.252* und **Netzmaske** *255.255.255.0* vorkonfiguriert ist.

Die Geräte der **bintec W1003n**-Serie haben nur den Ethernet-Port ETH 1.

6.1.1 Portkonfiguration

Ihr Gerät bietet die Möglichkeit, die zwei Ethernet-Schnittstellen getrennt zu konfigurieren.

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

Felder im Menü Portkonfiguration

Feld	Beschreibung
Port	Zeigt den jeweiligen Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Schnittstelle	Zeigt die logische Schnittstelle an, die dem jeweiligen Ethernet-Port zugeordnet ist.
Konfigurierte Geschwindigkeit/konfigu-	Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll.

Feld	Beschreibung
rierter Modus	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vollständige automatische Aushandlung (Standardwert)</i> • <i>Auto 1000 Mbit/s only</i> • <i>Auto 100 Mbit/s only</i> • <i>Auto 10 Mbit/s only</i> • <i>Auto 100 Mbit/s / Full Duplex</i> • <i>Auto 100 Mbit/s / Half Duplex</i> • <i>Auto 10 Mbit/s / Full Duplex</i> • <i>Auto 10 Mbit/s / Half Duplex</i> • <i>Fest 1000 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Half Duplex</i> • <i>Fest 10 Mbit/s / Full Duplex</i> • <i>Fest 10 Mbit/s / Half Duplex</i> • <i>Keiner</i> : Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	<p>Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>100 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Half Duplex</i> • <i>10 Mbit/s / Full Duplex</i> • <i>10 Mbit/s / Half Duplex</i> • <i>Inaktiv</i>

Kapitel 7 LAN

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

7.1 IP-Konfiguration

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

7.1.1 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

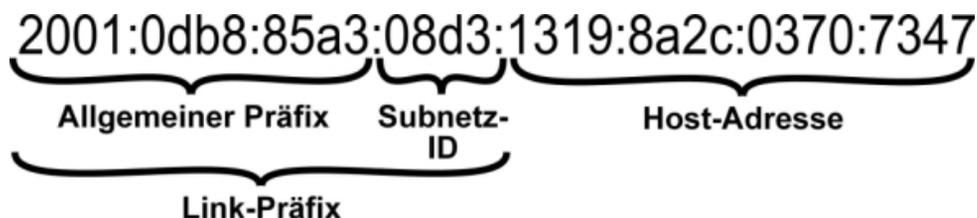
Falls Ihr Gerät an ein LAN angeschlossen ist, das aus zwei Teilnetzen besteht, sollten Sie für das zweite Teilnetz eine zweite **IP-Adresse / Netzmaske** eintragen.

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**.

7.1.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	<p>Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird.</p> <p>Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.</p>
Schnittstellenmodus	<p>Nur bei physikalischen Schnittstellen im Routing-Modus und bei virtuelle Schnittstellen.</p> <p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Untagged</i> (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet. • <i>Tagged (VLAN)</i>: Diese Option gilt nur für Routing-Schnittstellen. <p>Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu. Dies geschieht über die VLAN-ID, die in diesem Modus angezeigt wird und konfiguriert werden kann. Die Definition einer MAC-Adresse in MAC-Adresse ist in diesem Modus optional.</p>

Feld	Beschreibung
VLAN-ID	<p>Nur für Schnittstellenmodus = <i>Tagged</i> (VLAN)</p> <p>Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben.</p> <p>Mögliche Werte sind 1 (Standardwert) bis 4094.</p>
MAC-Adresse	<p>Geben Sie die mit der Schnittstelle verbundene MAC-Adresse ein. Sie können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde, wenn Sie Voreingestellte verwenden aktivieren. Die VLAN IDs müssen sich jedoch unterscheiden. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt (sie können jedoch geändert werden).</p> <p>Wenn Voreingestellte verwenden aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet.</p> <p>Standardmäßig ist Voreingestellte verwenden aktiv.</p>

Felder im Menü Grundlegende IPv4-Parameter

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 346 konfigurieren.</p>
Adressmodus	<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"> • <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse / Netzmaske zugewiesen. • <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
DHCP Metrik	<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>
IP-Adresse / Netzmaske	<p>Nur für Adressmodus = <i>Statisch</i></p> <p>Fügen Sie mit Hinzufügen einen neuen Adresseintrag hinzu und geben Sie die IP-Adresse und die entsprechende Netzmaske der virtuellen Schnittstelle ein.</p>

Felder im Menü Grundlegende IPv6-Parameter

Feld	Beschreibung
IPv6	<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>
Sicherheitsrichtlinie	<p>Hier nur für IPv6 = <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"> • <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind.

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"> • <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LANs verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 346 konfigurieren.</p>
IPv6-Modus	<p>Nur für IPv6 = <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"> • <i>Router (Router-Advertisement übermitteln)</i> (Standardwert): Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle gesendet werden sollen. <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"> • <i>Host</i>: Die Schnittstelle wird im Host-Modus betrieben.
DHCP-Server	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <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>
IPv6-Adressen	<p>Nur für IPv6 = <i>Aktiviert</i></p> <p>Sie können der gewählten Schnittstelle IPv6-Adressen zuordnen.</p> <p>Mit Hinzufügen 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 (IPv6-Modus = <i>Host</i>, Router Advertisement annehmen <i>Aktiviert</i> und DHCP-Client <i>Aktiviert</i>), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen.</p> <p>Wenn Ihr Gerät im Router-Modus arbeitet (IPv6-Modus = <i>Router (Router-Advertisement übermitteln)</i>, Router Advertisement übertragen <i>Aktiviert</i> und DHCP-Server <i>Aktiviert</i>), so müssen Sie hier seine IPv6-Adressen konfigurieren.</p>
Router Advertisement annehmen	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <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>
DHCP-Client	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <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</p>

Feld	Beschreibung
	<p>den DNS-Servern zu erhalten.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	<p>und wenn ein Allgemeiner Präfix gewählt ist.</p> <p>Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID <i>0</i> verwendet, für das zweite Subnetz die Subnetz-ID <i>1</i>, usw.</p> <p>Mögliche Werte für die Subnetz-ID 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>
Subnetz-ID	<p>Nur wenn Automatische Subnetzerstellung nicht aktiv ist.</p> <p>Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix.</p> <p>Mögliche Werte sind <i>0</i> bis <i>65535</i>.</p> <p>Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.</p>
Link-Präfix	<p>Nur für Art der Einrichtung = <i>Statisch</i></p> <p>Sie können den Link-Präfix einer IPv6-Adresse eingeben. Dieser Präfix muss mit <i>::</i> enden. Seine Länge ist mit <i>64</i> vorgegeben.</p>

Felder im Menü Host-Adresse

Feld	Beschreibung
Erzeugungsmethode	<p>Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
	<p>EUI-64 setzt folgenden Prozess in Gang:</p> <ul style="list-style-type: none"> • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird <code>FFFF</code> eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf <code>1</code> gesetzt.
Statische Adressen	<p>Sie können, unabhängig von der automatischen Erzeugung, die unter Erzeugungsmethode festgelegt ist, mit Hinzufügen den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit <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
On Link Flag	<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>
Autonomous Flag	<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>
Bevorzugte Gültigkeitsdauer	<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>
Gültigkeitsdauer	<p>Geben Sie eine Zeitspanne in Sekunden an, für die das Präfix gültig ist.</p> <p>Der Standardwert ist <i>2592000</i> Sekunden.</p>
<div style="border: 1px solid gray; padding: 10px; background-color: #f0f0f0;">  <p>Hinweis</p> <p>Der Wert für die Gültigkeitsdauer sollte niedriger sein als derjenige, der unter Erweiterte IPv6-Einstellungen für die Option Router-Gültigkeitsdauer konfiguriert ist.</p> </div>	

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

Felder im Menü **Erweiterte IPv4-Einstellungen**

Feld	Beschreibung
DHCP-MAC-Adresse	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Ist Voreingestellte verwenden aktiviert (Standardeinstellung) wird die Hardware-MAC-Adresse der Ethernet-Schnittstelle verwendet. Bei physikalischen Schnittstellen ist die aktuelle MAC-Adresse standardmäßig eingetragen.</p> <p>Wenn Sie Voreingestellte verwenden deaktivieren, geben Sie eine MAC-Adresse für die virtuelle Schnittstelle ein, z. B. <i>00:e1:f9:06:bf:03</i>.</p> <p>Manche Provider verwenden hardware-unabhängige MAC-Adressen, um ihren Clients IP-Adressen dynamisch zuzuweisen. Sollte Ihnen Ihr Provider eine MAC-Adresse zugewiesen haben, so tragen Sie diese hier ein.</p>
DHCP-Hostname	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Geben Sie den Hostnamen ein, der vom Provider gefordert wird. Die maximale Länge des Eintrags beträgt 45 Zeichen.</p>
DHCP Broadcast Flag	<p>Nur für Adressmodus = <i>DHCP</i></p>

Feld	Beschreibung
	<p>Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Standardroute erstellen	<p>Nur für Adressmodus = <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>
Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für definierte Gegenstellen beantworten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-MSS-Clamping	<p>Wählen Sie aus, ob Ihr Gerät das Verfahren MSS Clamping anwenden soll. Um die Fragmentierung von IP-Paketen zu verhindern, wird hierbei vom Gerät automatisch die MSS (Maximum Segment Size) auf den hier einstellbaren Wert verringert.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Bei Aktivierung ist im Eingabefeld der Standardwert <i>1350</i> eingetragen.</p>

Felder im Menü Erweiterte IPv6-Einstellungen

Feld	Beschreibung
Router-Gültigkeitsdauer	<p>Nur für IPv6 = <i>Aktiviert</i>, IPv6-Modus = <i>Router (Router-Advertisement übermitteln)</i> und Router Advertisement übertragen = <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 1316 707" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p> Hinweis</p> <p>Der Wert für die Router-Gültigkeitsdauer sollte höher sein als die kürzeste Link-Präfix-Gültigkeitsdauer, die im unter Grundlegende IPv6-Parameter für die Schnittstelle konfiguriert ist.</p> </div>
<p>Router-Präferenz</p>	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router (Router-Advertisement übermitteln) und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die Präferenz Ihres Routers für die Wahl des Standardrouters. Dies ist in Fällen nützlich, in denen ein Knoten Advertisements von mehreren Routern erhält oder in Back-Up-Szenarien.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hoch</i> • <i>Mittel</i> (Standardwert) • <i>Niedrig</i>
<p>DHCP-Modus</p>	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router (Router-Advertisement übermitteln) und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus.</p> <div data-bbox="539 1492 1316 1614" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p> Hinweis</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>
DNS-Propagation	<p>Nur für IPv6-Modus = Router (<i>Router-Advertisement übermitteln</i>) und Router Advertisement übertragen <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"> • <i>Aus</i>: Es wird keine DNS-Server-Adresse propagiert. • <i>Selbst</i>: Die eigene IP-Adresse wird als DNS-Server-Adresse propagiert. Bei mehreren Adressen, werden die Adressen in folgender Reihenfolge propagiert: <ul style="list-style-type: none"> • Globale Adressen • ULA (Unique Local Addresses) • Link-Lokale-Adressen • <i>Sonstige</i>: Die statisch konfigurierten und die dynamisch gelernten DNS-Server-Einträge werden gemäß ihrer Priorität propagiert. Sind keine Einträge vorhanden, werden keine Adressen propagiert.

7.2 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**.

7.2.1 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.

7.2.1.1 Bearbeiten oder Neu

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

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

Felder im Menü VLAN konfigurieren

Feld	Beschreibung
VLAN Identifier	Geben Sie die Ziffer ein, die das VLAN identifiziert. Im  -

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

7.2.2 Portkonfiguration

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

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

Felder im Menü Portkonfiguration

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

Feld	Beschreibung
	gewählte Port nicht Mitglied ist.

7.2.3 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
VLAN aktivieren	<p>Aktivieren oder deaktivieren Sie die spezifizierte Bridge-Gruppe für VLAN.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>

Kapitel 8 Wireless LAN

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

Netzwerkfunktionen

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

Derzeit gültiger Standard: IEEE 802.11. Informationen zu den in diesem Standard enthaltenen Modi und den damit erreichbaren Übertragungsgeschwindigkeiten finden Sie z. B. bei [Wikipedia](#). Beachten Sie die Informationen zur Sicherheit und Konformität, die Ihrem Produkt beiliegen!

8.1 WLAN

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

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

8.1.1 Einstellungen Funkmodul

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

8.1.1.1 Einstellungen Funkmodul->

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.



Hinweis

Der WLAN-Funktionsumfang unterscheidet sich ggf. zwischen unseren Produktfamilien. Wenn Sie eine Option in der Konfigurationsoberfläche nicht angeboten bekommen, so wird diese von Ihrem Gerät nicht unterstützt. Informieren Sie sich ggf. im Datenblatt Ihres Geräts.

Wählen Sie das Symbol  um die Konfiguration zu bearbeiten.

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

Felder im Menü WLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	<p>Legen Sie fest, in welchem Modus das Funkmodul Ihres Geräts betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Das Funkmodul ist nicht aktiv. • <i>Access-Point / Bridge Link Master</i>: Ihr Gerät dient als Access Point oder als Bridge Link Master in Ihrem Netzwerk. • <i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk. • <i>Access Client</i>: Ihr Gerät dient als Access Client in Ihrem Netzwerk. • <i>Bridge Link Client</i>: Ihr Gerät dient als Wireless Bridge in Ihrem Netzwerk.
Frequenzband	<p>Wählen Sie das Frequenzband und ggf. den Einsatzbereich des Funkmoduls aus.</p> <p>Für Betriebsmodus = <i>Access-Point / Bridge Link Master</i> oder <i>Bridge Link Client</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2,4 GHz In/Outdoor</i> (Standardwert): Ihr Gerät wird mit 2.4 GHz innerhalb oder außerhalb von Gebäuden betrieben. • <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz innerhalb von Gebäuden betrieben.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz außerhalb von Gebäuden betrieben. • <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz innerhalb oder außerhalb von Gebäuden betrieben.
Nutzungsbereich	<p>Nur für Betriebsmodus = <i>Access Client</i> und Frequenzband = <i>2,4 und 5 GHz</i> oder <i>5 GHz</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Indoor-Outdoor</i> (Standardwert) • <i>Indoor</i> • <i>Outdoor</i>
Kanal	<p>Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.</p> <p>Access-Point-Modus / Bridge-Modus:</p> <p>Durch das Einstellen des Netzwerknamens (SSID) im Access-Point-Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens 4 Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt.</p> <p>Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden Clients diese Kanäle auch unterstützen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>2,4 GHz In/Outdoor</i> <p>Mögliche Werte sind <i>1 bis 13</i> und <i>Auto</i> (Standardwert).</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz Indoor</i> <p>Mögliche Werte sind <i>36, 40, 44, 48</i> und <i>Auto</i> (Standardwert)</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Out-</i>

Feld	Beschreibung
	<p><i>door</i></p> <p>Hier ist nur die Option <i>Auto</i> möglich.</p> <p>Access Client Modus:</p> <p>Im Access Client Modus können Sie kein Kanal auswählen. Der verwendete Kanal wird angezeigt.</p>
Ausgewählter Kanal	Zeigt den verwendeten Kanal an.
Zweiter Verwendeter Kanal	<p>Nicht für Betriebsmodus = <i>Access-Point / Bridge Link Master</i></p> <p>Zeigt den zweiten verwendeten Kanal an.</p>
Sendeleistung	<p>Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die tatsächlich abgestrahlte Antennenleistung kann abhängig von der übertragenen Datenrate auch niedriger liegen als der eingestellte Maximalwert. Der Maximalwert der verfügbaren Sendeleistung ist länderabhängig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet. • <i>5 dBm</i> • <i>8 dBm</i> • <i>11 dBm</i> • <i>14 dBm</i> • <i>16 dBm</i> • <i>17 dBm</i>

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	<p>Wählen Sie die Wireless-Technologie aus, die der Access Point anwenden soll.</p> <p>Für Betriebsmodus = <i>Access-Point / Bridge Link Master</i> und Frequenzband = <i>2,4 GHz In/Outdoor</i> oder für Betriebsmodus = <i>Access Client</i> und Frequenzband = <i>2,4</i></p>

Feld	Beschreibung
	<p data-bbox="639 189 682 210"><i>GHz</i></p> <p data-bbox="639 244 811 264">Mögliche Werte:</p> <ul data-bbox="639 298 1310 1140" style="list-style-type: none"> <li data-bbox="639 298 1263 355">• <i>802.11g</i>: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. <li data-bbox="639 377 1306 433">• <i>802.11b</i>: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. <li data-bbox="639 456 1310 548">• <i>802.11 mixed (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. <li data-bbox="639 570 1300 758">• <i>802.11 mixed long (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Nur die Datenrate von 1 und 2 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). Dieser Modus wird auch für Centrino Clients benötigt, falls Verbindungsprobleme aufgetreten sind. <li data-bbox="639 780 1286 935">• <i>802.11 mixed short (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). <li data-bbox="639 958 1272 1014">• <i>802.11b/g/n</i>: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. <li data-bbox="639 1036 1292 1093">• <i>802.11g/n</i>: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n. <li data-bbox="639 1115 1263 1140">• <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. <p data-bbox="639 1175 1310 1330">Für Betriebsmodus = <i>Access-Point / Bridge Link Master</i> und <i>Bridge Link Client</i> und Frequenzband = <i>5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor</i> und für Betriebsmodus = <i>Access Client</i> und Frequenzband = <i>5 GHz</i></p> <p data-bbox="639 1366 811 1386">Mögliche Werte:</p> <ul data-bbox="639 1421 1300 1608" style="list-style-type: none"> <li data-bbox="639 1421 1263 1446">• <i>802.11a</i>: Ihr Gerät arbeitet ausschließlich nach 802.11a. <li data-bbox="639 1463 1263 1489">• <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. <li data-bbox="639 1506 1292 1562">• <i>802.11a/n</i>: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n. <li data-bbox="639 1579 1300 1608">• <i>802.11ac/a/n</i>: (sofern von Ihrem Gerät unterstützt) Ihr Ge-

Feld	Beschreibung
	<p>rät arbeitet nach 802.11 ac, 802.11a oder nach 802.11n.</p> <ul style="list-style-type: none"> • <i>802.11ac/n</i>: (sofern von Ihrem Gerät unterstützt) Ihr Gerät arbeitet entweder nach 802.11ac oder 802.11n.
Bandbreite	<p>Für Betriebsmodus = <i>Access Client</i> oder <i>Access-Point / Bridge Link Master</i></p> <p>Nicht für Frequenzband = <i>2,4 GHz In/Outdoor</i></p> <p>Wählen Sie aus, wie viele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>20 MHz</i> (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • <i>40 MHz</i>: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontroll-Kanal und der andere als Erweiterungs-Kanal. • <i>80 MHz</i>: Im Modus 802.11ac steht zusätzlich eine Bandbreite von 80 MHz zur Verfügung.
Anzahl der Spatial Streams	<p>Nicht für Drahtloser Modus = <i>802.11a</i></p> <p>Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2</i>: Zwei Datenströme werden verwendet. • <i>1</i>: Ein Datenstrom wird verwendet.
Airtime Fairness	<p>Diese Funktion ist nicht für alle Geräte verfügbar.</p> <p>Mit der Airtime Fairness -Funktion wird gewährleistet, dass Senderressourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
	Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.

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

Felder im Menü **Erweiterte Einstellungen** für Betriebsmodus = **Access-Point / Bridge Link Master**

Feld	Beschreibung
Kanalplan	<p>Nur für Betriebsmodus = <i>Access-Point / Bridge Link Master</i> und Kanal = <i>Auto</i></p> <p>Wählen Sie den gewünschten Kanalplan aus.</p> <p>Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d. h. dass zwischen den verwendeten Kanälen ein Abstand von vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i>: Alle Kanäle können bei der Kanalwahl gewählt werden. • <i>Auto</i>: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • <i>Benutzerdefiniert</i>: Wählen Sie die gewünschten Kanäle selbst aus.
Ausgewählte Kanäle	<p>Nur für Kanalplan = <i>Benutzerdefiniert</i></p> <p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <p>Mit Hinzufügen können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen.</p> <p>Mithilfe von -Symbol können Sie Einträge löschen.</p>
RTS Threshold	Hier wählen Sie aus, wie der RTS/CTS-Mechanismus ein- bzw. ausgeschaltet werden soll.

Feld	Beschreibung
	Wählen Sie <i>Benutzerdefiniert</i> aus, können Sie in das Eingabefeld den Schwellwert in Bytes (1 - 2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch unabhängig von der Datenpaketlänge ein- bzw. ausgeschaltet werden, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.
Short Guard Interval	Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
Fragmentation Threshold	Geben Sie die maximale Größe an, ab der Datenpakete fragmentiert (d. h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert. Möglich Werte sind <i>256</i> bis <i>2346</i> . Der Standardwert ist <i>2346</i> Bytes.

Wurde für **Betriebsmodus** *Bridge Link Client* ausgewählt, stehen unter **Erweiterte Einstellungen** zusätzlich folgende Parameter zur Verfügung:

Felder im Menü **Erweiterte Einstellungen für Access Client Modus**

Feld	Beschreibung
Kanäle scannen	Wählen Sie aus, auf welchen Kanälen der WLAN-Client automatisch nach verfügbaren Drahtlosnetzwerken scannen soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Damit wird auf allen Kanälen gescannt. • <i>Auto</i>: Der Kanal wird automatisch ausgewählt. • <i>Benutzerdefiniert</i>: Damit können die gewünschten Kanäle manuell festgelegt werden.
Benutzerdefinierter Kanalplan	Nur für Kanäle scannen = <i>Benutzerdefiniert</i> Legen Sie fest, auf welchen Kanälen der WLAN-Client nach verfügbaren Drahtlosnetzwerken scannen soll.

Feld	Beschreibung
Roaming-Profil	<p>Wählen Sie das Roaming-Profil aus. Die zur Verfügung stehende Optionen fassen typische Roaming-Funktionen zusammen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnelles Roaming</i>: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, sobald das Funksignal der bestehenden Funkverbindung für höhere Datenraten ungeeignet ist. • <i>Normales Roaming</i> (Standardwert): Standard-Roaming. • <i>Langsames Roaming</i>: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, sobald das Funksignal der bestehenden Funkverbindung schwächer wird. • <i>Kein Roaming</i>: Der WLAN-Client sucht nach verfügbaren Drahtlosnetzwerken, wenn er nicht mit einem Drahtlosnetzwerk verbunden ist. • <i>Benutzerdefiniertes Roaming</i>: Legen Sie individuelle Roaming-Parameter fest.
Scan-Schwelle	<p>Zeigt an, ab welchem Wert in dBm im Hintergrund nach verfügbaren Drahtlosnetzwerken gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist -70 dBm.</p>
Scan-Intervall	<p>Zeigt an, in welchen Abständen in Millisekunden nach verfügbaren Drahtlosnetzwerken gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 5000 ms.</p>
Min. Zeitraum aktiver Scan	<p>Zeigt die minimale, aktive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 10 ms.</p>
Max. Zeitraum aktiver Scan	<p>Zeigt die maximale, aktive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i></p>

Feld	Beschreibung
	<i>tes Roaming</i> verändert werden. Der Standardwert ist <i>40 ms</i> .
Min. Zeitraum passiver Scan	<p>Zeigt die minimale, passive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = Benutzerdefiniertes Roaming verändert werden. Der Standardwert ist <i>20 ms</i>.</p>
Max. Zeitraum passiver Scan	<p>Zeigt die maximale, passive Scanzeit für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = Benutzerdefiniertes Roaming verändert werden. Der Standardwert ist <i>120 ms</i>.</p>
Max. Scan-Dauer	<p>Zeigt die maximale Scandauer für eine Frequenz in Millisekunden an.</p> <p>Der Wert kann nur für Roaming-Profil = Benutzerdefiniertes Roaming verändert werden. Der Standardwert ist <i>50000 ms</i>.</p>

8.1.2 Drahtlosnetzwerke (VSS)

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



Hinweis

Das voreingestellte Drahtlosnetzwerk default verfügt im Auslieferungszustand über folgende Sicherheitseinstellungen:

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

Einstellen von Netzwerknamen

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

Absicherung von Funknetzwerken

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

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

WEP

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

IEEE 802.11i

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

WPA

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

802.1x (z. B. RADIUS) an.

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

WPA 2

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

Zugangskontrolle

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

Sicherheitsmaßnahmen

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

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

- Beschränken Sie den Zugriff im WLAN auf zugelassene Clients. Tragen Sie die MAC-Adressen der Funknetzwerkarten dieser Clients in die **Erlaubte Adressen**-Liste im Menü **MAC-Filter** ein (siehe *Felder im Menü MAC-Filter* auf Seite 142).

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

8.1.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	<p>Geben Sie den Namen des Wireless Netzwerks (SSID) ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.</p> <p>Wählen Sie außerdem aus, ob der Netzwerkname (SSID) übertragen werden soll.</p> <p>Mit Auswahl von <i>Sichtbar</i> wird der Netzwerkname sichtbar übertragen.</p> <p>Standardmäßig ist er sichtbar.</p>
Intra-cell Repeating	<p>Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Die Nutzer des Gäste-WLANs sollen normalerweise zwar Zugang zum Internet haben, aber keinen Zugriff auf das Intranet der Firma. Um dies zu verhindern, muss die Option deaktiviert sein.</p>
U-APSD	<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>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

Felder im Menü Sicherheitseinstellungen

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>WPA</i>: Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA 2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA</i> und <i>WPA und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i>: AES wird angewendet. • <i>TKIP</i>: TKIP wird angewendet • <i>AES und TKIP</i> (Standardwert): AES oder TKIP werden angewendet.
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA 2</i> und <i>WPA und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA 2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i>: AES wird angewendet. • <i>AES und TKIP</i> (Standardwert): AES oder TKIP werden angewendet.
Preshared Key	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.</p>
	<div style="border: 1px solid gray; padding: 5px;">  <p>Hinweis</p> <p>Ändern Sie unbedingt den Standard Preshared Key! Solange der Schlüssel nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p> </div>
EAP-	<p>Nur für Sicherheitsmodus = <i>WPA-Enterprise</i></p>

Feld	Beschreibung
Vorabauthentifizierung	<p>Wählen Sie aus, ob EAP-Vorabauthentifizierung aktiviert werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p> <p>Mögliche Werte sind ganze Zahlen von 1 bis 254.</p> <p>Der Standardwert ist 32.</p>
Max. Anzahl Clients - Soft Limit	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Um eine vollständige Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehnt. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des Max. Anzahl Clients - Hard Limit werden Anfragen strikt abgelehnt.</p> <p>Der Wert der Max. Anzahl Clients - Soft Limit muss gleich oder kleiner sein als der Max. Anzahl Clients - Hard Limit.</p>

Feld	Beschreibung
	<p>Der Standardwert ist <i>28</i>.</p> <p>Sie können diese Funktion deaktivieren, indem Sie Max. Anzahl Clients - Soft Limit und Max. Anzahl Clients - Hard Limit auf den gleichen Wert einstellen.</p>
Auswahl des Client-Bands	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist.</p> <p>Die Option Auswahl des Client-Bands ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert, optimiert für Fast Roaming</i> (Standardwert): Die Funktion wird für dieses VSS nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • <i>2,4-GHz-Band bevorzugt</i>: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • <i>5-GHz-Band bevorzugt</i>: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	<p>Wählen Sie aus, ob für dieses Wireless Netzwerk nur bestimmte Clients zugelassen werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erlaubte Adressen	<p>Nur bei Zugriffskontrolle = <i>Aktiviert</i></p> <p>Legen Sie Einträge mit Hinzufügen an und geben Sie die MAC-</p>

Feld	Beschreibung
	Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.

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

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

Felder im Menü **Erweiterte Einstellung**

Feld	Beschreibung
Beacon Period	<p>Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an.</p> <p>Dieser Wert wird in Beacon und Probe Response Frames übermittelt.</p> <p>Mögliche Werte sind <i>1 bis 65535</i>.</p> <p>Der Standardwert ist <i>100 ms</i>.</p>
DTIM Period	<p>Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an.</p> <p>Das DTIM-Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Strom-</p>

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

Felder im Menü Data-Rate Trimming

Feld	Beschreibung
Geschwindigkeitsprofil im 5-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"> • <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. • <i>Ab 12 MBit/s</i> - s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit • <i>Ab 24 MBit/s</i> - s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit

Felder im Menü Unterer RSSI-Schwellwert

Feld	Beschreibung
RSSI-Schwellwert	<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 -110 dBm.</p>
Toleranzzeit	<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> <p>Der Standardwert ist 5 Sekunden.</p>

8.1.3 Client Link

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

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

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

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

8.1.3.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

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

Felder im Menü Basisparameter

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

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Keys
Übertragungsschlüssel	Nur für Sicherheitsmodus = <i>WEP 104</i> Wählen Sie einen der in WEP-Schlüssel <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus. Der Standardwert ist <i>Schlüssel 1</i> .
WEP-Schlüssel 1 - 4	Nur für Sicherheitsmodus = <i>WEP 40</i> , <i>WEP 104</i> Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen.
WPA-Modus	Nur für Sicherheitsmodus = <i>WPA-PSK</i> Wählen Sie aus, ob Sie WPA oder WPA 2 anwenden wollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>WPA</i> (Standardwert): Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 wird angewendet.

Feld	Beschreibung
Preshared Key	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.</p>
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA</i></p> <p>Wählen Sie aus welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): Temporal Key Integrity Protocol • <i>AES</i>: Advanced Encryption Standard. <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.</p>
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA2</i></p> <p>Wählen Sie aus, welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): Advanced Encryption Standard. • <i>TKIP</i>: Temporal Key Integrity Protocol <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.</p>

8.1.3.2 Client Link Scan

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

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

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

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

Felder im Menü Scan

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des von Ihnen konfigurierten Client-Links an.
Aktion	Lösen Sie den Scan durch Klicken von Scan aus. Bei sachgerechter Installation der Antennen auf beiden Seiten und freier Line of Sight (LOS, Sichtverbindung) wird der Client verfügbare Access Points finden und in der folgenden Liste anzeigen. Sollte der gewünschte Partner-Access-Point nicht gefunden werden, überprüfen Sie die Line-of-Sight und die Antenneninstallation. Führen Sie dann erneut Scan aus. Der Partner sollte daraufhin gefunden werden.
AP-MAC-Adresse	Zeigt die MAC-Adresse der gefundenen Access Points an.
Netzwerkname (SSID)	Zeigt den Namen der gefundenen Access-Points an.
Kanal	Zeigt die verwendeten Kanäle der entfernten Access Points an.
Modus	Zeigt den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes an.
Signal	Zeigt die Signalstärke des erkannten Client-Links in dBm an.
Verbunden	Zeigt den Status des Links auf Ihrem Client an.
Aktion	Sie können den Status der Client-Links verändern. In diesem Feld werden die zur Verfügung stehenden Aktionen angezeigt.

8.1.4 Bridge-Links



Hinweis

Beachten Sie, dass die Bridge-Link-Funktion dieser Geräteserie nicht kompatibel mit älteren Bridge-Link bzw. WDS-Implementierungen ist.

Mit **Bridge-Links** können Sie mehrere WLAN-Geräte eine dedizierte Verbindung aufbauen lassen. Dies dient vor allem der zuverlässigen Verbindung von Netzwerken über eine WLAN-Strecke.

8.1.4.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Name des Bridge Links (ID)	<p>Je nachdem, ob Sie das Funkmodul als Access Point oder als Wireless Bridge Link betreiben, legen Sie hier Bridge Links im Master- oder im Slave-Modus an.</p> <p>Befindet sich das Funkmodul im Betriebsmodus Access-Point / Bridge Link Master, können Sie Bridge Links im Master-Modus und im Slave-Modus anlegen, im Betriebsmodus Bridge Link Client können Sie Links nur im Slave-Modus erstellen.</p> <p>Geben Sie einen Namen für den Bridge Link ein. Im Master-Modus dient er anderen Geräten als ID, unter der sie sich mit diesem Bridge Link verbinden können.</p> <p>Im Betriebsmodus Bridge Link Client, befindet sich der Bridge Link automatisch im Slave-Modus. Geben Sie hier die ID desjenigen Bridge Links ein, mit dem sich das Gerät verbinden soll.</p>
Preshared Key	<p>Geben Sie das Passwort für diesen Bridge-Link ein. Im Master-Modus ist dies das Passwort, mit dem andere Geräte sich mit diesem Bridge Link verbinden können, im Slave-Modus das Passwort desjenigen Bridge Links, mit dem eine Verbindung aufgebaut werden soll.</p>
Rolle	<p>Hier legen Sie die Rolle fest, die Ihr Gerät übernehmen soll.</p> <p>Mögliche Werte:</p> <p><i>Master:</i> Im Master-Modus verbinden sich Clients als Slaves mit Ihrem Gerät. Neben dem Bridge Link kann es dann gleichzeitig auch die Funktion eines Access Points für WLAN Clients zur Verfügung stellen.</p> <p><i>Slave:</i> Im Slave-Modus verbindet sich Ihr Gerät mit einem der konfigurierten Bridge Links.</p>

8.2 Verwaltung

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

8.2.1 Grundeinstellungen

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

Felder im Menü WLAN Administration

Feld	Beschreibung
Region	<p>Wählen Sie das Land, in welchem der Access Point betrieben werden soll.</p> <p>Mögliche Werte sind alle auf dem Wireless-Modul des Geräts vorkonfigurierten Länder.</p> <p>Der Bereich der auswählbaren Kanäle (Kanal im Menü Wireless LAN->WLAN->Einstellungen Funkmodul) variiert je nach Ländereinstellung.</p> <p>Der Standardwert ist <i>Germany</i>.</p>

Kapitel 9 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.

9.1 Wizard

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



Hinweis

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

9.1.1 Wireless LAN Controller Wizard

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

9.1.1.1 Grundeinstellungen

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

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

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

Schnittstelle

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

DHCP-Server

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

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

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

Wenn Sie z. B. ein bintec elmeg Gateway als DHCP-Server verwenden wollen, klicken Sie im **GUI** Menü dieses Geräts unter **Lokale Dienste->DHCP-Server->DHCP-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.

9.1.1.2 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.

9.1.1.3 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.

9.1.1.3.1 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 WPA oder WPA 2 oder beides anwenden wollen.

Preshared Key

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

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



Wichtig

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

RADIUS-Server

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

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

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

EAP-Vorabauthentifizierung

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

VLAN

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

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



Hinweis

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

9.1.1.4 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 da-

zu in der Spalte **Manage** auf die gewünschten Einträge oder klicken Sie auf **Alle auswählen**, um alle Einträge auszuwählen. Klicken Sie auf die Schaltfläche **Alle deaktivieren**, um alle Einträge zu deaktivieren und danach bei Bedarf einzelne Einträge auszuwählen (z. B. bei großen Listen).

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



Hinweis

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

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

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

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

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

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

9.1.2 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.

9.1.2.1 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
VLAN-ID	Wählen Sie eine der existierenden VLAN-IDs aus dem Auswahlmenü. Es werden nur IDs angezeigt, für die noch keine Konfiguration vorliegt.
IP-Adresse/Netzmaske	Geben Sie hier die IP-Konfiguration der neuen Schnittstelle ein. Achten Sie darauf, dass diese noch nicht verwendet worden ist.
DHCP-Server	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"> • <i>Extern oder statisch</i>: Verwenden Sie diese Option, wenn Sie in Ihrem Netzwerk bereits einen DHCP-Server betreiben oder die Clients, die sich mit den VLAN verbinden, ei-

Feld	Beschreibung
	<p>ne 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"> • <i>Intern</i>: Verwenden Sie diese Option, wenn Sie Ihr Gerät als DHCP-Server für das VLAN einsetzen wollen.
IP-Adressbereich	<p>Nur bei DHCP-Server = Intern</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 Lokale Dienste->DHCP Server->DHCP-Konfiguration.</p>

9.2 Controller-Konfiguration

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

9.2.1 Allgemein

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Status	<p>Aktivieren Sie die Option Status um die Grundeinstellungen für den Wireless LAN Controller zu konfigurieren.</p> <p>Standarmäßig ist die Funktion nicht aktiv.</p>
Delete the complete WLAN Controller configuration	<p>Nur für Status = nicht aktiviert.</p> <p>Mithilfe des Symbols  können Sie eine Konfiguration löschen.</p>
Region	<p>Wählen Sie das Land, in welchem der Wireless LAN Controller</p>

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

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

9.2.2 Slave-AP-Autoprofil

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

9.2.2.1 Bearbeiten oder Neu

Das Menü **Wireless LAN**

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

Felder im Menü Access-Point-Filter

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

Felder im Menü Access-Point-Einstellungen

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

Felder im Menü Funkmodul 1 oder im Funkmodul 2

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

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

9.3 Slave-AP-Konfiguration

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

9.3.1 Slave Access Points

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

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

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

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

Mögliche Werte für Status

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

Status	Bedeutung
	bzw. ohne Stromversorgung o.ä.

9.3.1.1 Bearbeiten

Wählen Sie das Symbol  , um vorhandene Einträge zu bearbeiten.

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

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Access-Point-Einstellungen

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

Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
Betriebsmodus	Zeigt, in welchem Modus das Funkmodul betrieben werden soll. Sie können den Modus ändern.

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

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

9.3.2 Funkmodulprofile

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

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

9.3.2.1 Bearbeiten oder Neu

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

Das Menü **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile->Neu** besteht aus folgenden Feldern:

Felder im Menü Funkmodulprofil-Konfiguration

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

Felder im Menü Performance-Einstellungen

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

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

Feld	Beschreibung
	<p>Wählen Sie aus, wieviele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>20 MHz</i> (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • <i>40 MHz</i>: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal. • <i>80 MHz</i>: Im Modus 802.11ac steht zusätzlich eine Bandbreite von 80 MHz zur Verfügung.
<p>Anzahl der Spatial Streams</p>	<p>Nicht für Frequenzband = <i>2,4 GHz In/Outdoor</i> und</p> <p>Drahtloser Modus = <i>802.11g, 802.11b, 802.11 mixed (b/g), 802.11 mixed long (b/g), 802.11 mixed short (b/g)</i> und für Frequenzband = <i>5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor</i> oder <i>5,8 GHz Outdoor</i> und Drahtloser Modus= <i>802.11a</i></p> <p>Wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>3</i>: Drei Datenströme werden verwendet. • <i>2</i>: Zwei Datenströme werden verwendet. • <i>1</i>: Ein Datenstrom wird verwendet.
<p>Airtime Fairness</p>	<p>Diese Funktion ist nicht für alle Geräte verfügbar.</p> <p>Mit der Airtime Fairness -Funktion wird gewährleistet, dass Senderressourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames</p>

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

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	<p>Mit Hinzufügen können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen.</p> <p>Mithilfe von -Symbol können Sie Einträge löschen.</p>
Beacon Period	<p>Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an.</p> <p>Dieser Wert wird in Beacon und Probe Response Frames übermittelt.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 100.</p>
DTIM Period	<p>Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an.</p> <p>Das DTIM Feld ist ein Datenfeld in den ausgesendeten Beacons, das Clients über das Fenster zur nächsten Broadcast- oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 2.</p>
RTS Threshold	<p>Sie können hier den Schwellwert in Bytes (1..2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden.</p>
Short Guard Interval	<p>Aktivieren Sie diese Funktion, um den Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.</p>
Max. Übertragungsrate	<p>Wählen Sie die Übertragungsgeschwindigkeit aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Die Übertragungsgeschwindigkeit wird

Feld	Beschreibung
	<p>automatisch ermittelt.</p> <ul style="list-style-type: none"> • <i><Wert></i>: Je nach Einstellung für Frequenzband, Bandbreite, Anzahl der Spatial Streams und Drahtloser Modus stehen verschiedene feste Werte in MBit/s zur Auswahl.
Short Retry Limit	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Frames ein, dessen Länge kürzer oder gleich dem in RTS Threshold definierten Wert ist. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 7.</p>
Long Retry Limit	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, dessen Länge größer ist als der in RTS Threshold definierte Wert. Nach dieser Anzahl an Fehlversuchen wird dieses Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 4.</p>
Fragmentation Threshold	<p>Geben Sie die maximale Größe in Byte an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert.</p> <p>Möglich Werte sind 256 bis 2346.</p> <p>Der Standardwert ist 2346.</p>

9.3.3 Drahtlosnetzwerke (VSS)

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

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

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

9.3.3.1 Bearbeiten oder Neu

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

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

Felder im Menü Service Set Parameter

Feld	Beschreibung
Netzwerkname (SSID)	<p>Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.</p> <p>Wählen Sie außerdem aus, ob der Netzwerkname (SSID) übertragen werden soll.</p> <p>Mit Auswahl von <i>Sichtbar</i> wird der Netzwerkname sichtbar übertragen.</p> <p>Standardmäßig ist er sichtbar.</p>
Intra-cell Repeating	<p>Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <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>
U-APSD	<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>
IGMP Snooping	<p>IGMP Snooping reduziert den Datenverkehr und damit die Netzlast, weil Multicast Pakete aus dem LAN nicht weitergeleitet werden. Es werden ausschließlich Multicast-Pakete weitergeleitet, die von den entsprechenden Clients angefordert werden.</p>

Feld	Beschreibung
	<p>Wenn Sie IGMP Snooping aktivieren, gibt IGMP Snooping daher den Rahmen vor, in dem Multicast angewendet wird.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	<p>Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Key • <i>WPA-Enterprise</i>: 802.11x
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Der Standardwert ist <i>Schlüssel 1</i>.</p>
WEP-Schlüssel 1-4	<p>Nur für Sicherheitsmodus = <i>WEP 40</i>, <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein.</p> <p>Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> und <i>WPA 2</i> (Standardwert): WPA und WPA 2 können angewendet werden. • <i>WPA</i>: Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA</i> und <i>WPA</i> und <i>WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): TKIP wird angewendet. • <i>AES</i>: AES wird angewendet. • <i>AES</i> und <i>TKIP</i>: AES oder TKIP wird angewendet.
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA 2</i> und <i>WPA</i> und <i>WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): AES wird angewendet. • <i>TKIP</i>: TKIP wird angewendet. • <i>AES</i> und <i>TKIP</i>: AES oder TKIP wird angewendet.
Preshared Key	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.</p> <p>Beachten Sie: Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p>

Feld	Beschreibung
RADIUS-Server	<p>Nur für Sicherheitsmodus = <i>WPA-Enterprise</i> Sie können den Zugang zu einem Drahtlosnetzwerk über einen RADIUS-Server regeln.</p> <p>Mit Hinzufügen können Sie neue Einträge anlegen. Geben Sie die IP-Adresse und das Passwort des RADIUS-Servers ein.</p>
EAP-Vorabauthentifizierung	<p>Nur für Sicherheitsmodus = <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob EAP-Vorabauthentifizierung aktiviert werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p> <p>Mögliche Werte sind ganze Zahlen von 1 bis 254.</p> <p>Der Standardwert ist 32.</p>
Max. Anzahl Clients - Soft Limit	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Um eine vollständige Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, wer-</p>

Feld	Beschreibung
	<p>den neue Verbindungsanfragen zunächst abgelehnt. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des Max. Anzahl Clients - Hard Limit werden Anfragen strikt abgelehnt.</p> <p>Der Wert der Max. Anzahl Clients - Soft Limit muss gleich oder kleiner sein als der Max. Anzahl Clients - Hard Limit.</p> <p>Der Standardwert ist <i>28</i>.</p> <p>Sie können diese Funktion deaktivieren, indem Sie Max. Anzahl Clients - Soft Limit und Max. Anzahl Clients - Hard Limit auf den gleichen Wert einstellen.</p>
Auswahl des Client-Bands	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist.</p> <p>Die Option Auswahl des Client-Bands ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert, optimiert für Fast Roaming</i> (Standardwert): Die Funktion wird für dieses VSS nicht angewendet. Dies ist dann sinnvoll, wenn Clients zwischen unterschiedlichen Funkzellen möglichst verzögerungsfrei wechseln sollen, z. B. bei Voice over WLAN. • <i>2,4-GHz-Band bevorzugt</i>: Clients werden bevorzugt im 2,4-GHz-Band akzeptiert. • <i>5-GHz-Band bevorzugt</i>: Clients werden bevorzugt im 5-GHz-Band akzeptiert.

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	<p>Wählen Sie aus, ob für dieses Drahtlosnetzwerk nur bestimmte Clients zugelassen werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erlaubte Adressen	<p>Legen Sie Einträge mit Hinzufügen an und geben Sie die MAC-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.</p>
Dynamische Black List	<p>Mithilfe der Funktion Dynamische Black List ist es möglich, Clients, die sich möglicherweise unbefugt Zugriff auf das Netzwerk verschaffen wollen, zu erkennen und für einen bestimmten Zeitraum zu sperren. Ein Client wird dann gesperrt, wenn die Anzahl erfolgloser Anmeldeversuche innerhalb einer definierten Zeit eine bestimmte Anzahl überschreitet. Diese Grenzwerte ebenso wie die Dauer der Sperrung können konfiguriert werden. Ein gesperrten Client wird auf allen vom Wireless LAN Controller verwalteten APs für das betroffene VSS gesperrt, kann sich also auch nicht in einer anderen Funkzelle an diesem VSS anmelden. Soll ein Client permanent gesperrt bleiben, so kann dies im Menü Wireless LAN Controller->Monitoring->Rogue Clients erfolgen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiviert.</p>
Fehlversuche per Zeitraum	<p>Geben Sie hier die Anzahl der Fehlversuche ein, die innerhalb einer bestimmten Zeit von einer MAC-Adresse ausgehen müssen, damit ein Eintrag in der dynamischen Black List angelegt wird.</p> <p>Standardwerte sind <i>10</i> Fehlversuche in <i>60</i> Sekunden.</p>
Sperrzeit für Black List	<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
VLAN	<p>Wählen Sie aus, ob für dieses Drahtlosnetzwerk VLAN-Segmentierung verwendet werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
VLAN-ID	<p>Geben Sie den Zahlenwert ein, der das VLAN identifiziert.</p> <p>Mögliche Werte sind 2 bis 4094.</p> <p>VLAN ID 1 ist nicht möglich, da sie bereits verwendet wird.</p>

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

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>

Feld	Beschreibung
	<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"> • <i>Alle (Min. 1 MBit/s)</i> - Alle Clients, die eine Übertragungsgeschwindigkeit von 1 MBit/s aufrecht erhalten können, können sich am Access Point anmelden. • <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. • <i>Min. 12 MBit/s (keine 802.11b-Geräte)</i>- s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit • <i>Min. 24 MBit/s (keine 802.11b-Geräte)</i>- s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit
Geschwindigkeitsprofil im 5-GHz-Band	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <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. • <i>Ab 12 MBit/s</i> - s.o. für Clients mit 12 Mbit/s Mindestgeschwindigkeit • <i>Ab 24 MBit/s</i> - s.o. für Clients mit 24 Mbit/s Mindestgeschwindigkeit

Felder im Menü Unteren RSSI-Schwellwert verwalten

Feld	Beschreibung
RSSI-Schwellwert	<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</p>

Feld	Beschreibung
	zum betroffenen Client ein. Der Standardwert ist -110 dBm.
Toleranzzeit	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. Der Standardwert ist 5 Sekunden.

9.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.



Hinweis

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

9.4.1 WLAN Controller

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

Werte in der Liste Übersicht

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

9.4.2 Slave Access Points

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

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

9.4.2.1 Übersicht

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

Werte in der Liste Übersicht

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

9.4.2.2 Funkmodul 1

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

Werte in der Liste Funkmodul

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

9.4.3 Aktive Clients

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

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

Rx-Bytes, Tx Discards, Rx Discards, Status und Uptime.

Mögliche Werte für Status

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

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

Werte in der Liste WLAN Client

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

9.4.4 Drahtlosnetzwerke (VSS)

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

9.4.5 Client-Verwaltung

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

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

9.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Access Points und Clients.

9.5.1 Benachbarte APs

Im Menü **Wireless LAN Controller+Umgebungs-Monitoring->Benachbarte APs** werden die benachbarten APs angezeigt, die während des Scannens gefunden wurden. **Rogue APs**, d.h. APs, die eine vom WLAN-Controller verwaltete SSID verwenden, aber nicht vom WLAN-Controller administriert werden, sind rot hinterlegt.



Hinweis

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

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

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

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

9.5.2 Rogue APs

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

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



Hinweis

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

Sie können einen Rogue AP als vertrauenswürdig einstufen, indem Sie die Checkbox in der Spalte **Angenommen** aktivieren. Ein eventuell konfigurierter Alarm wird dadurch gelöscht und ab sofort nicht mehr gesendet. Der rote Hintergrund verschwindet.

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

9.5.3 Rogue Clients

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

Mögliche Werte für Rogue Clients

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

Status	Bedeutung
	werden.
Löschen	Mithilfe des  -Symbols können Sie Einträge löschen.

9.5.3.1 Neu

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Neuer Eintrag in die Blacklist

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

9.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

9.6.1 Firmware-Wartung

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

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

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

Mögliche Werte für Status

Status	Bedeutung
Image bereits vorhanden.	Das Software Image ist bereits vorhanden, es ist kein Update nötig.
Fehler	Es ist ein Fehler aufgetreten..

Status	Bedeutung
Wird ausgeführt	Das Update wird gerade ausgeführt.
Fertig	Das Update ist beendet.

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

Felder im Menü Firmware-Wartung

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

Kapitel 10 Netzwerk

10.1 Routen

Standard-Route (Default Route)

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

10.1.1 Konfiguration von IPv4-Routen

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

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

10.1.1.1 Bearbeiten oder Neu

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

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

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	<p>mationen zu einem bestimmten Netzwerk ergänzt.</p> <div data-bbox="539 280 1319 570" style="border: 1px solid gray; padding: 10px;"> <p> Hinweis</p> <p>Durch dem Ablauf des DHCP Leases oder durch einen Neustart des Geräts werden die Routen, die aus der Kombination von DHCP- und hier vorgenommenen Einstellungen entstehen, zunächst wieder aus dem aktiven Routing gelöscht. Mit einer erneuten DHCP-Konfiguration werden sie dann neu generiert und wieder aktiviert.</p> </div>
Schnittstelle	Wählen Sie die Schnittstelle aus, welche für diese Route verwendet werden soll.
Routenklasse	<p>Wählen Sie die Art der Routenklasse aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Definiert eine Route mit den Standardparametern. • <i>Erweitert</i>: Wählen Sie aus, ob die Route mit erweiterten Parametern definiert werden soll. Ist die Funktion aktiv, wird eine Route mit erweiterten Routing-Parametern wie Quell-Schnittstelle und Quell-IP-Adresse sowie Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und der Status der Geräte-Schnittstelle angelegt.

Felder im Menü Routenparameter

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

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

Felder im Menü Erweiterte Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IP-Route ein.
Quellschnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen.</p> <p>Der Standardwert ist <i>Keine</i>.</p>
Quell-IP-Adresse/Netzmaske	Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.
Layer 4-Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Mögliche Werte: <i>AH, Beliebig, ESP, GRE, ICMP, IGMP, L2TP, OSPF, PIM, TCP, UDP</i>.</p> <p>Der Standardwert ist <i>Beliebig</i>.</p>
Quell-Port	<p>Nur für Layer 4-Protokoll = <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"> • <i>Beliebig</i> (Standardwert): Die Route gilt für alle Port-Nummern. • <i>Einzeln</i>: Ermöglicht Eingabe einer Port-Nummer. • <i>Bereich</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • <i>Privilegiert</i>: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • <i>Server</i>: Eingabe von Server Port-Nummern: 5000 ... 32767. • <i>Clients 1</i>: Eingabe von Client Port-Nummern: 1024 ... 4999. • <i>Clients 2</i>: Eingabe von Client Port-Nummern: 32768 ... 65535. • <i>Nicht privilegiert</i>: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. <p>Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in Port (einzelner bzw. Anfangsport) und ggf. in bis Port (Endport) die entsprechenden Werte ein.</p>
Zielport	<p>Nur für Layer 4-Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie den Zielport an.</p> <p>Wählen Sie zunächst den Portnummernbereich aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Route gilt für alle Port-Nummern. • <i>Einzeln</i>: Ermöglicht Eingabe einer Port-Nummer. • <i>Bereich</i>: Ermöglicht Eingabe eines Bereiches von Port-Nummern. • <i>Privilegiert</i>: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • <i>Server</i>: Eingabe von Server Port-Nummern: 5000 ... 32767. • <i>Clients 1</i>: Eingabe von Client Port-Nummern: 1024 ... 4999.

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

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"> • <i>Verbindlich</i>: Die Route ist immer benutzbar. • <i>Wählen und fortfahren</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist. • <i>Nie einwählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. • <i>Immer wählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

10.1.2 Konfiguration von IPv6-Routen

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

10.1.2.1 Bearbeiten oder Neu

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

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

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

Felder im Menü Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IPv6-Route an.
Route aktiv	<p>Wählen Sie, ob die Route aktiv oder inaktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Route auf den Status aktiv gesetzt.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
Routentyp	<p>Wählen Sie die Art der Route aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standardroute über Schnittstelle</i>: Route über eine spezifische Schnittstelle, die verwendet wird, wenn keine andere passende Route verfügbar ist. • <i>Standardroute über Gateway</i>: Route über ein spezifisches Gateway, die verwendet wird, wenn keine andere passende Route verfügbar ist. • <i>Host-Route über Schnittstelle</i>: Route zu einem einzelnen Host über eine spezifische Schnittstelle. • <i>Host-Route via Gateway</i>: Route zu einem einzelnen Host über ein spezifisches Gateway. • <i>Netzwerkroute via Schnittstelle</i>: Route zu einem Netzwerk über eine spezifische Schnittstelle. • <i>Netzwerkroute via Gateway (Standardwert)</i>: Route zu einem Netzwerk über ein spezifisches Gateway.
Zielschnittstelle	<p>Wählen Sie die IPv6-Schnittstelle aus, welche für diese Route verwendet werden soll.</p> <p>Sie können unter den Schnittstellen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind und für welche die Nutzung von IPv6 aktiviert ist.</p>
Quelladresse/Länge	<p>Geben Sie die IPv6-Quelladresse mit der entsprechenden Präfixlänge ein.</p> <p>Die Eingabe <code>::</code> beschreibt eine unspezifische Adresse.</p> <p>Standardmäßig ist eine Präfixlänge von <code>64</code> vorgegeben.</p>
Zieladresse/Länge	<p>Geben Sie die IPv6-Zieladresse mit der entsprechenden Präfixlänge ein.</p> <p>Die Eingabe <code>::</code> beschreibt eine unspezifische Adresse.</p> <p>Standardmäßig ist eine Präfixlänge von <code>64</code> vorgegeben.</p>

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

10.1.3 IPv4-Routing-Tabelle

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

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

Felder im Menü IPv4-Routing-Tabelle

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

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

10.1.4 IPv6-Routing-Tabelle

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

Felder im Menü IPv6-Routing-Tabelle

Feld	Beschreibung
Route	Zeigt die Quell- und die Zieladresse, die für diese Route verwendet wird an, sowie die Gateway IP-Adresse. Im Falle von per DHCP erhaltenen Routen wird hier nichts angezeigt.
Schnittstelle	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
Metrik	Zeigt die Priorität der Route an. Je niedriger der Wert, desto höhere Priorität besitzt die Route.
Protokoll	Zeigt an, wie der Eintrag erzeugt wurde, z. B. manuell (<i>Lokal</i>) oder über eins der verfügbaren Protokolle.

10.1.5 Optionen

Überprüfung der Rückroute

Hinter dem Begriff "Überprüfung der Rückroute" (engl. "Back Route Verify") versteckt sich eine einfache, aber sehr leistungsfähige Funktion. Wenn die Überprüfung bei einer Schnittstelle aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden. Dadurch können Sie - auch ohne Filter - die Akzeptanz von Paketen mit gefälschten IP-Adressen verhindern.

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

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

Felder im Menü Überprüfung der Rückroute

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

10.2 Allgemeine IPv6-Präfixe

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

Das Konzept der Allgemeinen Präfixe hat zwei entscheidende Vorteile:

- Zwischen Provider und Kunde genügt eine einzige Route.
- Wenn der Provider einen neuen Allgemeinen Präfix per DHCP zuteilt oder einen statisch 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 109 sowie die für IPv6 relevanten Parameter im Menü **LAN->IP-Konfiguration->Schnittstellen**).

10.2.1 Konfiguration eines Allgemeinen Präfixes

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

10.2.1.1 Bearbeiten oder Neu

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

Optionen im Menü Basisparameter

Feld	Beschreibung
Aktiver Allgemeiner Präfix	Wählen Sie, ob das Präfix aktiv oder inaktiv sein soll. Mit <i>Aktiviert</i> wird das Präfix auf den Status aktiv gesetzt. Standardmäßig ist das Präfix aktiv.
Name	Geben Sie einen Namen für das Allgemeine Präfix ein. Ein sprechender Name dient dazu, das Allgemeine Präfix aus einer Präfixliste leichter auswählen zu können.
Typ	Wählen Sie, wie der Adressraum zugewiesen werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Dynamisch</i> (Standardwert): Der Allgemeine Präfix wird dynamisch mittels einer DHCP-Übertragung festgesetzt, z. B. von einem Provider. • <i>Statisch</i>: Das Präfix wird fest vorgegeben, z. B. durch

Feld	Beschreibung
	einen Provider.
Von Schnittstelle	<p>Nur bei Typ = <i>Dynamisch</i></p> <p>Wählen Sie die IPv6-Schnittstelle aus, von welcher ein Allgemeiner Präfix bezogen werden soll.</p> <p>Sie können unter den Schnittstellen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind und die folgende Bedingungen erfüllen:</p> <ul style="list-style-type: none"> • IPv6 ist <i>Aktiviert</i>. • IPv6-Modus = <i>Host</i> • DHCP-Client ist <i>Aktiviert</i>.
Benutzer Präfix/Länge	<p>Nur bei Typ = <i>Statisch</i></p> <p>Geben Sie das Präfix ein, das verwendet werden soll. Geben Sie die zugehörige Länge ein. Dieser Präfix muss mit :: enden.</p> <p>Standardmäßig ist eine Länge von <i>48</i> vorgegeben.</p>

10.3 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in [NAT-Konfiguration](#) auf Seite 202).

Konkrete Hinweise für die Konfiguration von NAT finden Sie am Ende des Kapitels unter [NAT - Konfigurationsbeispiel](#) auf Seite 209.

10.3.1 NAT-Schnittstellen

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

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

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

Optionen im Menü NAT-Schnittstellen

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

10.3.2 NAT-Konfiguration

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

10.3.2.1 Neu

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

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

Feld im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
Schnittstelle	<p>Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): NAT wird für alle Schnittstellen konfiguriert. • <i><Schnittstellename></i>: Wählen Sie eine der Schnittstellen aus der Liste aus.
Art des Datenverkehrs	<p>Wählen Sie, für welche Art von Datenverkehr NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>eingehend (Ziel-NAT)</i> (Standardwert): Der Datenverkehr, der von außen kommt. • <i>ausgehend (Quell-NAT)</i>: Der Datenverkehr, der nach außen geht. • <i>exklusiv (ohne NAT)</i>: Der Datenverkehr, der von NAT ausgenommen ist.
NAT-Methode	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i></p> <p>Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-Schnittstelle eine IP-Verbindung zu einem "externen" Ziel-Host initiiert hat und bei der eine intern gültige Quelladresse und ein intern gültiger Quellport auf eine extern gültige Quelladresse und einen extern gültigen Quellport umgesetzt werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>full-cone</i> (nur UDP): Jeder beliebige externe Host darf IP-

Feld	Beschreibung
	<p>Pakete über die externe Adresse und den externen Port an die initiiierende Quelladresse und den initialen Quellport senden.</p> <ul style="list-style-type: none"> • <i>restricted-cone</i> (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen. • <i>port-restricted-cone</i> (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • <i>symmetrisch</i> (Standardwert) Für beliebige Protokolle: In ausgehender Richtung werden eine extern gültige Quelladresse und ein extern gültiger Quell-Port administrativ festgelegt. In eingehender Richtung sind nur Antwortpakete innerhalb der bestehenden Verbindung zugelassen.

Im Menü **NAT-Konfiguration** ->**Ursprünglichen Datenverkehr angeben** können Sie konfigurieren, für welchen Datenverkehr NAT verwendet werden soll.

Felder im Menü Ursprünglichen Datenverkehr angeben

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Nicht ausschließen</i>: Alle Datenpakete, die mit den nachfolgend zu konfigurierenden Parametern (Protokoll, Quell-IP-Adresse/Netzmaske, Ziel-IP-Adresse/Netzmaske, usw.) nicht übereinstimmen, werden von NAT ausgenommen.
Protokoll	<p>Nur für bestimmte Dienste.</p> <p>Nicht für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i> und NAT-Methode = <i>full-cone, restricted-cone</i> oder <i>port-restricted-cone</i>. In diesem Fall wird UDP automatisch festgelegt.</p> <p>Wählen Sie ein Protokoll aus. Je nach ausgewähltem Dienst stehen verschiedene Protokolle zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>AH</i> • <i>Chaos</i> • <i>EGP</i> • <i>ESP</i> • <i>GGP</i> • <i>GRE</i> • <i>HMP</i> • <i>ICMP</i> • <i>IGMP</i> • <i>IGP</i> • <i>IGRP</i> • <i>IP</i> • <i>IPinIP</i> • <i>IPv6</i> • <i>IPX in IP</i> • <i>ISO-IP</i> • <i>Kryptolan</i> • <i>L2TP</i> • <i>OSPF</i>

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

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

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

Felder im Menü Substitutionswerte

Feld	Beschreibung
Neue Ziel-IP-Adresse/Netzmaske	Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i> Geben Sie diejenige Ziel-IP-Adresse und die zugehörige Netzmaske ein, auf welche die ursprüngliche Ziel-IP-Adresse umge-

Feld	Beschreibung
	<p>setzt werden soll.</p>
<p>Neuer Ziel-Port</p>	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i></p> <p>Belassen Sie den Ziel-Port oder geben Sie denjenigen Ziel-Port ein, auf den der ursprüngliche Ziel-Port umgesetzt werden soll.</p> <p>Mit Auswahl von <i>Original</i> belassen Sie den ursprünglichen Ziel-Port. Wenn Sie <i>Original</i> deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Ziel-Port eingeben.</p> <p>Standardmäßig ist <i>Original</i> aktiv.</p>
<p>Neue Quell-IP-Adresse/Netzmaske</p>	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i> und NAT-Methode = <i>symmetrisch</i></p> <p>Geben Sie diejenige Quell-IP-Adresse ein, auf welche die ursprüngliche Quell-IP-Adresse umgesetzt werden soll, gegebenenfalls mit zugehöriger Netzmaske.</p>
<p>Neuer Quell-Port</p>	<p>Nur für Art des Datenverkehrs = <i>ausgehend (Quell-NAT)</i>, NAT-Methode = <i>symmetrisch</i>, Dienst = <i>Benutzerdefiniert</i>, Protokoll = <i>TCP, UDP, TCP/UDP</i> und Original Quell-Port/Bereich = <i>-Alle- oder Port angeben</i></p> <p>Belassen Sie den Quell-Port oder geben Sie einen neuen Quell-Port ein, auf den der ursprüngliche Quell-Port umgesetzt werden soll.</p> <p>Mit Auswahl von <i>Original</i> belassen Sie den ursprünglichen Quell-Port. Wenn Sie <i>Original</i> deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Quell-Port eingeben. Standardmäßig ist <i>Original</i> aktiv.</p> <p>Haben Sie für Original Quell-Port/Bereich <i>Portbereich angeben</i> gewählt, stehen folgende Auswahlmöglichkeiten zur Verfügung:</p> <ul style="list-style-type: none"> • <i>Original Quell-Port/Bereich verwenden</i>: Der in Original Quell-Port/Bereich angegebene Bereich wird nicht verändert, die Portnummern bleiben erhalten. • <i>Verwende Port/Bereich beginnend bei</i>: Es erscheint

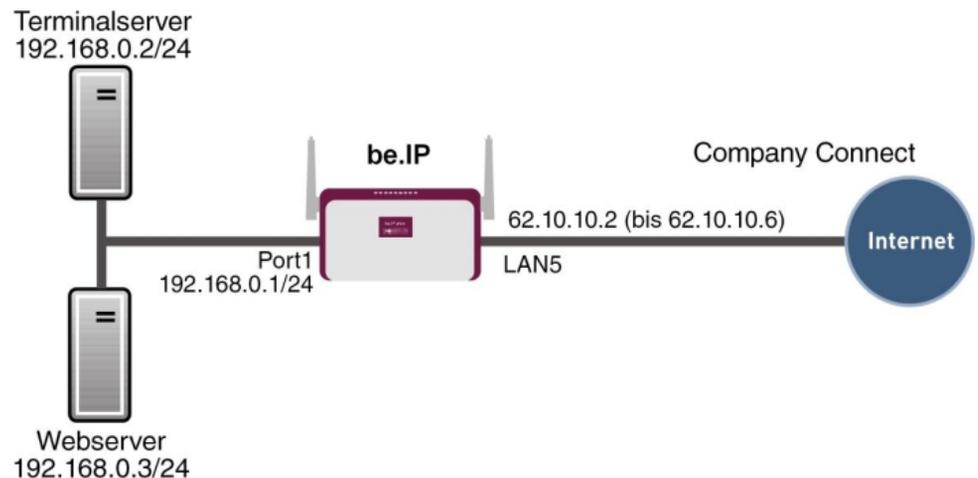
Feld	Beschreibung
	ein Eingabefeld, in das Sie die Portnummer eingeben können, bei der der Portbereich beginnen soll, durch den der ursprüngliche Portbereich ersetzt wird. Die Anzahl der Ports bleibt dabei gleich.

10.3.3 NAT - Konfigurationsbeispiel

Voraussetzungen

- Grundkonfiguration des Gateways
- Die Konfiguration erfordert einen funktionsfähigen Internetzugang, hier als Beispiel **Company Connect** mit acht IP-Adressen.
- Die Ethernet-Schnittstelle **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-Konfiguration->Neu	z. B. Webserver
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration->Neu	LAN_EN5-0

Feld	Menü	Wert
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>eingehend (Ziel-NAT)</i>
Dienst	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>http</i>
Quell-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Beliebig</i>
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Host, z. B. 62.10.10.3</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Host, z. B. 192.168.0.3</i>
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Original</i>

Terminal Server

Feld	Menü	Wert
Beschreibung	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>z. B. Terminal-Server</i>
Schnittstelle	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>LAN_EN5-0</i>
Art des Datenverkehrs	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>eingehend (Ziel-NAT)</i>
Dienst	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Benutzerdefiniert</i>
Protokoll	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>TCP</i>
Quell-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Beliebig</i>
Original Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Host, z. B. 62.10.10.4</i>
Original Ziel-Port/Bereich	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Port angeben, 3389</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Host, z. B. 192.168.0.2</i>
Neuer Ziel-Port	Netzwerk->NAT->NAT-Konfiguration->Neu	<i>Original</i>

10.4 Lastverteilung

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

Konkrete Hinweise für die Konfiguration von Lastverteilung finden Sie unter [Lastverteilung - Konfigurationsbeispiel](#) auf Seite 219.

10.4.1 Lastverteilungsgruppen

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

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

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



Hinweis

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

10.4.1.1 Neu

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

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	nur Schnittstellen im Zustand aktiv berücksichtigt.

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

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

Felder im Menü Basisparameter

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

Felder im Menü Schnittstellenauswahl für Verteilung

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Routenselektor	Der Parameter Routenselektor ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten Anwendungsfällen notwendig, um die vom Router verwalteten IP Sessions eindeutig je Loadbalancing-Gruppe bilanzieren zu können. Für die Anwendung des Para-

Feld	Beschreibung
	<p>meters gelten folgende Regeln:</p> <ul style="list-style-type: none"> • Ist eine Schnittstelle nur einer Lastverteilungsgruppe zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig. • Ist eine Schnittstelle mehreren Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich. • Innerhalb einer Lastverteilungsgruppe muss der Routenselektor aller Schnittstelleneinträge identisch konfiguriert sein. <p>Wählen Sie die Ziel-IP-Adresse der gewünschten Route aus.</p> <p>Sie können unter allen Routen und allen erweiterten Routen wählen.</p>
<p>IP-Adresse zur Nachverfolgung</p>	<p>Mit dem Parameter IP-Adresse zur Nachverfolgung können Sie eine bestimmte Route überwachen lassen.</p> <p>Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die Konfiguration von Host-Überwachungseinträgen zwingend erforderlich. Konfiguriert werden kann dies im Menü Lokale Dienste->Überwachung->Hosts. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion Überwachen berücksichtigt werden. Über die Konfiguration der IP-Adresse zur Nachverfolgung im Menü Lastverteilung->Lastverteilungsgruppen->Erweiterte Einstellungen erfolgt die Verknüpfung zwischen der Lastverteilungsfunktion und der Host-Überwachungsfunktion. Der Lastverteilungsstatus der Schnittstelle wechselt nun in Abhängigkeit vom Status des zugewiesenen Host-Überwachungseintrages.</p> <p>Wählen Sie die IP-Adresse der Route, die überwacht werden soll.</p> <p>Sie können unter den IP-Adressen wählen, die Sie im Menü Lokale Dienste->Überwachung->Hosts->Neu unter Überwachte IP-Adresse eingegeben haben und die mit Hilfe des Feldes</p>

Feld	Beschreibung
	Auszuführende Aktion überwacht werden (Aktion = <i>überwachen</i>) .

10.4.2 Special Session Handling

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

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

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

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

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

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

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

10.4.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<p>Wählen Sie aus, ob Special Session Handling aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Beschreibung	<p>Geben Sie eine Bezeichnung für den Eintrag ein.</p>
Dienst	<p>Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Der Standardwert ist <i>Benutzerdefiniert</i>.</p>
Protokoll	<p>Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Ziel-IP-Adresse/Netzmaske	<p>Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	<p>Geben Sie, falls gewünscht, eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein.</p> <p>Mögliche Werte:</p>

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

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Unveränderliche Para-	Legen Sie fest, ob die beiden Parameter Zieladresse und Ziel-

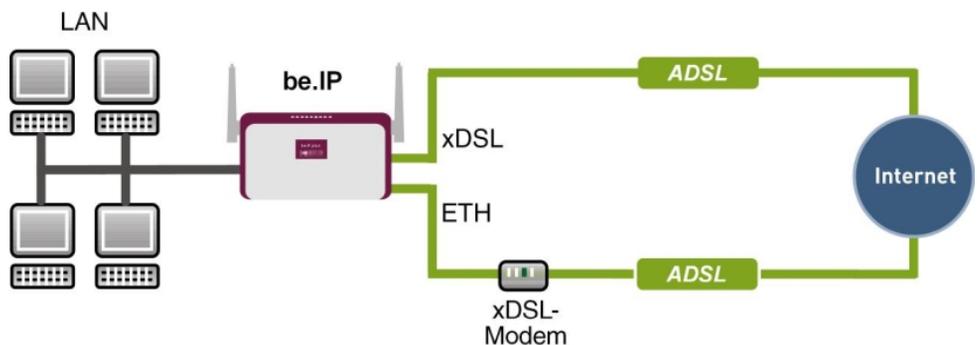
Feld	Beschreibung
meter	<p>port bei später gesendeten Datenpaketen denselben Wert haben müssen wie beim ersten Datenpaket, d. h. ob die nachfolgenden Datenpakete über denselben Zielport zur selben Zieladresse geroutet werden müssen.</p> <p>Standardmäßig sind die beiden Parameter Zieladresse und Zielport aktiv.</p> <p>Belassen Sie die Voreinstellung <i>Aktiviert</i> bei einem oder bei beiden Parametern, so muss der Wert des jeweiligen Parameters bei den später gesendeten Datenpaketen derselbe sein wie beim ersten Datenpaket.</p> <p>Sie können, falls gewünscht, einen oder beide Parameter deaktivieren.</p> <p>Der Parameter Quell-IP-Adresse muss bei später gesendeten Datenpaketen immer denselben Wert haben wie beim ersten Datenpaket. Er kann daher nicht deaktiviert werden.</p>

10.4.3 Lastverteilung - Konfigurationsbeispiel

Voraussetzungen

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

Beispielszenario



Konfigurationsziel

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



Hinweis

Beim Aufbau der ADSL-Verbindungen bezieht das Gateway neben der öffentlichen IP-Adresse auch die IP-Adressen der DNS-Server zur Namensauflösung von dem konfigurierten Internet-Provider. Vor allem bei der Verwendung von unterschiedlichen Internet-Providern müssen die DNS-Server verbindungspezifisch 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	<i>Internes ADSL-Modem</i>
Beschreibung	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. <i>ADSL-1</i>
Typ	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>
Benutzername	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. <i>fes-te_ip@provider.de</i>
Passwort	Assistenten->Internetzugang->Internetverbindungen->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->Internetverbindungen->Neu->Weiter	z. B. <i>ADSL-2</i>
Physischer Ethernet-Port	Assistenten -> Internetzugang->Internetverbindungen->Neu->Weiter	z. B. <i>ETH5</i>
Typ	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	<i>Benutzerdefiniert</i>
Benutzername	Assistenten->Internetzugang->Internetverbindungen->Neu->Weiter	z. B. <i>#0001@t-online.de</i>
Passwort	Assistenten->Internetzugang->Internetverbindungen->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>
Schnittstelle	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	<i>WAN_ADSL-2</i>
Verteilungsverhältnis	Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu->Hinzufügen	<i>50</i>

Special Session Handling

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

Feld	Menü	Wert
Special Handling Timer	Netzwerk->Lastverteilung->Special Session Handling->Neu	900 Sekunden

10.5 QoS

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

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen
- Daten klassifizieren
- Daten priorisieren

10.5.1 IPv4/IPv6-Filter

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

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

10.5.1.1 Neu

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

Das Menü **Netzwerk->QoS->IPv4/IPv6-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Der Standardwert ist <i>any</i>.</p>
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Wählen Sie einen Typ aus.</p> <p>Mögliche Werte: <i>Beliebig, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply</i>.</p> <p>Siehe RFC 792.</p> <p>Der Standardwert ist <i>Beliebig</i>.</p>
Verbindungsstatus	<p>Bei Protokoll = <i>TCP</i> können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.
IPv4-Zieladresse/-netzmaske	<p>Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein.

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

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

Feld	Beschreibung
	<p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7. Wertebereich 0 bis 7.</p> <p>Der Standardwert ist <i>Nicht beachten</i>.</p>

10.5.2 QoS-Klassifizierung

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

10.5.2.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Klassenplan	<p>Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an. • <i><Name des Klassenplans></i>: Zeigt einen bereits angelegten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	<p>Nur für Klassenplan = <i>Neu</i></p> <p>Geben Sie die Bezeichnung des Klassenplans ein.</p>
Filter	<p>Wählen Sie ein IP-Filter aus.</p> <p>Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll.</p> <p>Bei einem bestehenden Klassenplan wählen Sie das Filter, das</p>

Feld	Beschreibung
	<p>an den Klassenplan angehängt werden soll.</p> <p>Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü Netzwerk->QoS->QoS-Filter konfiguriert sein.</p>
Richtung	<p>Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Eingehend</i>: Eingehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet. • <i>Ausgehend</i> (Standardwert): Ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet. • <i>Beide</i>: Eingehende und ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet.
High-Priority-Klasse	<p>Aktivieren oder deaktivieren Sie die High-Priority-Klasse. Wenn die High-Priority-Klasse aktiv ist, werden die Datenpakete der Klasse mit der höchsten Priorität zugeordnet, die Priorität 0 wird automatisch gesetzt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Klassen-ID	<p>Nur für High-Priority-Klasse nicht aktiv.</p> <p>Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zuweist.</p> <div data-bbox="539 1277 1315 1465" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p> Hinweis</p> <p>Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.)</p> </div> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 254.</p>
DSCP/Traffic-Class-Filter setzen	<p>Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (Klassen-ID) setzen bzw.</p>

Feld	Beschreibung
(Layer 3)	<p>ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erhalten</i> (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
Setze COS Wert (802.1p/Layer 2)	<p>Im Header der Ethernet-Pakete, die vom ausgewählten Filter erfasst werden, können Sie hier die Serviceklasse (Layer-2-Priorität) setzen/ändern.</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Der Standardwert ist <i>Erhalten</i>.</p>
Schnittstellen	<p>Nur für Klassenplan = <i>Neu</i></p> <p>Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.</p>

10.5.3 QoS-Schnittstellen/Richtlinien

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



Hinweis

Daten können nur ausgehend priorisiert werden.

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

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

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

10.5.3.1 Neu

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

Das Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, für die QoS konfiguriert werden soll.
Priorisierungsalgorithmus	<p>Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausgewählten Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Priority Queueing</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. • <i>Weighted Round Robin</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird gemäß der Gewichtung (weight) der Queues verteilt. Ausnahme: High-Priority-Pakete

Feld	Beschreibung
	<p>werden immer vorrangig behandelt.</p> <ul style="list-style-type: none"> • <i>Weighted Fair Queueing</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird möglichst "fair" unter den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig bedient. • <i>Deaktiviert</i> (Standardwert): QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.
Traffic Shaping	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate in Senderichtung.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upload-Geschwindigkeit	<p>Nur für Traffic Shaping = 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>
Größe des Protokoll-Headers unterhalb Layer 3	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Benutzerdefiniert</i> Wert in Byte. <p>Mögliche Werte sind 0 bis 100.</p> <ul style="list-style-type: none"> • <i>Undefiniert</i> (<i>Protocol Header Offset=0</i>) (Standardwert) <p>Nur für Ethernet-Schnittstellen auswählbar</p> <ul style="list-style-type: none"> • <i>Ethernet</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Ethernet und VLAN</i> • <i>PPP over Ethernet</i> • <i>PPPoE und VLAN</i> <p>Nur für IPSec-Schnittstellen auswählbar:</p> <ul style="list-style-type: none"> • <i>IPSec über Ethernet</i> • <i>IPSec über Ethernet und VLAN</i> • <i>IPSec via PPP over Ethernet</i> • <i>IPSec via PPPoE und VLAN</i>
Verschlüsselungsmethode	<p>Nur wenn als Schnittstelle ein IPSec Peer gewählt ist, Traffic Shaping <i>Aktiviert</i> ist und die Größe des Protokoll-Headers unterhalb Layer 3 nicht <i>Undefiniert (Protocol Header Offset=0)</i> ist.</p> <p>Wählen Sie die Verschlüsselungsmethode, die für die IPSec-Verbindung genutzt wird. Der Verschlüsselungsalgorithmus bestimmt die Länge der Blockchiffre, die bei der Bandbreitenkalkulation berücksichtigt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DES, 3DES, Blowfish, Cast - (Cipher-Blockgröße = 64 Bit)</i> • <i>AES128, AES192, AES256, Twofish - (Cipher-Blockgröße = 128 Bit)</i>
Real Time Jitter Control	<p>Nur für Traffic Shaping = aktiviert</p> <p>Real Time Jitter Control führt zu einer Optimierung des Latenzverhaltens bei der Weiterleitung von Real-Time-Datagrammen. Die Funktion sorgt für eine Fragmentierung großer Datenpakete in Abhängigkeit von der verfügbaren Upload-Bandbreite.</p> <p>Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s).</p> <p>Aktivieren oder deaktivieren Sie Real Time Jitter Control.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
Kontrollmodus	<p>Nur für Real Time Jitter Control = aktiviert.</p> <p>Wählen Sie den Modus für die Optimierung der Sprachübertragung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream erkannt wurde. • <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt. • <i>Nur kontrollierte RTP-Streams</i>: Dieser Modus wird verwendet, wenn entweder das VoIP Application Layer Gateway (ALG) oder das VoIP Media Gateway (MGW) aktiv ist. Die Aktivierung des Real-Time-Jitter-Control-Mechanismus erfolgt über die Kontrollinstanzen ALG oder MGW. • <i>Immer</i>: Der Real-Time-Jitter-Control-Mechanismus ist immer aktiv, auch wenn keine Real-Time-Daten geroutet werden.

Felder im Menü Queues/Richtlinie

Feld	Beschreibung
Queues/Richtlinien	<p>Konfigurieren Sie die gewünschten QoS-Queues.</p> <p>Für jede angelegte Klasse aus dem Klassenplan, die mit der gewählten Schnittstelle verbunden ist, wird automatisch eine Queue erzeugt und hier angezeigt (nur für ausgehend klassifizierten Datenverkehr sowie für in beide Richtungen klassifizierten Datenverkehr).</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu. Das Menü Queue/Richtlinie bearbeiten öffnet sich.</p> <p>Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag DEFAULT mit der niedrigsten Priorität 255 erstellt.</p>

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

Felder im Menü Queue/Richtlinie bearbeiten

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung der Queue/Richtlinie an.
Ausgehende Schnittstelle	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
Priorisierungsqueue	<p>Wählen Sie den Typ für die Priorisierung der Queue aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Klassenbasiert</i> (Standardwert): Queue für "normal"-klassifizierte Daten. • <i>Hohe Priorität</i>: Queue für "high-priority"- klassifizierte Daten. • <i>Standard</i>: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	<p>Nur für Priorisierungsqueue = <i>Klassenbasiert</i></p> <p>Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll.</p> <p>Dazu muss vorher im Menü Netzwerk->QoS->QoS-Klassifizierung mindestens eine Klassen-ID vergeben worden sein.</p>
Priorität	<p>Nur für Priorisierungsqueue = <i>Klassenbasiert</i></p> <p>Wählen Sie die Priorität der Queue. Mögliche Werte sind <i>1 (hohe Priorität) bis 254 (niedrige Priorität)</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
Gewichtung	<p>Nur für Priorisierungsalgorithmus = <i>Weighted Round Robin</i> oder <i>Weighted Fair Queueing</i></p> <p>Wählen Sie die Gewichtung der Queue. Mögliche Werte sind <i>1 bis 254</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
RTT-Modus (Realtime-Traffic-Modu	Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten.

Feld	Beschreibung
s)	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen.</p> <p>Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.</p>
Traffic Shaping	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung.</p> <p>Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.)</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upload-Geschwindigkeit	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie eine maximale Datenrate in kBit pro Sekunde für die ausgewählte Schnittstelle ein.</p> <p>Mögliche Werte sind 0 bis 1000000.</p> <p>Der Standardwert ist 0, d. h. es erfolgt keine Begrenzung, die ausgewählte Schnittstelle kann ihre maximale Bandbreite belegen.</p>
Überbuchen zugelassen	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Aktivieren oder deaktivieren Sie die Funktion. Die Funktion steuert das Bandbreitenbegrenzungsverhalten.</p> <p>Bei aktiviertem Überbuchen zugelassen kann die Bandbreitenbegrenzung überschritten werden, die für die Queue eingestellt ist, sofern freie Bandbreite auf der Schnittstelle vorhanden ist.</p>

Feld	Beschreibung
	<p>Bei deaktiviertem Überbuchen zugelassen kann die Queue niemals Bandbreite über die eingestellte Bandbreitenbegrenzung hinaus belegen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Burst-Größe	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie die maximale Anzahl an Bytes ein, die kurzfristig noch übertragen werden darf, wenn die für diese Queue erlaubte Datenrate bereits erreicht ist.</p> <p>Mögliche Werte sind <i>0</i> bis <i>64000</i>.</p> <p>Der Standardwert ist <i>0</i>.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Dropping-Algorithmus	<p>Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Tail Drop</i> (Standardwert): Das neu hinzugekommene Paket wird verworfen. • <i>Head Drop</i>: Das älteste Paket in der Queue wird verworfen. • <i>Random Drop</i>: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Vermeidung von Datenstau (RED)	<p>Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen.</p> <p>Pakete, deren Datengröße zwischen Min. Queue-Größe und Max. Queue-Größe liegt, werden vorbeugend verworfen, um einen Queue-Überlauf zu verhindern (RED=Random Early Detection). Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine insgesamt kleinere Queue, sodass selbst Traffic-Bursts meist ohne größere Paketverluste übertragen werden</p>

Feld	Beschreibung
	<p>können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Min. Queue-Größe	<p>Geben Sie den unteren Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 0.</p>
Max. Queue-Größe	<p>Geben Sie den oberen Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 16384.</p>

10.6 Zugriffsregeln

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

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

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

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

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

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

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

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

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

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

oder

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

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

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

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

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.



Achtung

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

Greifen Sie zur Filter-Konfiguration möglichst über die serielle Konsolen-Schnittstelle (nicht für alle Geräte verfügbar) oder mit ISDN-Login auf Ihr Gateway zu.

10.6.1 Zugriffsfilter

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

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

10.6.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>Echo reply</i> • <i>Destination unreachable</i> • <i>Source quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time exceeded</i> • <i>Timestamp</i> • <i>Timestamp reply</i> <p>Der Standardwert ist <i>Beliebig</i>.</p> <p>Siehe RFC 792.</p>
Verbindungsstatus	<p>Nur bei Protokoll = <i>TCP</i></p> <p>Sie können ein Filter definieren, das den Status von TCP-Verbindung berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete. • <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden.
IPv4-Zieladresse/-netzmaske	<p>Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p>

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

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

10.6.2 Regelketten

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

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

10.6.2.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Zulassen, wenn Filter nicht passt</i>: Paket annehmen, wenn das Filter nicht passt. • <i>Verweigern, wenn Filter passt</i>: Paket abweisen, wenn das Filter passt. • <i>Verweigern, wenn Filter nicht zutrifft</i>: Paket abweisen, wenn das Filter nicht passt. • <i>Nicht beachten</i>: Nächste Regel anwenden.

Um die Regeln einer Regelkette in eine andere Reihenfolge zu bringen, wählen Sie im Listenmenü bei dem Eintrag, der verschoben werden soll, die Schaltfläche . Daraufhin öffnet sich ein Dialog, bei dem Sie unter **Verschieben** entscheiden können, ob der Eintrag *unter* (Standardwert) oder *über* eine andere Regel dieser Regelkette verschoben wird.

10.6.3 Schnittstellenzuweisung

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

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

10.6.3.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.
Verwerfen ohne Rückmeldung	<p>Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll.</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert) : Der Absender wird nicht informiert. • <i>Deaktiviert</i>: Der Absender erhält eine ICMP-Nachricht.

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

10.7 Drop-In

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

Die Netzwerkkomponenten eines Segments, die an einem Anschluss angeschlossen sind, können dann gemeinsam z. B. mit einer Firewall geschützt werden. Der Datenverkehr von Netzwerkkomponenten zwischen einzelnen Segmenten, die unterschiedlichen Ports zugeordnet sind, wird dann entsprechend der konfigurierten Firewall-Regeln kontrolliert.

10.7.1 Drop-In-Gruppen

Im Menü **Netzwerk->Drop-In->Drop-In-Gruppen** wird eine Liste aller konfigurierten **Drop-In-Gruppen** angezeigt. Eine **Drop-In**-Gruppe repräsentiert jeweils ein Netzwerk.

10.7.1.1 Neu

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

Das Menü **Netzwerk->Drop-In->Drop-In-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine eindeutige Bezeichnung für die Drop-In -Gruppe ein.

Feld	Beschreibung
Modus	<p>Wählen Sie, welcher Modus für die Übermittlung der MAC-Adressen von Netzwerkkomponenten verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Transparent</i> (Standardwert): ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet. • <i>Proxy</i>: ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden mit der MAC-Adresse der entsprechenden Schnittstelle weitergeleitet.
Vom NAT ausnehmen (DMZ)	<p>Hier können Sie Datenverkehr von NAT ausnehmen.</p> <p>Verwenden Sie diese Funktion, um zum Beispiel die Erreichbarkeit bestimmter Web-Server in einer DMZ sicherzustellen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Netzwerkconfiguration	<p>Wählen Sie aus, auf welche Weise dem Drop-In-Netzwerk eine IP-Adresse/Netzmaske zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert) • <i>DHCP</i>
Netzwerkadresse	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die Netzwerkadresse des Drop-In-Netzwerks ein.</p>
Netzmaske	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die zugehörige Netzmaske ein.</p>
Lokale IP-Adresse	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die lokale IP-Adresse ein. Diese IP-Adresse muss für alle Ethernet-Ports eines Netzwerks identisch sein.</p>
DHCP Client an Schnittstelle	<p>Nur für Netzwerkconfiguration = <i>DHCP</i></p> <p>Hier können Sie eine Ethernet-Schnittstelle Ihres Routers wäh-</p>

Feld	Beschreibung
	<p>len, die als DHCP-Client agieren soll.</p> <p>Diese Einstellung benötigen Sie zum Beispiel, wenn der Router Ihres Providers als DHCP-Server dient.</p> <p>Sie können unter den Schnittstellen wählen, welche Ihr Gerät zur Verfügung stellt, die Schnittstelle muss jedoch Mitglied der Drop-In-Gruppe sein.</p>
ARP Lifetime	<p>Legt die Zeitspanne fest, während derer ARP-Einträge im Cache gehalten werden.</p> <p>Der Standardwert ist <i>3600</i> Sekunden.</p>
DNS-Zuweisung über DHCP	<p>Das Gateway kann DHCP-Pakete, die die Drop-In-Gruppe durchlaufen, modifizieren und sich selbst als angebotenen DNS-Server eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Unverändert</i> (Standardwert)• <i>Eigene IP-Adresse</i>
Schnittstellenauswahl	<p>Wählen Sie alle Ports aus, die in der Drop-In-Gruppe (im Netzwerk) enthalten sein sollen.</p> <p>Fügen Sie mit Hinzufügen weitere Einträge hinzu.</p>

Kapitel 11 Routing-Protokolle

11.1 RIP

Die Einträge in der Routing-Tabelle können entweder statisch festgelegt werden oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-Informationen zwischen mehreren Geräten. Diesen Austausch regelt ein sogenanntes Routing-Protokoll, z. B. RIP (Routing Information Protocol). Standardmäßig ungefähr alle 30 Sekunden (dieser Wert kann in **Aktualisierungstimer** verändert werden) sendet ein Gerät Meldungen zu entfernten Netzwerken, wobei es Informationen aus seiner eigenen aktuellen Routing-Tabelle verwendet. Dabei wird immer die gesamte Routing-Tabelle ausgetauscht. Mit Triggered RIP findet nur ein Austausch statt, wenn sich Routing-Informationen geändert haben. In diesem Fall werden nur die geänderten Informationen versendet.

Durch Beobachtung der Informationen, die von anderen Geräten verschickt werden, werden neue Routen und kürzere Wege für bestehende Routen in der Routing-Tabelle gespeichert. Da Routen zwischen Netzwerken unerreichbar werden können, entfernt RIP Routen, die älter als 5 Minuten sind (d. h. Routen, die in den letzten 300 Sekunden - **Garbage Collection Timer** + **Routentimeout** - nicht verifiziert wurden). Mit Triggered RIP gelernte Routen werden jedoch nicht gelöscht.

Ihr Gerät unterstützt sowohl Version 1 als auch Version 2 von RIP, wahlweise einzeln oder gemeinsam.

11.1.1 RIP-Schnittstellen

Im Menü **Routing-Protokolle** -> **RIP** -> **RIP-Schnittstellen** wird eine Liste aller RIP-Schnittstellen angezeigt.

11.1.1.1 Bearbeiten

Für jede RIP-Schnittstelle sind über das -Menü die Optionen *Version in Senderichtung*, *Version in Empfangsrichtung* und *Routenankündigung* auswählbar.

Das Menü **Netzwerk** -> **RIP** -> **RIP-Schnittstellen** ->  besteht aus folgenden Feldern:

Felder im Menü RIP-Parameter für

Feld	Beschreibung
Version in Senderich-	Entscheiden Sie, ob über RIP Routen propagiert werden sollen,

Feld	Beschreibung
Sendung	<p>und wenn ja, wählen Sie die RIP-Version für das Senden von RIP-Paketen über die Schnittstelle in Senderichtung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): RIP ist nicht aktiv. • <i>RIP V1</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • <i>RIP V2</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • <i>RIP V1/V2</i>: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • <i>RIP V2 Multicast</i>: Ermöglicht das Senden von RIP-V2-Nachrichten über die Multicast-Adresse 224.0.0.9. • <i>RIP V1 Triggered</i>: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • <i>RIP V2 Triggered</i>: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP).
Version in Empfangsrichtung	<p>Entscheiden Sie, ob über RIP Routen importiert werden sollen und wenn ja, wählen Sie die RIP-Version für das Empfangen von RIP-Paketen über die Schnittstelle in Empfangsrichtung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): RIP ist nicht aktiv. • <i>RIP V1</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • <i>RIP V2</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • <i>RIP V1/V2</i>: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • <i>RIP V1 Triggered</i>: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • <i>RIP V2 Triggered</i>: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet

Feld	Beschreibung
	(Triggered RIP).
Routenankündigung	<p>Wählen Sie aus, wann ggf. aktivierte Routing-Protokolle (z. B. RIP) die für diese Schnittstelle definierten IP-Routen propagieren sollen.</p> <p>Beachten Sie: Diese Einstellung hat keinen Einfluss auf die oben erwähnte Schnittstellen-spezifische RIP-Konfiguration.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv oder Ruhend</i> (nicht für LAN-Schnittstellen, Schnittstellen im Bridge-Modus und Schnittstellen für Standleitungen): Routen werden propagiert, wenn der Status der Schnittstelle auf aktiv oder bereit steht. • <i>Nur aktiv</i> (Standardwert): Routen werden nur propagiert, wenn der Status der Schnittstelle auf aktiv steht. • <i>Immer</i>: Routen werden immer propagiert unabhängig vom Betriebsstatus.

11.1.2 RIP-Filter

Im diesem Menü können Sie exakt festlegen, welche Routen exportiert oder importiert werden sollen oder nicht.

Hierbei können Sie nach folgenden Strategien vorgehen:

- Sie deaktivieren das Importieren bzw. Exportieren bestimmter Routen explizit. Der Import bzw. Export aller anderen Routen, die nicht aufgeführt werden, bleibt erlaubt.
- Sie aktivieren das Importieren bzw. Exportieren bestimmter Routen explizit. Dann müssen Sie den Import bzw. Export aller anderen Routen auch explizit deaktivieren. Dieses erreichen Sie mittels eines Filters für **IP-Adresse/Netzmaske** = kein Eintrag (dies entspricht der IP-Adresse 0.0.0.0 mit der Netzmaske 0.0.0.0). Damit dieses Filter als letztes angewendet wird, muss es an der niedrigsten Position eingeordnet werden.

Ein Filter für eine Standard-Route konfigurieren Sie mit folgenden Werten:

- **IP-Adresse/Netzmaske** = für IP-Adresse keine Eintrag (dies entspricht der IP-Adresse 0.0.0.0), für Netzmaske = 255.255.255.255

Im Menü **Routing-Protokolle->RIP->RIP-Filter** wird eine Liste aller RIP-Filter angezeigt.

Mit der Schaltfläche  können Sie vor dem Listeneintrag ein weiteres Filter einfügen. Es

öffnet sich das Konfigurationsmenü zum Erstellen eines neuen Filters.

Mit der Schaltfläche  können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position das Filter verschoben werden soll.

11.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere RIP-Filter einzurichten.

Das Menü **Routing-Protokolle->RIP->RIP-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie aus, für welche Schnittstelle die zu konfigurierende Regel gilt.
IP-Adresse/Netzmaske	Geben Sie die IP-Adresse und Netzmaske ein, auf welche die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen. Die Regeln für eingehende und ausgehende RIP-Pakete (Importieren oder Exportieren) müssen für dieselbe IP-Adresse getrennt konfiguriert werden. Sie können einzelne Host-Adressen ebenso angeben wie Netz-adressen.
Richtung	Wählen Sie aus, ob das Filter für das Exportieren oder das Importieren von Routen gilt. Mögliche Werte: <ul style="list-style-type: none"> • <i>Importieren</i> (Standardwert) • <i>Exportieren</i>
Metrik-Offset für Aktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Aktiv" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Aktiv" ist. Mögliche Werte sind -16 bis 16 . Der Standardwert ist 0 .
Metrik-Offset für Inakti-	Wählen Sie den Wert aus, der der Metrik der Route beim Import

Feld	Beschreibung
ve Schnittstellen	<p>hinzugefügt werden soll, wenn der Status der Schnittstelle "Ruhend" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Ruhend" ist.</p> <p>Mögliche Werte sind -16 bis 16.</p> <p>Der Standardwert ist 0.</p>

11.1.3 RIP-Optionen

Das Menü **Routing-Protokolle->RIP->RIP-Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale RIP-Parameter

Feld	Beschreibung
RIP-UDP-Port	<p>Die Einstellungsmöglichkeit des UDP-Ports, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, dass Ihr Gerät auf einem Port sendet und lauscht, den keine weiteren Geräte benutzen. Der Standardwert 520 sollte eingestellt bleiben.</p>
Standardmäßige Routenverteilung	<p>Wählen Sie aus, ob die Standard-Route Ihres Geräts über RIP-Updates propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Poisoned Reverse	<p>Wählen Sie das Verfahren zur Verhinderung von Routing-Schleifen.</p> <p>Bei Standard RIP werden die gelernten Routen über alle Schnittstellen mit aktiviertem RIP SENDEN propagiert. Bei Poisoned Reverse propagiert Ihr Gerät jedoch über die Schnittstelle, über die es die Routen gelernt hat, diese mit der Metrik (Next Hop Count) 16 ("Netz ist nicht erreichbar").</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
RFC 2453-Variabler Ti-	<p>Wählen Sie aus, ob für die in RFC 2453 beschriebenen Timer</p>

Feld	Beschreibung
mer	<p>diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für RIP V2 (RFC 2453) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Wenn Sie die Funktion deaktivieren, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.</p>
RFC 2091-Variabler Timer	<p>Wählen Sie aus, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für Triggered RIP (RFC 2091) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion nicht aktiv ist, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.</p>

Felder im Menü Timer für RIP V2 (RFC 2453)

Feld	Beschreibung
Aktualisierungstimer	<p>Nur für RFC 2453-Variabler Timer = Aktiviert</p> <p>Nach Ablauf dieses Zeitraums wird eine RIP-Aktualisierung gesendet.</p> <p>Der Standardwert ist <i>30</i> (Sekunden).</p>
Routentimeout	<p>Nur für RFC 2453-Variabler Timer = Aktiviert</p> <p>Nach der letzten Aktualisierung einer Route wird der Routentimeout aktiv.</p> <p>Nach dessen Ablauf wird die Route deaktiviert und der Garbage Collection Timer gestartet.</p> <p>Der Standardwert ist <i>180</i> (Sekunden).</p>
Garbage Collection Timer	<p>Nur für RFC 2453-Variabler Timer = Aktiviert</p> <p>Der Garbage Collection Timer wird gestartet, sobald der Routentimeout abgelaufen ist.</p>

Feld	Beschreibung
	<p>Nach Ablauf dieses Zeitraums wird die ungültige Route aus der IPROUTETABLE gelöscht, sofern keine Aktualisierung für die Route erfolgt.</p> <p>Der Standardwert ist <i>120</i> (Sekunden).</p>

Felder im Menü Timer für Triggered RIP (RFC 2091)

Feld	Beschreibung
<p>Hold Down Timer</p>	<p>Nur für RFC 2091-Variabler Timer = <i>Aktiviert</i></p> <p>Der Hold Down Timer wird aktiv, sobald Ihr Gerät eine unerreichbare Route (Metric 16) erhält. Nach Ablauf dieses Zeitraums wird die Route ggf. gelöscht.</p> <p>Der Standardwert ist 120 (in Sekunden).</p>
<p>Retransmission Timer</p>	<p>Nur für RFC 2091-Variabler Timer = <i>Aktiviert</i></p> <p>Nach Ablauf dieses Zeitraums werden Update-Request- bzw. Update-Response-Pakete erneut versendet, bis ein Update-Flush- bzw. Update-Acknowledge-Paket eintrifft.</p> <p>Der Standardwert ist 5 (in Sekunden).</p>

Kapitel 12 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.

12.1 Allgemein

12.1.1 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
Multicast-Routing	Wählen Sie aus, ob Multicast-Routing verwendet werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

12.2 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.

12.2.1 IGMP

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

12.2.1.1 Bearbeiten oder Neu

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

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

Felder im Menü IGMP-Einstellungen

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

Feld	Beschreibung
	<p>Möglich Werte sind 2 bis 8.</p> <p>Der Standardwert ist 2.</p>
Antwortintervall (Letztes Mitglied)	<p>Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet.</p> <p>Wenn Sie den Wert verkleinern, wird schneller erkannt, ob das letzte Mitglied eine Gruppe verlassen hat und somit keine Pakete mehr für diese Gruppe an diese Schnittstelle weitergeleitet werden müssen.</p> <p>Möglich Werte sind 0,0 bis 25,0.</p> <p>Der Standardwert ist 1,0.</p>
Maximale Anzahl der IGMP-Statusmeldungen	<p>Limitieren Sie die Anzahl der Reports/Queries pro Sekunde für die gewählte Schnittstelle.</p>
Modus	<p>Wählen Sie aus, ob die hier definierte Schnittstelle nur im Host-Modus oder auch im Routing Modus arbeitet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Routing</i> (Standardwert): Die Schnittstelle wird im Routing-Modus betrieben. • <i>Host</i>: Die Schnittstelle wird nur im Host-Modus betrieben.

IGMP Proxy

Mit IGMP Proxy können mehrere lokal angeschlossene Schnittstellen als ein Subnetz zu einem benachbarten Router simuliert werden. Auf der IGMP-Proxy-Schnittstelle eingehende Queries werden in die lokalen Subnetze weitergeleitet. Lokale Reports werden auf der IPGM-Proxy-Schnittstelle weitergeleitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IGMP Proxy	<p>Wählen Sie aus, ob Ihr Gerät die IGMP-Meldungen der Hosts im Subnetz über seine definierte Proxy-Schnittstelle weiterleiten soll.</p>

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

12.2.2 Optionen

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
IGMP-Status	Wählen Sie den IGMP-Status aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Multicast wird für Hosts automatisch eingeschaltet, wenn diese Anwendungen öffnen, die Multicast verwenden. • <i>Aktiv</i>: Multicast ist immer aktiv. • <i>Inaktiv</i>: Multicast ist immer inaktiv.
Modus	Nur für IGMP-Status = <i>Aktiv</i> oder <i>Auto</i> Wählen Sie den Multicast-Modus aus.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Kompatibilitätsmodus</i> (Standardwert): Der Router verwendet IGMP Version 3. Bemerkt er eine niedrigere Version im Netz, verwendet er die niedrigste Version, die er erkennen konnte. • <i>Nur Version 3</i>: Nur IGMP Version 3 wird verwendet.
Maximale Gruppen	<p>Geben Sie ein, wie viele Gruppen sowohl intern als auch in Reports maximal möglich sein sollen.</p> <p>Der Standardwert ist <i>64</i>.</p>
Maximale Quellen	<p>Geben Sie die maximale Anzahl der Quellen ein, die in den Reports der Version 3 spezifiziert sind, als auch die maximale Anzahl der intern verwalteten Quellen pro Gruppe.</p> <p>Der Standardwert ist <i>64</i>.</p>
Maximale Anzahl der IGMP-Statusmeldungen	<p>Geben Sie die maximale Anzahl der insgesamt möglichen eingehenden Queries bzw. Meldungen pro Sekunde ein.</p> <p>Der Standardwert ist <i>0</i>, d. h. die Anzahl der IGMP-Statusmeldungen ist nicht begrenzt.</p>

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.

12.3 Weiterleiten

12.3.1 Weiterleiten

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

12.3.1.1 Neu

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

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

Felder im Menü Basisparameter

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

12.4 PIM

Protocol Independent Multicast (PIM) ist ein Multicast-Routingverfahren, das dynamisches Routing von Multicast-Paketen ermöglicht. Bei PIM wird die Informationsverteilung über einen zentralen Punkt geregelt, der als Rendezvous Point bezeichnet wird. Dorthin werden die Datenpakete initial geleitet und auf Anfrage anderer Router den Empfängern zur Verfügung gestellt.

Bei Multicast-Routing-Protokollen unterscheidet man grundsätzlich zwischen Sparse Mode und Dense Mode. Beim Dense Mode werden alle Pakete weitergeleitet und nur die Pakete an Gruppen verworfen, die explizit abbestellt wurden. Beim Sparse Mode werden nur Pa-

kete an Gruppen weitergeleitet, die von diesen bestellt wurden. Ihr Gerät verwendet PIM im Sparse Mode.

12.4.1 PIM-Schnittstellen

Im Menü **Multicast->PIM->PIM-Schnittstellen** wird eine Liste aller PIM-Schnittstellen angezeigt.

12.4.1.1 Bearbeiten oder Neu

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

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

Felder im Menü PIM-Schnittstelleneinstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle, die für PIM benutzt werden soll, d.h. über die Multicast Routing betrieben werden soll.
PIM-Modus	Zeigt den Modus an, der für PIM benutzt wird. Ihr Gerät verwendet den PIM Sparse Mode. Der Eintrag kann nicht verändert werden.
Stub Interface Mode	Bestimmen Sie, ob die Schnittstelle für PIM-Datenpakete genutzt werden soll. Mit diesem Parameter können Sie z. B. eine Schnittstelle für IGMP benutzen, aber vor (gefälschten) PIM-Nachrichten schützen. Ist diese Funktion deaktiviert (Standardwert), werden die PIM-Datenpakete für diese Schnittstelle blockiert. Wenn die Funktion aktiv ist, ist die Schnittstelle für die PIM-Datenpakete freigegeben.
Designated-Router-Priorität	Bestimmen Sie den Wert der Designated Router Priority, der in die Option Designated-Router-Priorität eingefügt wird. Je höher dieser Wert ist, desto größer ist die Wahrscheinlichkeit, dass der entsprechende Router als Designated Router verwendet wird. Der Standardwert ist <i>1</i> .

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Hello-Intervall	<p>Bestimmen Sie, in welchen Zeitabständen (in Sekunden) PIM Hello Messages über diese Schnittstelle gesendet werden.</p> <p>Der Wert 0 bedeutet, dass auf dieser Schnittstelle keine PIM Hello Messages gesendet werden.</p> <p>Wertebereich: 0 bis 18000 Sekunden.</p> <p>Der Standardwert ist 30.</p>
Triggered-Hello-Intervall	<p>Bestimmen Sie, wie lange maximal gewartet werden darf, bis eine PIM Hello Message nach einem Systemstart oder nach einem Neustart eines Nachbarn gesendet wird.</p> <p>Der Wert 0 bedeutet, dass PIM Hello Messages immer sofort gesendet werden.</p> <p>Wertebereich: 0 bis 60 Sekunden.</p> <p>Der Standardwert ist 5.</p>
Hello Hold Time	<p>Bestimmen Sie den Wert des Holdtime Feldes in einer PIM Hello Message.</p> <p>Daraus ergibt sich, wie lange ein PIM-Router als verfügbar gilt. Sobald die Hello Hold Time abgelaufen ist und keine weitere Hello Message empfangen wurde, wird dieser PIM-Router als nicht erreichbar betrachtet.</p> <p>Wertebereich: 0 bis 65535 Sekunden.</p> <p>Der Standardwert ist 105.</p>
Join/Prune-Intervall	<p>Bestimmen Sie die Häufigkeit, mit der PIM Join/Prune Messages auf der Schnittstelle gesendet werden sollen.</p> <p>Der Wert 0 bedeutet, dass auf dieser Schnittstelle keine periodischen PIM Join/Prune Messages gesendet werden.</p> <p>Wertebereich: 0 bis 18000 Sekunden.</p> <p>Der Standardwert ist 60.</p>
Join/Prune Hold Time	<p>Bestimmen Sie den Wert, der in das Holdtime Feld einer PIM</p>

Feld	Beschreibung
	<p>Join/Prune Message eingefügt wird.</p> <p>Dies ist die Zeitspanne, die ein Empfänger den Join/Prune State halten muss.</p> <p>Wertebereich: 0 bis 65535 Sekunden.</p> <p>Der Standardwert ist 210.</p>
Propagation Delay	<p>Bestimmen Sie den Wert, der in das Propagation Delay Feld eingefügt wird. Dieses Feld ist ein Bestandteil der LAN Prune Delay Option in den PIM Hello Messages, die auf dieser Schnittstelle gesendet werden.</p> <p>Propagation Delay und Override Interval stellen die sogenannten LAN-Prune-Delay-Einstellungen dar. Sie bewirken eine verzögerte Verarbeitung von Prune-Messages bei Upstream Routern.</p> <p>Wenn Propagation Delay zu klein ist, kann es zum Abbruch der Übertragung von Multicast-Paketen kommen, bevor ein Downstream Router eine Prune Override Message geschickt hat.</p> <p>Wertebereich: 0 bis 32 Sekunden.</p> <p>Der Standardwert ist 1.</p>
Override Interval	<p>Bestimmen Sie den Wert, den das Gateway in das Feld Override Interval der LAN Prune Delay Option einfügt.</p> <p>Override Interval bestimmt, wie lange ein Downstream Router höchstens warten darf, bis er eine Prune Override Message schickt.</p> <p>Wertebereich: 0 bis 65 Sekunden.</p> <p>Der Standardwert ist 3.</p>

12.4.2 PIM-Rendezvous-Punkte

Im Menü **Multicast->PIM->PIM-Rendezvous-Punkte** können Sie festlegen, welcher Rendezvous Point für welche Gruppen zuständig sein soll.

Es wird eine Liste aller PIM Rendezvous Points angezeigt.

12.4.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um PIM Rendezvous Points zu konfigurieren.

Das Menü **Multicast->PIM->PIM-Rendezvous-Punkte->Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen für PIM-Rendezvous-Punkt

Feld	Beschreibung
Multicast-Gruppenbereich	Wählen Sie die Multicast-Gruppen für den PIM Rendezvous Point aus. Sie können <ul style="list-style-type: none"> • <i>Alle Gruppen</i> (Standardwert) angeben oder mit Auswahl von • <i>Bestimmter Bereich</i> ein Multicast-Netzwerksegment spezifizieren.
Multicast-Gruppen-Adresse	Nur bei Multicast-Gruppenbereich = <i>Bestimmter Bereich</i> Geben Sie hier die IP-Adresse des Multicast-Netzwerksegments ein.
Präfixlänge der Multicast-Gruppe	Nur bei Multicast-Gruppenbereich = <i>Bestimmter Bereich</i> Geben Sie hier die Netzmaskenlänge des Multicast-Netzwerksegments ein. 224.0.0.0/4 bezeichnet das komplette Multicast Class D Segment. Wertebereich: 4 (Standardwert) bis 32.
Rendezvous Point IP-Adresse	Geben Sie die IP-Adresse oder den Hostnamen des Rendezvous Points ein.
Vorrang	Geben Sie den Wert für pimGroupMappingPrecedence ein, der für statische RP Konfigurationen verwendet werden soll. Dieses erlaubt die genaue Kontrolle darüber, welche Konfiguration durch diese statische Konfiguration ersetzt werden soll. Wenn die Funktion aktiviert ist, wird pimStaticRPOVERRIDE-Dyna-

Feld	Beschreibung
	<p>mic ignoriert. Die absoluten Werte dieses Objekts haben nur Bedeutung auf dem lokalen Router und müssen nicht mit anderen Routern abgestimmt werden.</p> <p>Die Funktion ist mit dem Standardwert 0 deaktiviert. Wenn die Funktion durch Setzen eines Wertes nicht 0 aktiviert wird, kann das verschiedene Auswirkungen auf andere Router haben. Verwenden Sie daher diese Funktion nicht, wenn eine genaue Kontrolle des Verhaltens des statischen RP nicht benötigt wird.</p>

12.4.3 PIM-Optionen

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
PIM-Status	<p>Wählen Sie aus ob PIM aktiviert werden soll. Mit Auswahl von <i>Aktivieren</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Keepalive-Periode	<p>Geben Sie die Zeitspanne in Sekunden ein, in der eine Keepalive Nachricht gesendet werden muss.</p> <p>Mögliche Werte: 0 bis 65535.</p> <p>Der Standardwert ist 210.</p>
Register Suppression Timer	<p>Geben Sie die Zeit in Sekunden an, nach der ein PIM Designated Router (DR) keine register-encapsulated Daten mehr zum Rendezvous Point (RP) schicken soll, nachdem die Register-Stop-Nachricht empfangen wurde. Dieses Objekt wird verwendet, um sowohl am DR als auch am RP Timer zu nutzen. Dieser Zeitraum wird in der PIM-SM Spezifikation Register_Suppression_Time genannt.</p> <p>Mögliche Werte: 0 bis 65535.</p> <p>Der Standardwert ist 60.</p>

Kapitel 13 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.

13.1 Internet + Einwählen

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

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

Wenn Sie einen Internetzugang herstellen wollen, müssen Sie eine Verbindung zu Ihrem Internet-Service-Provider (ISP) einrichten. Für Breitband-Internetzugänge stellt Ihr Gerät die Protokolle PPP-over-Ethernet (PPPoE) und PPP-over-PPTP 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
✓	verbunden
⌚	nicht verbunden (Wählverbindung); Verbindungsaufbau möglich
⊘	nicht verbunden (z. B. ist aufgrund eines Fehlers beim Aufbau einer ausgehenden Verbindung ein erneuter Versuch erst nach einer definierten Anzahl von Sekunden möglich)
✘	administrativ auf inaktiv gesetzt (deaktiviert); Verbindungsaufbau nicht möglich

Authentifizierung

Wenn ein Ruf eingeht, wird je nach Konfiguration eine PPP-Authentifizierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird. Dazu benötigt Ihr Gerät Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentifizierungsverhandlung ausgeführt werden soll, anschließend tragen Sie ein gemeinsames Passwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf Ihrem Gerät eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Default Route

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

NAT aktivieren

Mit Network Address Translation (NAT) verbergen Sie Ihr gesamtes Netzwerk nach außen hinter nur einer IP-Adresse. Für die Verbindung zum Internet Service Provider (ISP) sollten Sie dies auf jeden Fall tun.

Bei aktiviertem NAT sind zunächst nur ausgehende Sessions zugelassen. Um bestimmte Verbindungen von außen zu Hosts innerhalb des LANs zu erlauben, müssen diese explizit definiert und zugelassen werden.

Timeout bei Inaktivität festlegen

Der Timeout bei Inaktivität wird festgelegt, um die Verbindung bei Nichtbenutzen, d. h. wenn keine Nutzdaten mehr gesendet werden, automatisch zu trennen und somit ggf. Gebühren zu sparen.

Blockieren nach Verbindungsfehler

Mit dieser Funktion richten Sie eine Wartezeit für ausgehende Verbindungsversuche ein, nachdem ein Verbindungsversuch durch Ihr Gerät fehlgeschlagen ist.

13.1.1 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.

13.1.1.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	<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> <p>Wenn Sie für PPPoE Multilink zusätzlich ein externes Modem</p>

Feld	Beschreibung
	benutzen wollen, müssen Sie den Ethernet-Switch Ihres Geräts im Split-Port-Modus betreiben.
PPPoE-Ethernet-Schnittstelle	<p>Nur für PPPoE-Modus = <i>Standard</i></p> <p>Wählen Sie die Ethernet-Schnittstelle aus, die für eine Standard-PPPoE-Verbindung vorgegeben wird.</p> <p>Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist.</p> <p>Bei Verwendung des internen DSL-Modems, wählen Sie hier die in WAN->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle aus.</p> <p>Wählen Sie den Wert <i>Automatisch</i> um den automatischen VDSL-/ADSL-Modus zu unterstützen. In diesem Modus wird die Schnittstelle für der Internetzugang automatisch gewählt. Achten Sie darauf, dass für einen ADSL-Zugang im Menü ATM eine Schnittstelle angelegt sein muss, für einen VDSL-Zugang ist dies nicht notwendig.</p>
PPPoE-Schnittstelle für Mehrfachlink	<p>Nur für PPPoE-Modus= <i>Mehrfachverbindung</i></p> <p>Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die Hinzufügen-Schaltfläche, um weitere Einträge anzulegen.</p>
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
VLAN	Einige Internet Service Provider erfordern eine VLAN-ID. Aktivieren Sie diese Funktion, um unter VLAN-ID einen Wert eingeben zu können.
VLAN-ID	<p>Nur wenn VLAN aktiviert ist.</p> <p>Geben Sie die VLAN-ID ein, die Sie von Ihrem Provider erhalten haben.</p>
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	<p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold.</p> <p>Der Standardwert ist 300.</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 346 konfigurieren.</p>
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die statische IP-Adresse des Verbindungspartners ein.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob die gewählte PPPoE- Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Sicherheitsrichtlinie	<p>Nur für IPv6 = <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"> • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 346 konfigurieren.</p>
IPv6-Modus	<p>Nur für IPv6 = <i>Aktiviert</i></p> <p>Die gewählte PPPoE-Schnittstelle wird im Host-Modus betrieben.</p>
Router Advertisement annehmen	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <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>
DHCP-Client	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <i>Host</i></p> <p>Legen Sie fest, ob Ihr Gerät als DHCP-Client agieren soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
IPv6-Adressen	<p>Nur für IPv6 = <i>Aktiviert</i></p> <p>Sie können der gewählten Schnittstelle IPv6-Adressen zuordnen.</p> <p>Mit Hinzufügen 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 (IPv6-Modus = <i>Host</i>, Router Advertisement annehmen <i>Aktiviert</i> und DHCP-Client <i>Aktiviert</i>), werden seine IPv6-Adressen per SLAAC festgelegt. Sie brauchen keine IPv6-Adressen manuell zu konfigurieren, können aber auf Wunsch zusätzliche Adressen eintippen.</p> <p>Wenn Ihr Gerät im Router-Modus arbeitet (IPv6-Modus = <i>Router (Router-Advertisement übermitteln)</i>, Router Advertisement übertragen <i>Aktiviert</i> und DHCP-Server <i>Aktiviert</i>), so müssen Sie hier seine IPv6-Adressen konfigurieren.</p>

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

Felder im Menü Link-Präfix

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

Feld	Beschreibung
	<p>abgeleitet werden soll. Sie können unter den Allgemeinen Präfixen wählen, die unter Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes->Neu angelegt sind.</p>
<p>Automatische Subnetzerstellung</p>	<p>Nur wenn Art der Einrichtung = <i>Von Allgemeinem Präfix</i> und wenn ein Allgemeiner Präfix gewählt ist.</p> <p>Wählen Sie, ob das Subnetz automatisch erstellt werden soll. Bei der automatischen Subnetzerstellung wird für das erste Subnetz die ID <i>0</i> verwendet, für das zweite Subnetz die Subnetz-ID <i>1</i>, usw.</p> <p>Mögliche Werte für die Subnetz-ID 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>
<p>Subnetz-ID</p>	<p>Nur wenn Automatische Subnetzerstellung nicht aktiv ist.</p> <p>Geben Sie eine Subnetz-ID ein, um ein Subnetz zu definieren. Die Subnetz-ID beschreibt das vierte der vier 16-Bit-Felder eines Link-Präfix.</p> <p>Mögliche Werte sind <i>0</i> bis <i>65535</i>.</p> <p>Bei der Subnetzerstellung wird der eingegebene dezimale Wert in einen hexadezimalen Wert umgerechnet.</p>
<p>Link-Präfix</p>	<p>Nur für Art der Einrichtung = <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
Erzeugungsmethode	<p>Legen Sie fest, ob der Host-Anteil der IPv6-Adresse mittels EUI-64 automatisch aus der MAC-Adresse erzeugt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>EUI-64 setzt folgenden Prozess in Gang:</p> <ul style="list-style-type: none"> • Die hexadezimale 48-Bit MAC Adresse wird in 2 x 24 Bit geteilt. • In die entstandene Lücke wird <i>FFFF</i> eingefügt, um 64 Bit zu erhalten. • Die hexadezimale Schreibweise der 64 Bit wird in die duale Schreibweise umgewandelt. • Im ersten 8-Bit-Feld wird Bit 7 auf <i>1</i> gesetzt.
Statische Adressen	<p>Sie können, unabhängig von der automatischen Erzeugung, die unter Erzeugungsmethode festgelegt ist, mit Hinzufügen den Host-Anteil einer IPv6-Adresse oder mehrerer IPv6-Adressen manuell eingeben. Seine Länge ist mit <i>64</i> vorgegeben. Beginnen Sie die Eingabe mit <i>: :</i></p>

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

Felder im Menü **Erweiterte Einstellungen**

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

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

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

Felder im Menü Erweiterte IPv4-Einstellungen

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

13.1.2 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.

13.1.2.1 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
Beschreibung	Weisen Sie Ihrer Dual-Stack-Lite-Verbindung einen Namen zu.
IPv6-Schnittstelle	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.
AFTR	Geben Sie die IPv6-Adresse oder den Domännennamen Ihres AFTR (Address Family Transition Router) ein. Sie erhalten die Adresse vom Anbieter Ihrer IPv6-Internetverbindung.
Standardroute	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.

13.1.3 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.

13.1.3.1 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
Beschreibung	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.
PPTP-Ethernet-Schnittstelle	<p>Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden.</p> <p>Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist.</p> <p>Bei Verwendung des internen DSL-Modems, wählen Sie hier die in Physikalische Schnittstellen->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle z. B. <i>ethoa50-0</i>, aus.</p>
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutzdatenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte sind 0 bis 3600 (Sekunden). 0 deaktiviert den Timeout.</p> <p>Der Standardwert ist 300.</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 346 konfigurieren.</p>
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine temporär gültige IP-Adresse vom Provider. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Weisen Sie der PPTP-Schnittstelle eine IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.</p>

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist 60.</p>
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind 0 bis 100.</p> <p>Der Standardwert ist 5.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
PPTP-Adressmodus	<p>Zeigt den Adressmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i>: Die Lokale PPTP-IP-Adresse wird dem ausgewählten Ethernet-Port zugewiesen.
Lokale PPTP-IP-Adresse	<p>Weisen Sie der PPTP-Schnittstelle eine IP-Adresse zu, die als Quelladresse verwendet wird.</p> <p>Der Standardwert ist <i>10.0.0.140</i>.</p>
Entfernte PPTP-IP-Adresse	<p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p> <p>Der Standardwert ist <i>10.0.0.138</i>.</p>

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

13.1.4 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.

13.1.4.1 Bearbeiten oder Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

13.2 Real Time Jitter Control

Bei Telefongesprächen über das Internet haben Sprachdaten-Pakete normalerweise höchste Priorität. Trotzdem können bei geringer Bandbreite der Upload Verbindung während eines Telefongesprächs merkbare Verzögerungen bei der Sprachübertragung auftreten, wenn gleichzeitig andere Datenpakete geroutet werden.

Die Funktion Real Time Jitter Control löst dieses Problem. Um die "Leitung" für die Sprachdaten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

13.2.1 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.

13.2.1.1 Neu

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Schnittstelle	Legen Sie fest, für welche Schnittstellen die Sprachübertragung

Feld	Beschreibung
	optimiert werden soll.
Kontrollmodus	<p>Wählen Sie den Modus für die Optimierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Nur kontrollierte RTP-Streams</i> (Standardwert): Anhand der Daten, die über das Media Gateway geroutet werden, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung.• <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert.• <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt.• <i>Immer</i>: Die Optimierung für die Übertragung der Sprachdaten wird immer durchgeführt.
Maximale Upload-Geschwindigkeit	Geben Sie die maximal zur Verfügung stehende Bandbreite in Upload-Richtung in kbit/s für die gewählte Schnittstelle ein.

Kapitel 14 VPN

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

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

Zum Aufbau eines VPN-Tunnels stehen verschiedene Protokolle zur Verfügung, wie z. B. IPSec oder PPTP.

Die Authentifizierung der Verbindungspartner erfolgt über ein Passwort, mithilfe von Pre-shared Keys oder über Zertifikate.

Bei IPSec wird die Verschlüsselung der Daten z. B. mit Hilfe von AES oder 3DES erledigt, bei PPTP kann MPPE benutzt werden.

14.1 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 96) integriert werden. Die IPSec-Implementierung erreicht dieses Ziel zum einen durch die Benutzung des Authentication-Header-(AH)-Protokolls und des Encapsulated-Security-Payload-(ESP)-Protokolls. Zum anderen werden kryptografische Schlüsselverwaltungsmechanismen wie das Internet-Key-Exchange-(IKE)-Protokoll verwendet.

Zusätzlicher Filter des IPv4-Datenverkehrs

bintec elmeg Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IPSec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des IPv4-Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des IPv4-Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des IPv4-Datenverkehrs**, so wird es verworfen.

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



Hinweis

Der Parameter **Zusätzlicher Filter des IPv4-Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.



Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

14.1.1 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 461.

14.1.1.1 Neu

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

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

Felder im Menü Peer-Parameter

Feld	Beschreibung
Administrativer Status	<p>Wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Peer-Konfiguration versetzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. • <i>Inaktiv</i>: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.
Beschreibung	<p>Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
Peer-Adresse	<p>Wählen Sie die IP-Version aus. Sie können wählen, ob IPv4 oder IPv6 bevorzugt verwendet werden soll oder ob nur eine der beiden IP-Versionen erlaubt sein soll.</p>
	<p> Hinweis</p> <p>Diese Auswahl ist nur relevant, wenn ein Host-Name als Peer-Adresse eingegeben wird.</p>
	<p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IPv4 bevorzugt</i> • <i>IPv6 bevorzugt</i> • <i>Nur IPv4</i> • <i>Nur IPv6</i> <p>Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein.</p> <p>Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.</p>
Peer-ID	<p>Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein.</p> <p>Die Eingabe kann in bestimmten Konfigurationen entfallen.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p> <p>Mögliche ID-Typen:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i>: Beliebige Zeichenkette • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüssel-ID</i>: Beliebige Zeichenkette <p>Auf dem Peer-Gerät entspricht diese ID dem Parameter Lokaler ID-Wert.</p>
IKE (Internet Key Exchange)	<p>Wählen Sie die Version des Internet-Key-Exchange-Protokolls, die verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IKEv1</i> (Standardwert): Internet Key Exchange Protocol Version 1 • <i>IKEv2</i>: Internet Key Exchange Protocol Version 2
Authentifizierungsmethode	<p>Nur für IKE (Internet Key Exchange) = IKEv2</p> <p>Wählen Sie die Authentifizierungsmethode aus.</p>

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i> • <i>IPv4 und IPv6</i>

Felder im Menü IPv4-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i> (Standardwert) : Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. • <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 346 konfigurieren.</p>
IPv4-Adressvergabe	<p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Geben Sie eine statische IP-Adresse ein. • <i>Client im IKE-Konfigurationsmodus</i>: Wählen Sie diese Option, wenn Ihr Gateway als IPSec-Client vom Server eine IP-Adresse erhalten soll. • <i>Server im IKE-Konfigurationsmodus</i>: Wählen Sie diese Option, wenn Ihr Gateway als Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten IP-Zuordnungspool entnommen.
Konfigurationsmodus	<p>Nur bei IPv4-Adressvergabe = Server im IKE-Konfigurationsmodus oder Client im IKE-Konfigurationsmodus</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Pull</i> (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage. • <i>Push</i>: Das Gateway schlägt dem Client eine IP-Adresse vor und der Client muss diese akzeptieren oder zurückweisen. <p>Dieser Wert muss für beide Seiten des Tunnels identisch sein.</p>
IP-Zuordnungspool	<p>Nur bei IPv4-Adressvergabe = <i>Server im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie einen im Menü VPN->IPSec->IP Pools konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung <i>Noch nicht definiert</i>.</p>
Standardroute	<p>Nur für IPv4-Adressvergabe = <i>Statisch oder Client im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IPv4-Adressvergabe = <i>Statisch oder Server im IKE-Konfigurationsmodus</i></p> <p>Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.</p>
Metrik	<p>Nur für IPv4-Adressvergabe = <i>Statisch oder Client im IKE-Konfigurationsmodus</i> und Standardroute = <i>Aktiviert</i></p> <p>Wählen Sie die Priorität der Route aus.</p> <p>Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.</p> <p>Wertebereich von 0 bis 15. der Standardwert ist 1.</p>
Routeneinträge	<p>Nur für IPv4-Adressvergabe = <i>Statisch oder Client im IKE-Konfigurationsmodus</i></p>

Feld	Beschreibung
	<p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <i>Netzmaske</i>: Netzmaske zu <i>Entfernte IP-Adresse</i>. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 - 15). der Standardwert ist 1.

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

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

Felder im Menü **IPv6-Schnittstellenrouten**

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i>: Es werden nur IP-Pakete durchgelassen, wenn die Verbindung von "innen" initiiert wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü Firewall auf Seite 346 konfigurieren.</p>
Lokales IPv6-Netzwerk	<p>Wählen Sie ein Netzwerk aus. Sie können unter den Link-Präfixen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind.</p>

Feld	Beschreibung
	Geben Sie die Lokale IPv6-Adresse mit der entsprechenden Präfixlänge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.
Entferntes IPv6-Netzwerk	Fügen Sie mit Hinzufügen einen neuen Präfix hinzu. Geben Sie die Adresse der Tunnelgegenstelle ein. Standardmäßig ist eine Länge von 64 und eine Priorität von 1 vorgegeben. Je niedriger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.

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
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Protokoll	Wählen Sie ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
Quell-IP-Adresse/Netzmaske	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i> (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i> Geben Sie den Quell-Port der Datenpakete ein. Die Standardinstellung <i>-Alle-</i> (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und die zugehörige Netzmaske der Datenpakete ein.
Ziel-Port	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i>

Feld	Beschreibung
	Geben Sie den Ziel-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.

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

Felder im Menü **Erweiterte IPSec-Optionen**

Feld	Beschreibung
Phase-1-Profil	<p>Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in VPN->IPSec->Phase-1-Profile als Standard markiert ist • <i>Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 1 die Proposals 3DES/MD5, AES/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü . • <i><Profilname></i>: Verwendet ein Profil, das im Menü VPN->IPSec->Phase-1-Profile für Phase 1 konfiguriert wurde.
Phase-2-Profil	<p>Wählen Sie ein Profil für die Phase 2 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in VPN->IPSec->Phase-2-Profile als Standard markiert ist • <i>*Multi-Proposal</i>: Verwendet ein spezielles Profil, das für Phase 2 die Proposals 3DES/MD5, AES-128/MD5 und Blowfish/MD5 enthält ungeachtet der Proposalauswahl im Menü VPN->IPSec->Phase-2-Profile. • <i><Profilname></i>: Verwendet ein Profil, das im Menü VPN->IPSec->Phase-2-Profile für Phase 2 konfiguriert wurde.
XAUTH-Profil	<p>Wählen Sie ein in VPN->IPSec->XAUTH-Profile angelegtes Profil aus, wenn Sie zur Authentifizierung dieses IPSec-Peers XAuth verwenden möchten.</p> <p>Wenn XAuth zusammen mit dem IKE-Konfigurationsmodus ver-</p>

Feld	Beschreibung
	wendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.
Anzahl erlaubter Verbindungen	<p>Wählen Sie aus, wieviele Benutzer sich mit diesem Peer-Profil verbinden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ein Benutzer</i> (Standardwert): Es kann sich nur ein Peer mit den in diesem Profil definierten Daten verbinden. • <i>Mehrere Benutzer</i>: Es können sich mehrere Peers mit den in diesem Profil definierten Daten verbinden. Bei jeder Verbindungsanfrage mit den in diesem Profil definierten Daten, wird der Peer-Eintrag dupliziert. <p>Die Konfiguration des dynamischen Peers darf keine Peer ID und keine Peer-IP-Adresse enthalten. Die Clients, die sich mit dem Gateway verbinden, müssen jedoch über eine Lokale ID 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>
Startmodus	<p>Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auf Anforderung</i> (Standardwert): Der Peer wird durch einen Trigger in den aktiven Zustand versetzt. • <i>Immer aktiv</i>: Der Peer ist immer aktiv.
Backup Peer	<p>Nur für Peers mit IKEv2.</p> <p>Wenn der Peer im Startmodus <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</p>

Feld	Beschreibung
	<p>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 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.</p>
Verzögerung bis zur Rückkehr zum primären Peer	<p>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.</p>

Felder im Menü Erweiterte IP-Optionen

Feld	Beschreibung
Öffentliche Schnittstelle	<p>Legen Sie diejenige öffentliche (oder WAN-) Schnittstelle fest, über die dieser Peer sich mit seinem VPN-Partner verbinden soll. Wenn Sie <i>Vom Routing ausgewählt</i> auswählen, wird die Entscheidung, über welche Schnittstelle der Datenverkehr geleitet wird, gemäß der aktuellen Routingtabelle getroffen. Wenn Sie eine Schnittstelle auswählen, wird unter Beachtung der Einstellung unter Öffentlicher Schnittstellenmodus diese Schnittstelle verwendet.</p>
Öffentlicher Schnittstellenmodus	<p>Nur wenn unter Öffentliche Schnittstelle eine Schnittstelle ausgewählt ist.</p> <p>Legen Sie fest, wie strikt die Einstellung gehandhabt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erzwingen</i>: Unabhängig von den Prioritäten der aktuellen Routingtabelle wird nur die ausgewählte Schnittstelle verwendet. • <i>Bevorzugt</i>: Die Prioritäten der aktuellen Routingtabelle werden verwendet. Nur wenn mehrere gleichwertige Routen zur Verfügung stehen, wird die Route über die gewählte Schnittstelle verwendet.

Feld	Beschreibung
Öffentliche IPv4-Quelladresse	<p>Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die Öffentliche IPv4-Quelladresse aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Öffentliche IPv6-Quelladresse	<p>Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die Öffentliche IPv6-Quelladresse aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Überprüfung der IPv4-Rückroute	<p>Wählen Sie aus, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
MobiKE	<p>Nur für Peers mit IKEv2.</p> <p>MobiKE ermöglicht es, bei wechselnden öffentlichen IP-Adressen lediglich diese Adressen in den SAs zu aktualisieren, ohne die SAs selbst neu aushandeln zu müssen.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Beachten Sie, dass MobiKE einen aktuellen IPSec Client voraussetzt, z. B. den aktuellen Windows-7- oder Windows-8-Client oder die neuste Version des bintec elmeg IPSec Clients.</p>

Feld	Beschreibung
IPv4 Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer <i>aktiv</i> (aktiv) oder <i>Ruhend</i> (ruhend) ist. Bei <i>Ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <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.
CA-Zertifikate	<p>Nur verfügbar, wenn auf dem Gerät Zertifikate verwendet werden.</p> <p>Wenn Sie die Option Folgenden CA-Zertifikaten vertrauen 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 304 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der automatischen Auswahl durch das Gerät sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.



Hinweis

Damit Ihr Gerät die Informationen des gerufenen Peers über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Geräten analog vorgenommen werden.

Folgende Rollenverteilungen sind möglich:

- Eine Seite übernimmt die aktive, die andere die passive Rolle.
- Beide Seiten können beide Rollen (Beide) übernehmen.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

- (1) Peer A (der Auslöser des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.
- (2) Ihr Gerät erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden MIB-Eintrag.
- (3) Ihr Gerät setzt den initialen ISDN-Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.
- (4) Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten Calling Party Number (der ISDN-

Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.

- (5) Der IPSec-Daemon auf Ihrem Gerät von Peer B kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil des Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.
- (6) Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.



Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Die folgenden Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü IPv4 IPSec Callback

Feld	Beschreibung
Modus	<p>Wählen Sie den Callback-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): IPSec-Callback ist deaktiviert. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • <i>Passiv</i>: Das lokale Gerät reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. • <i>Aktiv</i>: Das lokale Gerät setzt einen ISDN-Ruf an das entfernte Gerät ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gerät nicht. • <i>Beide</i>: Ihr Gerät kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gerät absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem ein-

Feld	Beschreibung
	gehenden ISDN-Ruf) als auch veranlasst (durch einen ausgehenden ISDN-Ruf).
Ankommende Rufnummer	<p>Nur für Modus = <i>Passiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.</p>
Ausgehende Rufnummer	<p>Nur für Modus = <i>Aktiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.</p>
Eigene IP-Adresse per ISDN/GSM übertragen	<p>Wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Geräts über ISDN übertragen werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Übertragungsmodus	<p>Nur für Eigene IP-Adresse per ISDN/GSM übertragen = aktiviert</p> <p>Wählen Sie aus, in welchem Modus Ihr Gerät versuchen soll, seine IP-Adresse an den Peer zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung des besten Modus</i>: Ihr Gerät bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird. (Die Verwendung des B-Kanals verursacht Kosten.) • <i>Nur D-Kanalmodi automatisch erkennen</i>: Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. • <i>Spezifischen D-Kanalmodus verwenden</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. • <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. Ge-

Feld	Beschreibung
	<p>lingt das nicht, wird die IP-Adresse im B-Kanal übertragen. (Dies verursacht Kosten.)</p> <ul style="list-style-type: none"> • <i>Nur B-Kanalmodus verwenden</i>: Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.
Modus des D-Kanals	<p>Nur für Übertragungsmodus = <i>Spezifischen D-Kanalmodus verwenden</i> oder <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i></p> <p>Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LLC</i> (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen. • <i>SUBADDR</i>: Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen. • <i>LLC und SUBADDR</i>: Die IP-Adresse wird sowohl in den "LLC-" als auch in den "Subaddress Information Elements" übertragen.

14.1.2 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.

14.1.2.1 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
Beschreibung	Geben Sie eine Beschreibung ein, welche die Art der Regel ein-

Feld	Beschreibung
	deutig identifiziert.
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Nachrichten-Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Nachrichten-Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld. Mindestens ein Proposal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <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. • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. • <i>AES</i> (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. • <i>AES-128</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • <i>AES-192</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen

Feld	Beschreibung
	<p>Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet.</p> <ul style="list-style-type: none"> • <i>AES-256</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speichieranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i>: MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPsec verwendet. • <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. • <i>RipeMD 160</i>: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt. • <i>Tiger192</i>: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus. • <i>SHA2-256</i>: SHA 2 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus der als Nachfolger von SHA 1 standardisiert wurde. Er kann mit Hash-Längen von 256, 384 und 512 Bit verwendet werden. • <i>SHA2-384</i>: SHA-2 mit 384 Bit Hash-Länge. • <i>SHA2-512</i>: SHA-2 mit 512 Bit Hash-Länge. <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p> <p>Beachten Sie, dass die Qualität der Algorithmen relativen Gesichtspunkten unterliegt und sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern kann.</p>
DH-Gruppe	<p>Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec elmeg-Geräten unterstützt wird, steht für "modular exponentiation".</p> <p>Folgende Gruppen und zugehörige Bit-Werte der Exponentiati-</p>

Feld	Beschreibung
	<p>on stehen zur Verfügung:</p> <ul style="list-style-type: none"> • 1 (768 Bit) • 2 (1024 Bit) • 5 (1536 Bit) • 14 (2048 Bit) • 15 (3072 Bit) • 16 (4096 Bit) <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
Lebensdauer	<p>Legen Sie die Lebensdauer für Phase-1-Schlüssel fest.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <ul style="list-style-type: none"> • Eingabe in Sekunden: Geben Sie die Lebensdauer für Phase-1- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist <i>14400</i>, das bedeutet, dass die Schlüssel erneuert werden, wenn vier Stunden abgelaufen sind. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-1-Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist <i>0</i>; das bedeutet, dass die Anzahl der gesendeten kBytes keine Rolle spielt.
Authentifizierungsmethode	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Pre Shared Keys wählen. Diese werden bei der Peerkonfiguration im Menü VPN->IPSec->IPSec-Peers konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • <i>DSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert. • <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden

Feld	Beschreibung
	<p>unter Nutzung des RSA-Algorithmus authentifiziert.</p> <ul style="list-style-type: none"> • <i>RSA-Verschlüsselung</i>: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
Lokales Zertifikat	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Nur für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>
Modus	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie den Phase-1-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aggressiv</i> (Standardwert): Der Aggressive Modus ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden. Er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals. • <i>Main Modus (ID Protect)</i>: Dieser Modus (auch als Main Mode bezeichnet) erfordert sechs Meldungen für eine Diffie-Hellman-Schlüsselberechnung und damit für die Einrichtung eines sicheren Kanals, über den die IPSec-SAs ausgehandelt werden. Er setzt voraus, dass beide Peers statische IP-Adressen haben, falls für die Authentifizierung Preshared Keys genutzt werden. <p>Wählen Sie weiterhin aus, ob der gewählte Modus ausschließlich verwendet werden darf (Strikt) oder der Peer auch einen anderen Modus vorschlagen kann.</p>
Lokaler ID-Typ	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie den Typ der lokalen ID aus.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüsse-ID</i>
Lokaler ID-Wert	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i> wird die Option Subjektnamen aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektnamen aus Zertifikat verwenden 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
Erreichbarkeitsprüfung	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Methode aus, mit der die Funktionalität der IP-Sec-Verbindung überprüft werden soll.</p> <p>Neben dem Standardverfahren Dead Peer Detection (DPD) ist</p>

Feld	Beschreibung
	<p>auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Automatische Erkennung</i> (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt.• <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option.• <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen.• <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen.• <i>Heartbeats (Senden & Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.• <i>Dead Peer Detection</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Erreichbarkeit des Peers nur überprüft, wenn tatsächlich Daten an ihn gesendet werden sollen.• <i>Dead Peer Detection (Idle)</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vorgenommen.

Feld	Beschreibung
	<div data-bbox="539 211 1315 500" style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px;">  <p>Hinweis</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> </div> <p>Nur für Phase-1-Parameter (IKEv2)</p> <p>Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Blockzeit	<p>Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche.</p> <p>Zur Verfügung stehen Werte von -1 bis 86400 (Sekunden), der Wert -1 bedeutet die Übernahme des Wertes im Standardprofil, der Wert 0, dass der Peer in keinem Fall blockiert wird.</p> <p>Der Standardwert ist 30. Wenn ein Peer im Modus "Immer aktiv" konfiguriert ist, besteht eine implizite Minimalblockzeit von 15 Sekunden, die unabhängig vom eingegebenen Wert angewendet wird.</p>
NAT-Traversal	<p>NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.</p> <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>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert): NAT-Traversal ist aktiv. • <i>Deaktiviert</i>: NAT-Traversal ist deaktiviert. • <i>Erzwingen</i>: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. <p>Nur für <i>IKEv2-Profile</i></p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CA-Zertifikate	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Nur für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Wenn Sie die Option Folgenden CA-Zertifikaten vertrauen aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen.</p> <p>Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.</p>

14.1.3 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.

14.1.3.1 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
Beschreibung	Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.

Feld	Beschreibung
	Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <i>3DES</i>: 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. • <code>-- ALLE --</code>: Alle Optionen können verwendet werden. • <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. • <i>AES-128</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • <i>AES-192</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • <i>AES-256</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schnell-

Feld	Beschreibung
	<p>ler Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden.</p> <ul style="list-style-type: none"> • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i>: MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • -- <i>ALLE</i> --: Alle Optionen können verwendet werden. • <i>SHA1</i> (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. • <i>SHA2-256</i>: SHA 2 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus der als Nachfolger von SHA 1 standardisiert wurde. Er kann mit Hash-Längen von 256, 384 und 512 Bit verwendet werden. • <i>SHA2-384</i>: SHA-2 mit 384 Bit Hash-Länge. • <i>SHA2-512</i>: SHA-2 mit 512 Bit Hash-Länge. <p>Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.</p> <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
<p>PFS-Gruppe verwenden</p>	<p>Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (<i>Aktiviert</i>), sind die Optionen die gleichen, wie bei der Konfiguration von DH-Gruppe im Menü VPN->IPSec->Phase-1-Profil . 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 Exponentiati-</p>

Feld	Beschreibung
	<p>on stehen zur Verfügung:</p> <ul style="list-style-type: none"> • 1 (768 Bit) • 2 (1024 Bit) • 5 (1536 Bit) • 14 (2048 Bit) • 15 (3072 Bit) • 16 (4096 Bit) <p>Je nach Hardware Ihres Geräts stehen ggf. nicht alle Optionen zur Verfügung.</p>
Lebensdauer	<p>Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen.</p> <p>Die neuen SAs werden bereits kurz vor dem Ablauf der aktuellen SAs ausgehandelt. Der Standardwert beträgt gemäß RFC 2407 acht Stunden, das bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <ul style="list-style-type: none"> • Eingabe in Sekunden: Geben Sie die Lebensdauer für Phase-2- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist 7200. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-2- Schlüssel als Menge der verarbeiteten Daten in kBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist 0. <p>Schlüssel erneut erstellen nach: Legen Sie fest, bei welchem Prozentsatz des Ablaufes der Lebensdauer die Schlüssel der Phase 2 neu erstellt werden.</p> <p>Die eingegebene Prozentzahl wird sowohl auf die Lebensdauer in Sekunden als auch auf die Lebensdauer in kBytes angewendet.</p> <p>Der Standardwert ist 80 %.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
IP-Komprimierung	<p>Wählen Sie aus, ob eine Kompression vor der Datenverschlüsselung eingeschaltet wird. Das kann bei gut komprimierbaren Daten zu einer höheren Performance und geringerem zu übertragenden Datenvolumen führen. Bei schnellen Leitungen oder nicht komprimierbaren Daten wird von der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erreichbarkeitsprüfung	<p>Wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden.</p> <p>Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, ist ein bintec elmeg IPSec-Heartbeat implementiert worden. Dieser sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Automatische Erkennung, ob die Gegenstelle ein bintec elmeg-Gerät ist. Wenn ja, wird <i>Heartbeats (Senden &Erwarten)</i> (bei Gegenstelle mit bintec elmeg) oder <i>Inaktiv</i> (bei Gegenstelle ohne bintec elmeg) gesetzt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden &Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.

Feld	Beschreibung
	<div data-bbox="539 211 1315 599" style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px;">  <p>Hinweis</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>
PMTU propagieren	<p>Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

14.1.4 XAUTH-Profile

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

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

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

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

Im Server-Modus können sich mehrere Benutzer über XAuth authentifizieren, z. B. Nutzer von Apple iPhones. 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.

14.1.4.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für dieses XAuth-Profil ein. Mit den Einstellungen Rolle = <i>Server</i> und Modus = <i>Lokal</i> oder Rolle = <i>Client</i> (siehe unten) können Sie bis zu 10 XAuth-Profilen anlegen.
Rolle	Wählen Sie die Rolle des Gateways bei der XAuth-Authentifizierung aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Server</i> (Standardwert): Das Gateway fordert einen Berechtigungsnachweis an. • <i>Client</i>: Das Gateway weist seine Berechtigung nach.
Modus	Nur für Rolle = <i>Server</i>

Feld	Beschreibung
	<p>Wählen Sie aus, wie die Authentifizierung durchgeführt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>RADIUS</i> (Standardwert): Die Authentifizierung wird über einen RADIUS-Server durchgeführt. Dieser wird im Menü Systemverwaltung -> Remote Authentifizierung -> RADIUS konfiguriert und im Feld RADIUS-Server Gruppen-ID ausgewählt. • <i>Lokal</i>: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.
Name	<p>Nur für Rolle = Client</p> <p>Geben Sie den Authentifizierungsnamen des Clients ein.</p>
Passwort	<p>Nur für Rolle = Client</p> <p>Geben Sie das Authentifizierungspasswort ein.</p>
RADIUS-Server Gruppen-ID	<p>Nur für Rolle = Server</p> <p>Wählen Sie die gewünschte in Systemverwaltung -> Remote Authentifizierung -> RADIUS konfigurierte RADIUS-Gruppe aus.</p>
Benutzer	<p>Nur für Rolle = Server und Modus = Lokal</p> <p>Ist Ihr Gateway als XAuth-Server konfiguriert, können die Clients über eine lokal konfigurierte Benutzerliste authentifiziert werden. Definieren Sie hier die Mitglieder der Benutzergruppe dieses XAUTH-Profiles, indem Sie den Authentifizierungsnamen des Clients (Name) und das Authentifizierungspasswort (Passwort) eingeben. Fügen Sie weitere Mitglieder mit Hinzufügen hinzu.</p> <p>Die Zahl der Benutzer pro XAuth-Profil ist unbeschränkt.</p>

14.1.5 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.

14.1.5.1 Bearbeiten oder Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

14.1.6 Optionen

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

Felder im Menü Globale Optionen

Feld	Beschreibung
IPSec aktivieren	<p>Wählen Sie, ob Sie IPSec aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.</p>
Vollständige IPSec-Konfiguration löschen	<p>Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts.</p> <p>Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, können Sie mit einer kom-</p>

Feld	Beschreibung
	<p>plett neuen IPSec-Konfiguration beginnen.</p> <p>Das Löschen der Konfiguration ist nur möglich mit IPSec aktivieren = nicht aktiviert.</p>
IPSec-Debug-Level	<p>Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Information</i> • <i>Debug</i> (Standardwert, niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level "Debug" sämtliche erzeugten Meldungen aufgezeichnet werden.</p>

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen bintec elmeg-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	<p>Wählen Sie aus, ob IPSec über TCP verwendet werden soll.</p> <p>IPSec über TCP basiert auf der NCP-Path-Finder-Technologie. Diese Technologie sorgt dafür, dass der Datenverkehr (IKE, ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session</p>

Feld	Beschreibung
	<p>eingebettet wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Initial Contact Message senden	<p>Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von <i>Aktiv</i> zu <i>Inaktiv</i>, <i>Ruhend</i> oder <i>Blockiert</i> geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zero Cookies verwenden	<p>Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen.</p> <p>Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall <i>Aktiviert</i>.</p>
Größe der Zero Cookies	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten und auf Null gesetzten SPI in Bytes ein.</p> <p>Der Standardwert ist 32.</p>
Dynamische RADIUS-Authentifizierung	<p>Wählen Sie aus, ob die RADIUS-Authentifizierung über IPsec aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	<p>Wählen Sie aus, ob Zertifikatsanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungs-Payloads senden	<p>Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatsanforderungen gesendet werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Zertifikatsketten senden	<p>Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.</p>
CRLs senden	<p>Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Key Hash Payloads senden	<p>Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen.</p> <p>Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung. Aktivieren Sie diese Funktion mit <i>Aktiviert</i>, um dieses Verhalten zu unterdrücken.</p>

14.2 L2TP

Das Layer-2-Tunnelprotokoll (L2TP) ermöglicht das Tunneling von PPP-Verbindungen über eine UDP-Verbindung.

Ihr bintec elmeg-Gerät unterstützt die folgenden zwei Modi:

- L2TP-LNS-Modus (L2TP Network Server): nur für eingehende Verbindungen
- L2TP-LAC-Modus (L2TP Access Concentrator): nur für ausgehende Verbindungen.

Folgendes ist bei der Konfiguration von Server und Client zu beachten: Auf beiden Seiten (LAC und LNS) muss jeweils ein L2TP-Tunnelprofil angelegt werden. Auf der Auslöserseite (LAC) wird das entsprechende L2TP-Tunnelprofil für den Verbindungsaufbau verwendet. Auf der Responderseite (LNS) wird das L2TP-Tunnelprofil für die Verbindungsannahme benötigt.

14.2.1 Tunnelprofile

Im Menü **VPN->L2TP->Tunnelprofile** wird eine Liste aller konfigurierten Tunnelprofile angezeigt.

14.2.1.1 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
Beschreibung	Geben Sie eine Beschreibung für das aktuelle Profil ein. Ihr Gerät benennt die Profile automatisch mit <i>L2TP</i> und nummeriert diese, der Wert kann jedoch geändert werden.
Lokaler Hostname	Geben Sie den Hostnamen für LNS bzw. LAC ein. <ul style="list-style-type: none"> • <i>LAC</i>: Der lokale Hostname wird in abgehenden Tunnelaufbaumeldungen zur Identifizierung dieses Geräts aufgenommen und wird dem entfernten Hostnamen eines der am LNS konfigurierten Tunnelprofile zugeordnet. Bei diesen Tunnelaufbaumeldungen handelt es sich um die vom LAC ausgesandten SCCRQs (Start Control Connection Request) und die vom LNS ausgesandten SCCRPs (Start Control Connection Rep-

Feld	Beschreibung
	<p>ly).</p> <ul style="list-style-type: none"> • <i>LNS</i>: Entspricht dem Wert für Entfernter Hostname der eingehenden Tunnelaufbaumeldung vom LAC.
Entfernter Hostname	<p>Geben Sie den Hostnamen des LNS bzw. LAC ein:</p> <ul style="list-style-type: none"> • <i>LAC</i>: Definiert den Wert für Lokaler Hostname des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). Ein im LAC konfigurierter Lokaler Hostname muss zu Entfernter Hostnamen passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. • <i>LNS</i>: Definiert den Lokaler Hostnamen des LAC. Falls das Feld Entfernter Hostname auf dem LNS leer bleibt, wird das dazugehörige Profil als Standardeintrag qualifiziert, der für alle ankommenden Rufe benutzt wird, für die kein Profil mit passendem entfernten Hostnamen gefunden werden kann.
Passwort	<p>Geben Sie das Passwort ein, welches für die Tunnel-Authentifizierung benutzt wird. Die Authentifizierung zwischen LAC und LNS erfolgt in beiden Richtungen, d. h. der LNS prüft den Lokaler Hostnamen und das Passwort, die in der SCCRQ des LAC enthalten sind und vergleicht sie mit denen, die im relevanten Profil angegeben sind. Der LAC macht das Gleiche mit den jeweiligen Feldern der SCCRP des LNS.</p> <p>Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.</p>

Felder im Menü Parameter des LAC-Modus

Feld	Beschreibung
Entfernte IP-Adresse	<p>Geben Sie die feste IP-Adresse des LNS ein, die als Zieladresse für Verbindungen genutzt wird, die auf diesem Profil aufbauen.</p> <p>Das Ziel muss ein Gerät sein, welches sich wie ein LNS verhalten kann.</p>
UDP-Quellport	<p>Geben Sie an, wie die Portnummer ermittelt werden soll, die als Quellport für alle abgehenden L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.</p>

Feld	Beschreibung
	<p>Standardmäßig ist die Option Fest eingestellt 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>
UDP-Zielport	<p>Geben Sie die Zielportnummer ein, die für alle Rufe genutzt wird, die auf diesem Profil aufbauen. Der entfernte LNS, der den Ruf empfängt, muss diesen Port auf L2TP-Verbindungen überwachen.</p> <p>Mögliche Werte sind 0 bis 65535.</p> <p>Der Standardwert ist 1701 (RFC 2661).</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Lokale IP-Adresse	<p>Geben Sie die IP-Adresse ein, die als Quelladresse für alle L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.</p> <p>Falls dieses Feld frei gelassen wird, nutzt Ihr Gerät die IP-Adresse der Schnittstelle, über das der L2TP-Tunnel die entfernte IP-Adresse erreicht.</p>
Hello-Intervall	<p>Geben Sie den Zeitabstand (in Sekunden) zwischen dem Senden von zwei L2TP-HELLO-Meldungen ein. Diese Meldungen dienen dazu, den Tunnel offen zu halten.</p> <p>Verfügbare Werte sind 0 bis 255, der Standardwert ist 30. Der Wert 0 bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.</p>
Minimale Zeit zwischen Versuchen	<p>Geben Sie die Mindestzeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat.</p>

Feld	Beschreibung
	Die Wartezeit wird dynamisch verlängert, bis sie die Maximale Zeit zwischen Versuchen erreicht hat. Verfügbare Werte sind 1 bis 255, der Standardwert ist 1.
Maximale Zeit zwischen Versuchen	Geben Sie die maximale Zeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat. Verfügbare Werte sind 8 bis 255, der Standardwert ist 16.
Maximale Anzahl Wiederholungen	Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden. Verfügbare Werte sind 8 bis 255, der Standardwert ist 5.
Sequenznummern der Datenpakete	Wählen Sie aus, ob Ihr Gerät für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folge-nummern benutzen soll oder nicht. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

14.2.2 Benutzer

Im Menü **VPN->L2TP->Benutzer** wird eine Liste aller konfigurierten L2TP-Partner angezeigt.

14.2.2.1 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
Beschreibung	Geben Sie einen beliebigen Namen ein, um den L2TP-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.

Feld	Beschreibung
	Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.
Verbindungstyp	<p>Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerksservers (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LNS</i> (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • <i>LAC</i>: Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.
Tunnelprofil	<p>Nur für Verbindungstyp = <i>LAC</i></p> <p>Wählen Sie ein im Menü Tunnelprofil erstelltes Profil für die Verbindung zu diesem L2TP-Partner aus.</p>
Benutzername	Geben Sie die Kennung Ihres Geräts ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutzdatenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Zur Verfügung stehen Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Short Hold. Der Standardwert ist 300.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein. • <i>IP-Adresse bereitstellen</i>: Nur für Verbindungstyp = <i>LNS</i>. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Nur für Verbindungstyp = <i>LAC</i>. Ihr Gerät erhält dynamisch eine IP-Adresse.
IP-Zuordnungspool (IPCP)	<p>Nur für IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>Wählen Sie einen im Menü WAN->Internet + Einwählen->IP Pools konfigurierten IP Pool aus.</p>
Standardroute	<p>Nur für IP-Adressmodus = <i>IP-Adresse abrufen</i> und <i>Statisch</i></p> <p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv .</p>
NAT-Eintrag erstellen	<p>Nur für IP-Adressmodus = <i>IP-Adresse abrufen</i> und <i>Statisch</i></p> <p>Wählen Sie aus, ob Network Address Translation (NAT) für diese Verbindung aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die WAN-IP-Adresse Ihres Geräts ein.</p>
Routeneinträge	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie Entfernte IP-Adresse und Netzmaske des LANs</p>

Feld	Beschreibung
	des L2TP-Partners und die dazugehörige Metrik ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Der Standardwert ist <i>300</i>.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP/CHAP/MS-CHAP</i> (Standardwert): Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>PAP</i>: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	<p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i>: Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i> (Standardwert): Die MPP-Verschlüsselung V2 mit 128 Bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing-Informationen berücksichtigt und über aktive Schnittstellen propagiert. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.

Feld	Beschreibung
Proxy-ARP-Modus	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>Aktiv</i> (aktiv) oder <i>Ruhend</i> (ruhend) ist. Bei <i>Ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>Aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server und WINS-Server Primär und Sekundär vom L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

14.2.3 Optionen

Das Menü **VPN->L2TP->Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Optionen

Feld	Beschreibung
UDP-Zielport	<p>Geben Sie den Port ein, der vom LNS auf ankommende L2TP-Tunnelverbindungen überwacht werden soll.</p> <p>Verfügbare Werte sind alle ganzen Zahlen von 1 bis 65535, der Standardwert ist 1701, wie es in RFC 2661 vorgegeben ist.</p>
UDP-Quellportauswahl	Wählen Sie aus, ob der LNS nur den überwachten Port (UDP-

Feld	Beschreibung
	<p>Zielport) als lokalen Quellport für die L2TP-Verbindung nutzen soll.</p> <p>Mit <i>Fest eingestellt</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

14.3 PPTP

Zur Absicherung des Datenverkehrs über eine vorhandene IP-Verbindung kann mittels Point-to-Point-Tunneling-Protokoll (=PPTP) ein verschlüsselter PPTP-Tunnel aufgebaut werden.

Zunächst wird an beiden Standorten eine Verbindung zu einem ISP (=Internet Service Provider) aufgebaut. Wenn diese Verbindungen stehen, wird über das Internet ein Tunnel zum PPTP Partner, hier dann mit PPTP, aufgebaut.

Für diesen Vorgang baut das PPTP-Subsystem eine Kontrollverbindung zwischen den Tunnelendpunkten auf. Diese übermittelt Steuerungsdaten, welche die Verbindung zwischen den zwei PPTP-Tunnelendpunkten aufbauen, aufrechterhalten und beenden. Sobald diese Kontrollverbindung aufgebaut ist, überträgt das PPTP die in GRE-Pakete (GRE = Generic Routing Encapsulation) eingepackten Nutzdaten.

14.3.1 PPTP-Tunnel

Im Menü **PPTP-Tunnel** wird eine Liste aller PPTP-Tunnels angezeigt.

14.3.1.1 Neu

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

Das Menü **VPN->PPTP->PPTP-Tunnel->Neu** besteht aus folgenden Feldern:

Felder im Menü PPTP Partner Parameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen Namen ein, um den Tunnel eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.</p>
PPTP-Modus	Geben Sie die Rollenverteilung der PPTP-Schnittstelle an.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PNS</i> (Standardwert): Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Servers zu. • <i>Windows-Client-Modus</i>: Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Clients zu.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Timeout.</p> <p>Der Standardwert ist 300.</p> <p>Beispiel: 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>
Entfernte PPTP-IP-Adresse	<p>Nur für PPTP-Modus = <i>PNS</i></p> <p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p>
Entfernte PPTP-IP-Adresse / Hostname	<p>Nur für PPTP-Modus = <i>Windows-Client-Modus</i></p> <p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein. • <i>IP-Adresse bereitstellen</i>: Nur für PPTP-Modus = PNS. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Nur für PPTP-Modus = Windows-Client-Modus. Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	<p>Nur bei IP-Adressmodus = Statisch</p> <p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
NAT-Eintrag erstellen	<p>Nur bei IP-Adressmodus = Statisch</p> <p>Wenn eine PPTP-Verbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = Statisch</p> <p>Weisen Sie der PPTP-Schnittstelle die IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.</p>
Routeneinträge	<p>Nur für IP-Adressmodus = Statisch</p> <p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 - 15). Der Standardwert ist 1.
IP-Zuordnungspool (IPCP)	<p>Nur bei PPTP-Modus = PNS, IP-Adressmodus = IP-Adresse bereitstellen</p>

Feld	Beschreibung
	Wählen Sie hier einen im Menü VPN->PPTP->IP Pools konfigurierten IP-Pool aus.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Der Standardwert ist <i>300</i>.</p>
Nutzungsart	<p>Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Kein spezieller Typ ist ausgewählt. • <i>Mehrfacheinwahl (Nur Einwahl)</i>: Die Schnittstelle wird als Multi-User-Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen PPTP-Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i>: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP-Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.)

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>MS-CHAPv2</i> (Standardwert): Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	<p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i>: Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i> (Standardwert): Die MPP-Verschlüsselung V2 mit 128 bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 bit wird kompatibel zu Microsoft und Cisco angewendet.
Komprimierung	<p>Wählen Sie ggf. die Art der Komprimierung aus, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird keine Verschlüsselung angewendet. • <i>STAC</i> • <i>MS-STAC</i> • <i>MPPC</i>: Microsoft Point-to-Point Compression
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen PPTP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen PPTP-Partner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-Partner <i>Aktiv</i> (aktiv) oder <i>Ruhend</i> (ruhend) ist. Bei <i>Ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-Partner <i>Aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum PPTP-Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom PPTP-Partner erhalten soll oder diese zum PPTP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

Felder im Menü PPTP-Callback

Feld	Beschreibung
Callback	<p>Ermöglicht den Aufbau eines PPTP-Tunnels über das Internet mit einem PPTP-Partner, selbst wenn dieser momentan nicht online ist. In der Regel wird mittels ISDN-Ruf der PPTP-Partner aufgefordert, online zu gehen und eine PPTP-Verbindung aufzubauen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Beachten Sie, dass Sie die entsprechende Option auf den Gateways beider Partner aktivieren müssen. Für diese Funktion wird in der Regel ein ISDN-Anschluss benötigt. Ohne ISDN ist Callback nur in Spezialanwendungen zu aktivieren.</p>
Eingehende ISDN-Nummer	<p>Nur wenn Callback aktiviert ist.</p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number).</p>
Ausgehende ISDN-Nummer	<p>Nur wenn Callback aktiviert ist.</p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number).</p>

Felder im Menü Auswahl des Wählports (nur wenn Callback = aktiviert)

Feld	Beschreibung
Ausgewählte Ports	<p>Geben Sie die ISDN-Ports an, über die der Callback ausgeführt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle Ports</i>: Der Callback wird über einen der verfügbaren ISDN-Ports ausgeführt. • <i>Port angeben</i>: In Spezifische Ports können Sie die gewünschten ISDN-Ports auswählen.
Spezifische Ports	Nur für Ausgewählte Ports = <i>Port angeben</i> können Sie mit Hinzufügen weitere Ports auswählen.

14.3.2 Optionen

In diesem Menü können Sie allgemeine Einstellungen des globalen PPTP Profils vornehmen.

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

Felder im Menü Globale Optionen

Feld	Beschreibung
GRE-Win- dow-Anpassung	<p>Wählen Sie, ob Sie GRE Window Adaption aktivieren wollen.</p> <p>Diese Anpassung ist erst notwendig, wenn Sie unter Microsoft Windows XP das Service Pack 1 installiert haben. Da Microsoft mit dem SP1 den Bestätigungsalgorithmus innerhalb des GRE-Protokolls geändert hat, muss bei bintec elmeg-Geräten die automatische Window-Anpassung für GRE abgeschaltet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
GRE-Window-Größe	<p>Geben Sie die maximale Anzahl an GRE-Paketen ein, die ohne Bestätigung geschickt werden kann.</p> <p>Windows verwendet seit der Version XP ein höheres initiales Empfangs-Window im GRE, weshalb die maximale Sendewindow-Größe über den Wert GRE-Window-Größe angepasst werden sollte. Mögliche Werte sind 0 bis 256.</p> <p>Der Standardwert ist 0.</p>
Max. eingehende Kontrollverbindungen über entfernte IP-Adresse	Geben Sie die maximale Anzahl der Kontrollverbindungen ein.

14.3.3 IP Pools

Im Menü **IP Pools** wird eine Liste aller IP Pools für PPTP-Verbindungen angezeigt.

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

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

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere IP Pools einzurichten.

14.3.3.1 Bearbeiten oder Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

14.4 GRE

Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, das dazu dient, andere Protokolle einzukapseln und so in Form von IP-Tunneln zu den spezifizierten Empfänger zu transportieren.

Die Spezifikation des GRE-Protokolls liegt in zwei Versionen vor:

- GRE V.1 zur Verwendung in PPTP-Verbindungen (RFC 2637, Konfiguration im Menü **PPTP**)

- GRE V.0 (RFC 2784) zur allgemeinen Encapsulierung mittels GRE

Im diesem Menü können Sie ein virtuelles Interface zur Nutzung von GRE V.0 konfigurieren. Der Datenverkehr, der über dieses Interface geroutet wird, wird dann mittels GRE encapsuliert und an den spezifizierten Empfänger gesendet.

14.4.1 GRE-Tunnel

Im Menü **VPN->GRE->GRE-Tunnel** wird eine Liste aller konfigurierten GRE-Tunnel angezeigt.

14.4.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere GRE-Tunnel einzurichten.

Das Menü **VPN->GRE->GRE-Tunnel->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein. Wird keine IP-Adresse (dies entspricht der IP-Adresse 0.0.0.0) angegeben, wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse der GRE-Pakete zum GRE-Partner ein.
Standardroute	Wenn Sie die Standardroute aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Geben Sie hier die (LAN-seitige) IP-Adresse ein, die als Quelladresse Ihres Gerätes für eigene Pakete durch den GRE-Tunnel verwendet werden soll.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit Hinzufügen neue Einträge hinzu.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standard-Netzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf.</p> <p>Mögliche Werte sind 1 bis 8192.</p> <p>Der Standardwert ist 1500.</p>
Schlüssel verwenden	<p>Aktivieren Sie die Eingabe einer Kennung für die GRE-Verbindung, welche die Unterscheidung mehrerer parallel laufender GRE-Verbindungen zwischen zwei GRE-Partnern ermöglicht (siehe RFC 1701).</p> <p>Mit <i>Aktiviert</i> wird die Kennung aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Schlüsselwert	<p>Nur wenn Schlüssel verwenden aktiviert ist.</p> <p>Geben Sie die GRE-Verbindungskennung ein.</p> <p>Mögliche Werte sind 0 bis 2147483647.</p> <p>Der Standardwert ist 0.</p>

Kapitel 15 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 361.

15.1 Richtlinien

15.1.1 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.

15.1.1.1 Neu



Hinweis

Informationen zur Auswahl der Vertrauenswürdige Schnittstellen finden Sie hier: [IPv4-Filterregeln](#) auf Seite 348.

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	<p>Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.</p>
Ziel	<p>Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <i>dns</i> • <i>http</i> • <i>nntp</i> • <i>Internet</i> • <i>Netmeeting</i> <p>Weitere Dienste werden in Firewall->Dienste->Diensteliste angelegt.</p> <p>Außerdem stehen die in Firewall->Dienste->Gruppen konfigurierten Dienstegruppen zur Auswahl.</p>
Aktion	<p>Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll.</p> <p>Möglichen Werte:</p> <ul style="list-style-type: none"> • <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • <i>Verweigern</i>: Die Pakete werden abgewiesen. • <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

15.1.2 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.

15.1.2.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Verweigern</i>: Die Pakete werden abgewiesen. • <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.

15.1.3 Optionen

In diesem Menü können Sie die IPv4-Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wie vielen Sekunden Inaktivität eine Sitzung beendet werden soll.



Hinweis

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

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

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Status der IPv4-Firewall	<p>Aktivieren oder deaktivieren Sie die IPv4-Firewall-Funktion.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierte Aktionen	<p>Wählen Sie den Firewall-Syslog-Level aus.</p> <p>Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Alle Firewall-Aktivitäten werden angezeigt. • <i>Verweigern</i>: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion". • <i>Annehmen</i>: Nur Accept-Ereignisse werden angezeigt. • <i>Keiner</i>: Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige IPv4-Filterung	<p>Bei TCP-Sessions überwacht die SIF im ersten Schritt, ob eine</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 Vollständige IPv4-Filterung <i>Aktivieren</i> vorgesehen.</p> <p>Wenn bei zweiseitiger Kommunikation eine Richtung des Datenverkehrs über den Router läuft, die Datenpakete der entgegengesetzten Richtung aber einen anderen Weg nehmen, 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 Vollständige IPv4-Filterung deaktivieren. Etwaige existierende SIF-Filterregeln dazu werden ignoriert.</p>
STUN Handler	<p>Wenn Sie Geräten (vor allem SIP Clients) in Ihrem Netzwerk erlauben wollen, über STUN den Modus der Network Address Translation sowie die öffentliche IP-Adresse zu ermitteln, so aktivieren Sie diese Option. Die Firewall erstellt dann temporäre Regeln, die den RTP-Datenverkehr für SIP-Gespräche ermöglichen.</p>
Port-STUN-Server	<p>Nur für STUN Handler = Aktiviert</p> <p>Geben Sie Nummer des Ports ein, der für die Verbindung zum STUN-Server benutzt werden soll.</p> <p>Standardmäßig ist der Wert <i>3478</i> vorgegeben. Möglich ist eine 5-stellige Ziffernfolge.</p>

Felder im Menü Sitzungstimer

Feld	Beschreibung
UDP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine UDP - Session als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i>.</p> <p>Der Standardwert ist <i>180</i>.</p>
TCP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine TCP - Session als abgelaufen betrachtet werden soll (in Sekunden).</p>

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

Felder im Menü Firewall auf Werkseinstellungen zurücksetzen

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

15.2 Schnittstellen

15.2.1 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.

15.2.1.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv4-Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

15.2.2 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.

15.2.2.1 Neu

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

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

Felder im Menü Basisparameter

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

15.3 Adressen

15.3.1 Adressliste

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

15.3.1.1 Neu

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

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

Felder im Menü Basisparameter

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

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

15.3.2 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.

15.3.2.1 Neu

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

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

Felder im Menü Basisparameter

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

15.4 Dienste

15.4.1 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.

15.4.1.1 Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protokoll	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
Zielportbereich	Nur für Protokoll = <i>TCP, UDP/TCP</i> oder <i>UDP</i> Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll. Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen. Mögliche Werte sind 1 bis 65535.
Quellportbereich	Nur für Protokoll = <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 <i>1</i> bis <i>65535</i>.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Das Feld Typ gibt die Klasse der ICMP-Nachrichten an, das Feld Code spezifiziert die Art der Nachricht genauer.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Echo Reply</i> • <i>Destination Unreachable</i> • <i>Source Quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time Exceeded</i> • <i>Parameter Problem</i> • <i>Timestamp</i> • <i>Timestamp Reply</i> • <i>Information Request</i> • <i>Information Reply</i> • <i>Address Mask Request</i> • <i>Address Mask Reply</i>
Code	<p>Nur für Typ = <i>Destination Unreachable</i> stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Net Unreachable</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Host Unreachable</i> • <i>Protocol Unreachable</i> • <i>Port Unreachable</i> • <i>Fragmentation Needed</i> • <i>Communication with Destination Network is Administratively Prohibited</i> • <i>Communication with Destination Host is Administratively Prohibited</i>

15.4.2 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.

15.4.2.1 Neu

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

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

Felder im Menü Basisparameter

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

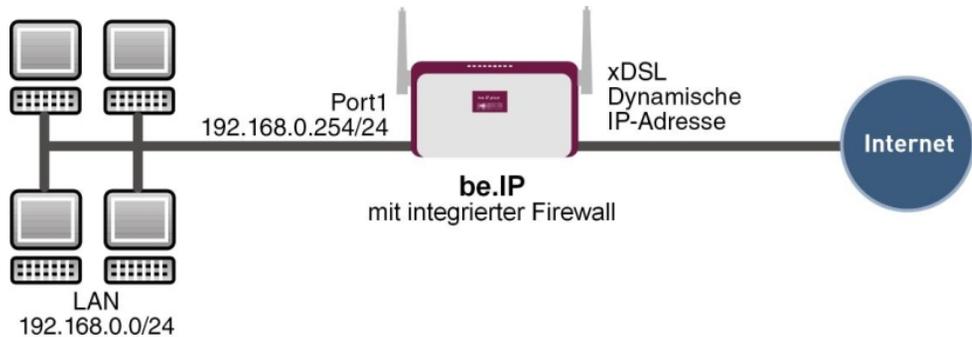
15.5 Konfiguration

15.5.1 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

Kapitel 16 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Automatische Erkennung und Konfiguration von bintec elmeg-Geräten
- Bereitstellung öffentlicher Internetzugänge (Hotspot).
- Ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten (Wake-On-LAN)

16.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste->DNS->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 entsprechende Schnittstellenstatus "up" ist, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (4) Ansonsten werden, falls eine Internet- oder Einwählverbindung als Standard-Schnittstelle ausgewählt ist, die dazugehörigen DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (5) Ansonsten wird, falls im Menü **WAN->Internet + Einwählen** ein Eintrag angelegt wurde und das Überschreiben der Adressen der globalen Name-Server zulässig ist (**Schnittstellenmodus = Dynamisch**), eine Verbindung zur ersten Internet- bzw. Einwählverbindung ggf. kostenpflichtig aufgebaut, die so konfiguriert ist, dass DNS-Server-Adressen von DNS-Servern angefordert werden können (**DNS-Aushandlung = Aktiviert**) - soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung stehen diese Name-Server somit für weitere Anfragen zur Verfügung.
- (6) Ansonsten wird die initiale Anfrage mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit `non-existent domain` antwortet, wird die initiale Anfrage sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache Ihres Geräts aufgenommen.

16.1.1 Globale Einstellungen

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
WINS-Server Primär Sekundär	Geben Sie die IP-Adresse des ersten und, falls erforderlich, des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	<p>Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Negativer Cache	<p>Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Cache-Größe	<p>Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein.</p> <p>Wird dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird Cache-Größe vom Benutzer heruntersgesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. Cache-Größe</p>

Feld	Beschreibung
	<p>kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden.</p> <p>Mögliche Werte: 0.. 1000.</p> <p>Der Standardwert ist 100.</p>
Maximale TTL für positive Cacheeinträge	<p>Geben Sie den Wert ein, auf den die TTL für einen positiven dynamischen DNS-Eintrag im Cache gesetzt werden soll, wenn dessen TTL 0 ist oder dessen TTL den Wert für Maximale TTL für positive Cacheeinträge überschreitet.</p> <p>Der Standardwert ist 86400.</p>
Maximale TTL für negative Cacheeinträge	<p>Geben Sie den Wert ein, auf den die TTL bei einem negativen dynamischen Eintrag im Cache gesetzt werden soll.</p> <p>Der Standardwert ist 86400.</p>
Alternative Schnittstelle, um DNS-Server zu erhalten	<p>Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.</p> <p>Der Standardwert ist <i>Automatisch</i>, d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.</p>

Felder im Menü Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse

Feld	Beschreibung
Als DHCP-Server	<p>Wählen Sie aus, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn Ihr Gerät als DHCP-Server genutzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i>: Es wird keine Name-Server-Adresse übermittelt. • <i>Eigene IP-Adresse</i> (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • <i>DNS-Einstellung</i>: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	<p>Wählen Sie aus, welche Name-Server-Adressen von Ihrem Gerät bei einer dynamischen Name-Server-Aushandlung übermit-</p>

Feld	Beschreibung
	<p>telt werden, wenn Ihr Gerät als IPCP-Server für PPP-Verbindungen genutzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i>: Es wird keine Name-Server-Adresse übermittelt. • <i>Eigene IP-Adresse</i>: Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • <i>DNS-Einstellung</i> (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

16.1.2 DNS-Server

Im Menü **Lokale Dienste->DNS->DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

16.1.2.1 Bearbeiten oder Neu

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

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern über unterschiedliche Schnittstellen eingerichtet sind und Lastverteilung verwendet wird.

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<p>Wählen Sie aus, ob der DNS-Server aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.
Priorität	Weisen Sie dem DNS-Server eine Priorität zu.

Feld	Beschreibung
	<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 (Primärer DNS-Server und Sekundärer DNS-Server) zuweisen. Verwendet wird das Paar mit der höchsten Priorität, wenn die Schnittstelle im Zustand "up" ist.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 9 (niedrigste Priorität).</p> <p>Der Standardwert ist 5.</p>
Schnittstellenmodus	<p>Wählen Sie aus, ob die IP-Adressen von Name-Servern für die Namensauflösung von Internet-Adressen automatisch bezogen oder ob abhängig von der Priorität bis zu zwei feste DNS-Server-Adressen eingetragen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> • <i>Dynamisch</i> (Standardwert)
Schnittstelle	<p>Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll.</p> <p>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 Schnittstellenmodus = <i>Dynamisch</i></p> <p>Mit der Einstellung <i>Keine</i> wird ein globaler DNS-Server angelegt.</p> <p>Bei Schnittstellenmodus = <i>Statisch</i></p> <p>Mit der Einstellung <i>Beliebig</i> wird ein DNS-Server für alle Schnittstellen konfiguriert.</p>
IP-Version	<p>Wählen Sie die verwendete IP-Version aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IPv4</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IPv6</i> <p>Standardmäßig ist <i>IPv4</i> ausgewählt.</p>
Primärer IPv4-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie die IPv4-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer IPv4-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie optional die IPv4-Adresse eines alternativen Name-Servers ein.</p>
Primärer IPv6-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie die IPv6-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer IPv6-DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Statisch</i></p> <p>Geben Sie optional die IPv6-Adresse eines alternativen Name-Servers ein.</p>

16.1.3 Statische Hosts

Im Menü **Lokale Dienste->DNS->Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

16.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü BasisparameterStandarddomäne

Feld	Beschreibung
Standarddomäne	Hier wird die Domäne angezeigt, die Sie im Menü DNS->Globale Einstellungen als Domänennamen eingetragen haben.
DNS-Hostname	Geben Sie den Host-Namen ein, dem die in diesem Menü definierte IP-Adresse zugeordnet werden soll, wenn eine DNS-Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage ne-

Feld	Beschreibung
	<p>gativ 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>
Antwort	<p>Wählen Sie die Art der Antwort auf DNS-Anfragen zu diesem Eintrag aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Negativ</i>: Eine DNS-Anfrage nach DNS-Hostname wird negativ beantwortet. • <i>Positiv</i> (Standardwert): Eine DNS-Anfrage nach DNS-Hostname wird mit der dazugehörigen IP-Adresse beantwortet. • <i>Keine</i>: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IPv4-Adresse	<p>Nur bei Antwort = <i>Positiv</i></p> <p>Geben Sie die IPv4-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>
IPv6-Adresse	<p>Nur bei Antwort = <i>Positiv</i></p> <p>Geben Sie die IPv6-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>

16.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste->DNS->Domänenweiterleitung** wird eine Liste aller konfigurierter Weiterleitungen für definierte Domänen angezeigt.

16.1.4.1 Neu

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

Das Menü **Lokale Dienste->DNS->Domänenweiterleitung->Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	<p>Wählen Sie aus, ob Anfragen bezüglich eines Hosts oder einer Domäne weitergeleitet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Host</i> (Standardwert) • <i>Domäne</i>
Host	<p>Nur für Weiterleiten = <i>Host</i> und Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie den Namen des Hosts ein, für den Anfragen weitergeleitet werden sollen.</p> <p>Bei Eingabe eines Namens ohne "." wird nach Bestätigung mit OK der Eintrag mit dem im Menü Lokale Dienste->DNS->Globale Einstellungen unter Domänenname eingetragenen Namen ergänzt.</p>
Domäne	<p>Nur für Weiterleiten = <i>Domäne</i> und Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie den Namen der Domäne ein, für die Anfragen weitergeleitet werden sollen.</p> <p>Der Eintrag kann mit der Wildcard "*" beginnen, z. B. "*.mustermann.lan".</p> <p>Bei Eingabe eines Namens ohne führende Wildcard "*" wird nach Bestätigung mit OK automatisch eine führende Wildcard "*" eingefügt.</p>
Weiterleiten an	<p>Wählen Sie aus, ob zutreffende DNS-Anfragen an den DNS-Server einer Schnittstelle oder an einen manuell konfigurierten</p>

Feld	Beschreibung
	<p>DNS-Server weitergeleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnittstelle</i> (Standardwert): Anfragen werden an den DNS-Server entweder einer automatisch gewählten oder einer manuell konfigurierten Schnittstelle weitergeleitet. • <i>DNS-Server</i>: Anfragen werden an einen definierten DNS-Server weitergeleitet.
Zielschnittstelle	<p>Nur für Weiterleiten an = <i>Schnittstelle</i></p> <p>Wählen Sie die Schnittstelle aus, an deren DNS-Server Anfragen weitergeleitet werden sollen.</p>
Quellschnittstelle	<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>
Primärer DNS-Server (IPv4/IPv6)	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie die IPv4/IPv6-Adresse des primären DNS-Servers ein.</p>
Sekundärer DNS-Server (IPv4/IPv6)	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie IPv4/IPv6-Adresse des sekundären DNS-Servers ein.</p>

16.1.5 Dynamische Hosts

Im Menü **Lokale Dienste->DNS->Dynamische Hosts** sehen Sie die relevanten Angaben zu den Dynamischen DNS-Einträgen.

16.1.6 Cache

Im Menü **Lokale Dienste->DNS->Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** markieren.

Durch Markieren eines Eintrags und Bestätigen mit **Als statisch festlegen** wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet aus dieser Liste und wird in der Liste im Menü **Statische Hosts** angezeigt. Die TTL wird übernommen.

16.1.7 Statistik

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der Cache-Treffer pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

16.2 HTTPS

Die Benutzeroberfläche Ihres Geräts können Sie von jedem PC aus mit einem aktuellen Web-Browser auch über eine HTTPS-Verbindung bedienen.

HTTPS (HyperText Transfer Protocol Secure) ist hierbei das Verfahren, um zwischen dem Browser, der zur Konfiguration verwendet wird, und dem Gerät eine verschlüsselte und au-

thentifizierte Verbindung mittels SSL aufzubauen.

16.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Das Menü besteht aus folgenden Feldern:

Felder im Menü HTTPS-Parameter

Feld	Beschreibung
HTTPS-TCP-Port	<p>Geben Sie den Port ein, über den die HTTPS-Verbindung aufgebaut werden soll.</p> <p>Möglich sind Werte von 0 bis 65535.</p> <p>Der Standardwert ist 443.</p>
Lokales Zertifikat	<p>Wählen Sie ein Zertifikat aus, das für die HTTPS-Verbindung verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Intern</i> (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möchten. • <i><Zertifikatsname></i>: Wählen Sie ein unter Systemverwaltung->Zertifikate->Zertifikatsliste eingetragenes Zertifikat aus.

16.3 DynDNS-Client

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Hostnamens bei einem DynDNS-Provider
- Konfiguration Ihres Geräts

Registrierung

Bei der Registrierung des Hostnamens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Hostname für Ihr Gerät ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt für Sie die Aufgabe, alle DNS-Anfragen bezüglich des Hosts *dyn_client.provider.com* mit der dynamischen IP-Adresse Ihres Geräts zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Geräts informiert ist, kontaktiert Ihr Gerät beim Aufbau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse.

16.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

16.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen genau so ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internetanbieters).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	Wählen Sie den DynDNS-Provider aus, bei dem die eingegebenen Daten registriert sind. Es stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren

Feld	Beschreibung
	<p>Protokolle unterstützt werden.</p> <p>Weitere DynDNS-Provider können im Menü Lokale Dienste->DynDNS-Client->DynDNS-Provider konfiguriert werden.</p> <p>Der Standardwert ist <i>DynDNS</i> .</p>
Aktualisierung aktivieren	<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>
HTTPS/SSL	<p>Diese Option steht nur zur Verfügung, wenn der von Ihnen ausgewählte DynDNS-Anbieter SSL unterstützt. Im Menü Lokale Dienste->DynDNS-Client->DynDNS-Provider 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>
Zertifikatsüberprüfung	<p>Aktivieren Sie diese Funktion, um das SSL-Zertifikat des Servers zu überprüfen.</p>
IP-Version	<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 an-</p>

Feld	Beschreibung
	sonsten gleichen Einstellungen an. Informieren Sie sich bei Ihrem Anbieter, ob dieser Mehrfachaktualisierungen unterstützt!

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Mail-Exchanger (MX)	Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll. Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.
Wildcard	Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von Hostname zur aktuellen IP-Adresse von Schnittstelle aktiviert werden soll (Erweiterte Namensauflösung). Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

16.3.2 DynDNS-Provider

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

16.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.

Feld	Beschreibung
Aktualisierungspfad	<p>Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist.</p> <p>Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.</p>
Port	<p>Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll.</p> <p>Erfragen Sie den entsprechenden Port bei Ihrem Provider.</p> <p>Der Standardwert ist <i>80</i>.</p>
Protokoll	<p>Wählen Sie eines der implementierten Protokolle aus. Welches Protokoll Ihr Anbieter verwendet, erfahren Sie in dessen Anleitung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DynDNS</i> (Standardwert) • <i>Static DynDNS</i> • <i>ODS</i> • <i>HN</i> • <i>DYNS</i> • <i>GnuDIP-HTML</i> • <i>GnuDIP-TCP</i> • <i>Custom DynDNS</i> • <i>DnsExit</i> • <i>dyndnss</i> • <i>dyndns2</i>
Aktualisierungsintervall	<p>Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf.</p> <p>Der Standardwert ist <i>300</i> Sekunden.</p>
IPv6-Server	<p>Geben Sie den Host-Namen oder die IPv6-Adresse des DynDNS-Servers ein, wenn Sie IPv6-Adressen aktualisieren wollen.</p>

Feld	Beschreibung
Supports SSL	Aktivieren Sie diese Option, wenn Ihr DynDNS-Anbieter SSL zur Absicherung der Datenübertragung unterstützt. Standardmäßig ist die Option deaktiviert.
Homepage	Hier können Sie eine Web-Adresse angeben, mit der Sie direkt auf die Seite des Anbieters gelangen.

16.4 DHCP-Server

Sie können Ihr Gerät als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) konfigurieren.

Jeder Rechner in Ihrem LAN benötigt, wie auch Ihr Gerät, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie Ihr Gerät als DHCP-Server einrichten, vergibt es anfragenden Rechnern im LAN automatisch IP-Adressen aus einem definierten IP-Adress-Pool.

Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine DHCP-Anfrage (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server. Daraufhin erhält der Client (im Zuge einer kurzen Kommunikation) vom bintec elmeg seine IP-Adresse.

Sie müssen so den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem Ihr Gerät jeweils für einen definierten Zeitraum IP-Adressen an Hosts im LAN vergibt. Ein DHCP-Server übermittelt auch die Adressen des statisch oder per PPP-Aushandlung eingetragenen Domain-Name-Servers (DNS), des NetBIOS Name Servers (WINS) und des Standard-Gateways.

Konkrete Hinweise für die Konfiguration eines DHCP-Servers, eines DHCP-Clients oder eines DHCP-Relay-Servers (siehe auch [DHCP-Relay-Einstellungen](#) auf Seite 389) finden Sie am Ende des Kapitels unter [DHCP - Konfigurationsbeispiel](#) auf Seite 389.

16.4.1 IP-Pool-Konfiguration

Im Menü **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration** wird eine Liste aller konfigurierten IP-Pools angezeigt. Diese Liste ist global und zeigt auch in anderen Menüs konfigurierte Pools an.

16.4.1.1 Bearbeiten oder Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

16.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration** wird eine Liste aller konfigurierten DHCP-Pools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. deaktivieren.



Hinweis

Im Auslieferungszustand ist der DHCP-Pool mit den IP-Adressen 192.168.0.10 bis 192.168.0.49 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

16.4.2.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die in IP-Adressbereich definierten Adressen an anfragende DHCP-Clients vergeben werden.</p> <p>Wenn eine DHCP-Anfrage über diese Schnittstelle eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.</p>
IP-Poolname	<p>Wählen Sie einen im Menü Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration konfigurierten IP-Poolnamen aus.</p>
Pool-Verwendung	<p>Wählen Sie aus, ob der DHCP-Pool für Anfragen von DHCP-Clients in einem direkt an die Schnittstelle angeschlossenen Ethernet verwendet werden soll oder für DHCP-Anfragen, die aus einem über Gateways erreichbaren Ethernet stammen und über eine DHCP-Relaisstation an Ihr Gerät weitergeleitet wurden.</p> <p>In letzterem Fall ist es möglich, einen IP-Adresspool für ein entfernt liegendes Netz zu verwenden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal</i> (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen aus einem direkt an die Schnittstelle angeschlossenen Ethernet verwendet. • <i>Relais</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus einem über Gateways erreichbaren Ethernet verwendet. • <i>Lokal/Relais</i>: Der DHCP-Pool kann für lokale und für weitergeleitete DHCP-Anfragen aus direkt angeschlossenen bzw. über Gateways erreichbaren Ethernets verwendet werden.
Beschreibung	<p>Geben Sie eine beliebige Beschreibung ein, um den DHCP-Pool eindeutig zu benennen.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Gateway	<p>Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Router als Gateway verwenden</i> (Standardwert): Hier wird die für die Schnittstelle definierte IP-Adresse übertragen. • <i>Kein Gateway</i>: Hier wird keine IP-Adresse übermittelt. • <i>Angeben</i>: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	<p>Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll.</p> <p>Nachdem Lease Time abgelaufen ist, kann die Adresse durch den Server neu vergeben werden.</p> <p>Der Standardwert ist <i>120</i>.</p>
DHCP-Optionen	<p>Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen.</p> <p>Mögliche Werte für Option:</p> <ul style="list-style-type: none"> • <i>Zeitserver</i> (Standardwert): Geben Sie die IP-Adresse des Zeitserver ein, die dem Client übermittelt werden soll. • <i>DNS-Server</i>: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • <i>DNS-Domänename</i>: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • <i>WINS/NBNS-Server</i>: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • <i>WINS/NBT Node Type</i>: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • <i>TFTP-Server</i>: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • <i>CAPWAP Controller</i>: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • <i>URL (Provisionierungsserver)</i>: Mit dieser Option kön-

Feld	Beschreibung
	<p>nen Sie einem Client eine beliebige URL übermitteln.</p> <p>Verwenden Sie diese Option, um anfragenden IP1x0-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form <code>http://<IP-Adresse des Provisionierungsservers>/eg_prov</code> haben.</p> <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche Hinzufügen 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
Hersteller auswählen	<p>Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Sonstige</i> (Standardwert) • <i>-bintec-</i>
APN	Nur für Hersteller auswählen = <i>-bintec-</i>

Feld	Beschreibung
	Geben Sie den Access Point Namen (APN) der SIM-Karte ein.
PIN	Nur für Hersteller auswählen = <i>-bintec-</i> Geben Sie die PIN der SIM-Karte ein.
Herstellerbeschreibung	Nur für Hersteller auswählen = <i>Sonstige</i> Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.
Hersteller-ID	Nur für Hersteller auswählen = <i>Sonstige</i> Um das Gerät zu identifizieren, geben Sie hier die Hersteller-ID ein.
Herstellerspezifische Informationen	Nur für Hersteller auswählen = <i>Sonstige</i> Geben Sie die Hersteller spezifischen Konfigurationsparameter ein.

Felder im Menü Basisparameter für Herstellergruppen

Feld	Beschreibung
Hersteller auswählen	Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Siemens</i> (Standardwert) • <i>Sonstige</i>
Provisioning-Server (code 3)	Nur für Hersteller auswählen = <i>Siemens</i> Geben Sie ein, welcher herstellerepezifische Wert übermittelt werden soll. Für die Einstellung Hersteller auswählen = <i>Siemens</i> wird der Standardwert <i>sdlp</i> angezeigt. Sie können die IP-Adresse des gewünschten Servers ergänzen.
Herstellerbeschreibung	Nur für Hersteller auswählen = <i>Sonstige</i> Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.

Feld	Beschreibung
Hersteller-ID	Nur für Hersteller auswählen = <i>Sonstige</i> Um das Gerät zu identifizieren, geben Sie hier die Hersteller-ID ein.
Benutzerdefinierte DHCP-Optionen	Nur für Hersteller auswählen = <i>Sonstige</i> Fügen Sie mit Hinzufügen weitere Einträge hinzu. Sie können DHCP-Optionen hinzufügen.

16.4.3 IP/MAC-Bindung

Im Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.



Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration** IP-Adressbereiche konfiguriert wurden, und im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration** ein gültiger IP-Pool zugewiesen ist.

16.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

Das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen MAC-Adresse die IP-Adresse gebunden wird.

Feld	Beschreibung
	Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.
IP-Adresse	Geben Sie die IP-Adresse ein, die der in MAC-Adresse angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in IP-Adresse angegebene IP-Adresse zugewiesen werden soll.

16.4.4 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

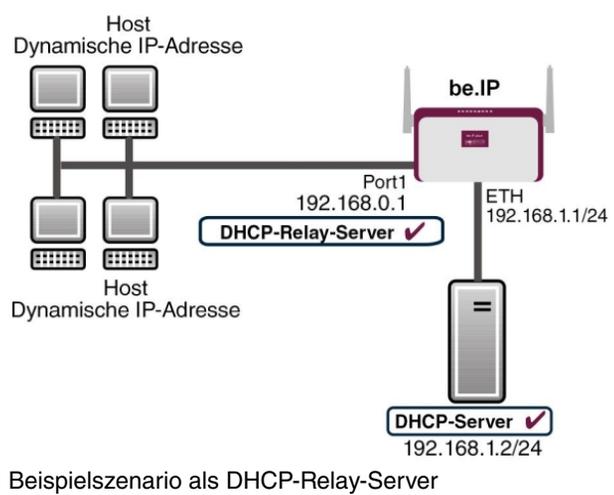
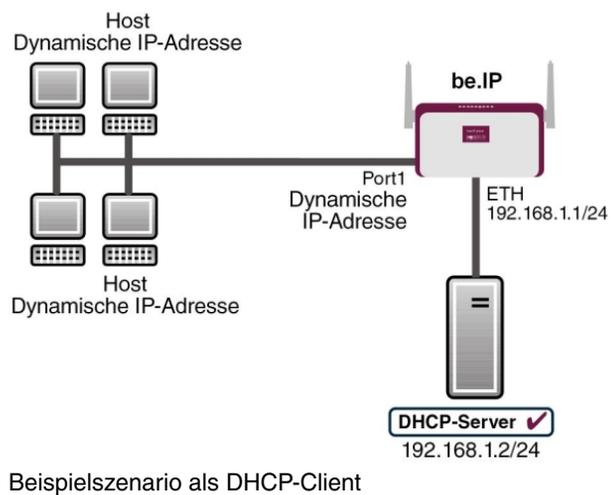
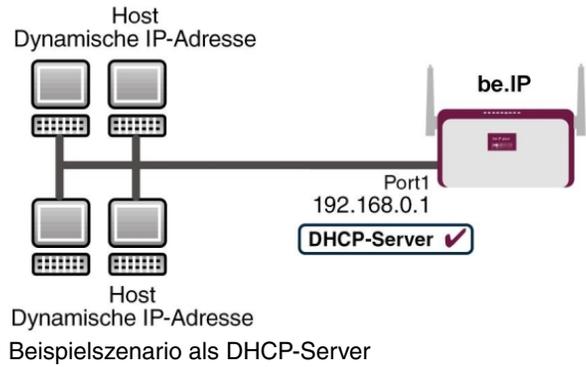
Feld	Beschreibung
Primärer DHCP-Server	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen. Der Standardwert ist <i>0.0.0.0</i> .
Sekundärer DHCP-Server	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein. Der Standardwert ist <i>0.0.0.0</i> .

16.4.5 DHCP - Konfigurationsbeispiel

Voraussetzungen

- Optional ein DHCP-Server

Beispiel-Szenarien



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>
Lease Time	Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu->Erweiterte Einstellungen	z. B. <i>120</i>
Für DNS- / WINS-Serverzuordnung zu verwendende IP-Adresse	Lokale Dienste->DNS->Globale Einstellungen->Erweiterte Einstellungen	z. B. <i>Eigene IP-Adresse</i>

DHCP-Client

Feld	Menü	Wert
Adressmodus	LAN->IP-Konfiguration->Schnittstellen-> <en1-4>-> 	<i>DHCP</i>

Feld	Menü	Wert
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. <i>192.168.1.2</i>
Sekundärer DHCP-Server (optional)	Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen	falls vorhanden

16.5 DHCPv6-Server

Sie können Ihr Gerät als DHCPv6-Server verwenden. Dieser DHCPv6-Server kann IP-Adressen und DHCP-Optionen an Clients verteilen oder auch nur DHCP-Optionen ohne Adressen. Diese Parameter werden in einem sogenannten "Option Set" zusammengefasst. Ein Option Set kann an eine Schnittstelle gebunden werden (siehe unter **Lokale Dienste->DHCPv6-Server->DHCPv6-Server->Neu**) oder es kann global konfiguriert werden (siehe unter **Lokale Dienste->DHCPv6-Server->Globale DHCPv6-Optionen->Neu**). DHCP-Optionen können zum Beispiel Informationen über DNS-Server oder Zeitserver enthalten.



Hinweis

Ein IPv6-Adress-Pool entsteht durch die Zuweisung eines IPv6-Link-Präfixes (Subnetz mit der Länge /64) zu einem DHCPv6 Option Set. Die Definition eines eigenen Abschnitts von IPv6-Adressen, wie z. B. `fc00:1:2:3::1.fc00:1:2:3::100` ist anders als im DHCPv4 nicht vorgesehen.

Für die Konfiguration eines IPv6-Adress-Pools müssen folgende Voraussetzungen erfüllt sein:

- (a) IPv6 muss auf der betreffenden Schnittstelle aktiviert sein.
- (b) Ein IPv6-Link-Präfix (Subnetz) mit der Länge /64 muss auf der gewünschten Schnittstelle konfiguriert sein. Ein IPv6-Link-Präfix kann auf zwei Arten definiert sein:
 - Der IPv6-Link-Präfix ist von einem Allgemeinen IPv6-Präfix (Präfix mit einer Länge von zum Beispiel /56 oder /48) abgeleitet. In diesem Fall muss der Allgemeine

IPv6-Präfix im Menü **Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes** konfiguriert sein.

- Der IPv6-Link-Präfix mit Länge /64 wird manuell auf der entsprechenden Schnittstelle konfiguriert und nicht von einem Allgemeinen IPv6-Präfix abgeleitet.

(c) Die Option **DHCP-Server** muss für die Schnittstelle aktiviert sein.

Darüber hinaus sind folgende Einstellungen empfehlenswert:

- Die Werte für die Optionen **Bevorzugte Gültigkeitsdauer** und **Gültigkeitsdauer** sollten auf Werte gesetzt werden, die größer sind als der Wert für **Router-Gültigkeitsdauer**.

Bei einer **Router-Gültigkeitsdauer** von 600 Sekunden, empfehlen sich z. B. eine **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**

16.5.1 DHCPv6-Server

Hier können Sie - bezogen auf eine Schnittstelle - in einem Option Set Adresspools anlegen und DHCP-Options definieren.

16.5.1.1 Bearbeiten oder Neu

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

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

Felder im Menü Basisparameter

Feld	Beschreibung
Name	Geben Sie einen Namen für das Option Set ein.
Schnittstelle	<p>Wählen Sie die IPv6-Schnittstelle, an die das Option Set gebunden sein soll.</p> <p>Zur Auswahl stehen Schnittstellen mit folgender Konfiguration:</p> <ul style="list-style-type: none"> • IPv6 ist aktiviert. • Die Option DHCP-Server ist aktiviert. <p>Im Auslieferungszustand ist IPv6 für alle Schnittstellen deaktiviert. Erscheint die gewünschte Schnittstelle nicht in der Auswahl, konfigurieren Sie sie im Menü LAN->IP-Konfiguration->Schnittstellen gemäß den in der Einleitung genannten Vorgaben.</p>
Address assignment	<p>Die Definition eines IPv6-Adresspools erfolgt durch Zuweisung eines IPv6-Link-Präfixes (Subnetz mit Länge /64) zu einem DHCPv6 Option Set. Der IPv6-Adress-Pool umfasst immer den kompletten 64-Bit-Adressraum des gewählten IPv6-Link-Präfixes. Die Adressvergabe erfolgt zufällig.</p> <p>Mit Hinzufügen können Sie dem IPv6 Option Set einen oder mehrere IPv6-Link-Präfixe zuordnen.</p>
	<div style="border: 1px solid gray; padding: 5px;">  <p>Hinweis</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
DNS-Domänen-Suchliste	<p>Mit Hinzufügen können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt.</p>

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

Felder im Menü **Erweiterte Server-Optionen**

Feld	Beschreibung
DNS-Server	<p>Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server").</p> <p>In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld DNS-Propagation im Menü LAN->IP-Konfiguration->Schnittstellen-> ->Erweiterte Einstellungen mit IPv6 = Aktiviert konfiguriert.)</p> <p>Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option RA oder globalen Fallback-DNS-Server verwenden und erstellen Sie mit Hinzufügen die gewünschten DNS-Server-Einträge.</p>
SNTP-Server	<p>Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit Hinzufügen können Sie die gewünschten Zeitserver-Einträge anlegen.</p>

16.5.2 Globale DHCPv6-Optionen

In diesem Menü können Sie die für den DHCPv6-Server global gültigen DHCPv6-Optionen konfigurieren. Eine hier konfigurierte Option wird immer dann propagiert, wenn für diese Option keine exaktere Definition (z.B. keine schnittstellenspezifische oder Vendor-ID-spezifische Definition) existiert.

Das Menü besteht aus folgenden Feldern:

Felder im Menü **Basisparameter**

Feld	Beschreibung
DNS-Domänen-Suchliste	<p>Mit Hinzufügen können Sie eine Liste von Domain-Namen erstellen, die auf Client-Seite als Domain-Suchliste bei der Namensauflösung verwendet werden soll (DHCPv6 Option 24 "Domain Search List"). Die Domain-Namen werden gemäß der durch die Liste vorgegebenen Reihenfolge an die Clients übermittelt. Der Domain-Name (z. B. dev.bintec.de.) muss mit Punkt (.) enden.</p>

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

Felder im Menü Server-Priorität

Feld	Beschreibung
Server-Priorität	<p>In den vom DHCPv6 Server an die Clients gesendeten DHCPv6 Advertisements kann die DHCPv6-Option 7 Preference enthalten sein.</p> <p>Mögliche Werte sind $0 \dots 255$. In einem Netzwerk mit mehreren DHCPv6 Servern wird über diese Option gesteuert, welcher DHCPv6-Server im Netzwerk die höchste Priorität besitzt. Empfängt ein Client DHCPv6 Advertisements mit unterschiedlicher Priorität von verschiedenen Servern, so wird der Client in der Regel die Werte des Servers mit der höchsten Priorität übernehmen. Der Client kann jedoch auch DHCPv6 Advertisements mit niedrigerer Priorität akzeptieren, wenn der im DHCPv6 Advertisement enthaltene Parametersatz mehr den vom Client angeforderten Optionen entspricht.</p> <p>Der Wert 0 bedeutet "nicht spezifiziert" (niedrigste Priorität), 255 bedeutet höchste Priorität.</p>

Felder im Menü Erweiterte Server-Optionen

Feld	Beschreibung
DNS-Server	<p>Hier können Sie die DNS-Server konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 23 "DNS Recursive Name Server").</p> <p>In der Standardeinstellung werden die globalen DNS-Server des Systems propagiert. (Die globalen DNS-Server werden im Feld DNS-Propagation im Menü LAN->IP-Konfiguration->Schnittstellen->  ->Erweiterte Einstellungen mit IPv6 = Aktiviert konfiguriert.)</p> <p>Sie können aber auch DNS-Server manuell angeben und an die Clients übertragen. Deaktivieren Sie hierzu die Option RA oder globalen Fallback-DNS-Server verwenden und erstellen Sie mit Hinzufügen die gewünschten DNS-Server-Einträge.</p>
SNTP-Server	<p>Hier können Sie die Zeitserver konfigurieren, die per DHCPv6 propagiert werden sollen (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Mit Hinzufügen können Sie die gewünschten Zeitserver-Einträge anlegen.</p>

16.5.3 Zustandsbehaftete Clients

Hier sehen Sie Informationen zu zustandsbehafteten Clients, sobald diese eine IPv6-Adresse bezogen haben.

16.5.4 Konfiguration von zustandsbehafteten Clients

Bei einer zustandsbezogenen Konfiguration von IPv6 Clients, wird dem Client neben den DHCP-Optionen auch der IPv6-Präfix übermittelt.

16.5.4.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um Einträge für Stateful Clients anzulegen. Normalerweise müssen Sie keine Einträge anlegen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Sie sollten jeden automatisch angelegten Eintrag einmal aufrufen, um den Inhalt zu prüfen und gegebenenfalls anzupassen.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DUID	Ein Client verwendet das Feld DUID (DHCP Unique Identifier), um sich zu identifizieren und eine IP-Adresse vom DHCPv6-Server zu beziehen. Wenn Sie mit der Schaltfläche Neu einen Eintrag anlegen, können Sie die DUID als 16- bis 20-stellige HEX-Zahl eingeben. Sie können sie mit den Trennzeichen Minus eingeben wie unter Windows oder als Block ohne Trennzeichen wie unter Linux.
Client FQDN akzeptieren	Wenn Client FQDN akzeptieren aktiviert ist, wird der Client mit dem Parameter FQDN (Fully Qualified Domain Name) im Cache des Domain Name Servers eingetragen.
Administrative FQDNs	Mit Hinzufügen können Sie - auch bei automatisch angelegten Einträgen - den Parameter FQDN (Fully Qualified Domain Name) eingeben.
Kennung der statischen Schnittstelle	Das Feld Kennung der statischen Schnittstelle ist der Host-Anteil der IPv6-Adresse, d.h. die letzten 64 Bit der IPv6-Adresse. Dieser Präfix muss mit :: anfangen.

16.6 Scheduling

Ihr Gerät verfügt über einen Aufgabenplaner, mit dem bestimmte Standardaktionen (beispielsweise Aktivierung bzw. Deaktivierung von Schnittstellen) durchgeführt werden können. Außerdem ist jede vorhandene MIB-Variable mit jedem beliebigen Wert konfigurierbar.

Sie legen die gewünschten **Aktionen** fest und definieren die **Auslöser**, die steuern, wann bzw. unter welchen Bedingungen die **Aktionen** durchgeführt werden sollen. Ein **Auslöser** kann ein einzelnes Ereignis sein oder eine Folge von Ereignissen, die in einer **Ereignisliste** zusammengefasst sind. Für ein einzelnes Ereignis legen Sie ebenfalls eine Ereignisliste an, die jedoch nur ein Element enthält.

Es ist möglich, zeitgesteuert Aktionen auszulösen. Außerdem kann der Status oder die Erreichbarkeit von Schnittstellen oder deren Datenverkehr zur Ausführung der konfigurierten Aktionen führen, oder aber auch die Gültigkeit von Lizenzen. Auch hier ist es möglich, jede beliebige MIB-Variable mit jedem beliebigen Wert als Auslöser einzurichten.

Um den Aufgabenplaner in Betrieb zu nehmen, aktivieren Sie das **Schedule-Intervall** unter **Optionen**. Dieses Intervall gibt den Zeitabstand vor, in dem das System prüft, ob mindestens ein Ereignis eingetreten ist. Dieses Ereignis dient als Auslöser für eine konfigurierte Aktion.

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.

16.6.1 Auslöser

Im Menü **Lokale Dienste->Scheduling->Auslöser** werden alle konfigurierten Ereignislisten angezeigt. Jede Ereignisliste enthält mindestens ein Ereignis, das als Auslöser für eine Aktion vorgesehen ist.

16.6.1.1 Neu

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

Das Menü **Lokale Dienste->Scheduling->Auslöser->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ereignisliste	<p>Mit <i>Neu</i> (Standardwert) können Sie eine neue Ereignisliste anlegen. Mit Beschreibung geben Sie dieser Liste einen Namen. Mit Hilfe der übrigen Parameter legen Sie das erste Ereignis in der Liste an.</p> <p>Wenn Sie eine bestehende Ereignisliste erweitern wollen, wählen Sie die gewünschte Ereignisliste aus und fügen ihr mindestens ein Ereignis hinzu.</p> <p>Über Ereignislisten können auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden. Die Ereignisse werden in derselben Reihenfolge abgearbeitet, wie sie in der Liste angelegt sind.</p>
Beschreibung	<p>Nur für Ereignisliste = <i>Neu</i></p> <p>Geben Sie eine beliebige Bezeichnung für die Ereignisliste ein.</p>
Ereignistyp	<p>Wählen Sie den Typ des Ereignisses aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zeit</i> (Standardwert): Die in Aktionen konfigurierten und zugewiesenen Aktionen werden zu bestimmten Zeitpunkten ausgelöst. • <i>MIB/SNMP</i>: Die in Aktionen konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen. • <i>Schnittstellenstatus</i>: Die in Aktionen konfigurierten

Feld	Beschreibung
	<p>und zugewiesene Aktionen werden ausgelöst, wenn die definierten Schnittstellen einen bestimmten Status annehmen.</p> <ul style="list-style-type: none"> • <i>Schnittstellenverkehr</i>: Die in Aktionen konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn der Datenverkehr auf den angegebenen Schnittstellen den definierten Wert unter- oder überschreitet. • <i>Ping-Test</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist. • <i>Lebensdauer eines Zertifikats</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist. • <i>Funktionstaste</i> (nicht für alle Geräte verfügbar): Mit der Option <i>Funktionstaste</i> legen Sie fest, dass das Drücken der Funktionstaste am Gerät als Auslöser für konfigurierte Aktionen dienen kann. Durch einen Druck von gut einer Sekunde (aber weniger als drei Sekunden) auf die Taste wird der Zustand der Taste auf <i>Aktiv</i> gesetzt, durch einen Druck von mehr als drei Sekunden wird er auf <i>Inaktiv</i> gesetzt. Aktionen, die vom Zustand der Taste abhängen, werden dann bei der nächsten zyklischen Abfrage gemäß dem Schedule-Intervall ausgelöst. Es kann also z. B. eine WLAN-Schnittstelle aktiviert werden, wenn die Funktionstaste eine Sekunde lang gedrückt wird. Bei einem Druck auf die Taste vom mehr als drei Sekunden wird die Schnittstelle wieder deaktiviert. • <i>Status der GEO-Zone</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierten GEO-Zonen einen bestimmten Status annehmen.
Überwachte GEO-Zone	<p>Nur für Ereignistyp <i>Status der GEO-Zone</i></p> <p>Wählen Sie eine konfigurierte GEO-Zone aus.</p>
GEO Zone Status	<p>Nur für Ereignistyp <i>Status der GEO-Zone</i></p> <p>Wählen Sie den GEO Zone Status aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Wahr</i>: Die aktuelle Position liegt innerhalb der definierten Zone. • <i>Falsch</i>: Die aktuelle Position liegt außerhalb der definierten

Feld	Beschreibung
	Zone.
Überwachte Variable	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren definierter Wert als Auslöser konfiguriert werden soll. Wählen Sie zunächst das System aus, in dem die MIB-Variable gespeichert ist, dann die MIB-Tabelle und dann die MIB-Variable selber. Es werden nur die MIB-Tabellen und MIB-Variablen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
Vergleichsbedingung	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie aus, ob die MIB-Variable <i>Größer</i> (Standardwert), <i>Gleich</i>, <i>Kleiner</i>, <i>Ungleich</i> dem in <i>Vergleichswert</i> angegebenen Wert sein oder innerhalb von <i>Bereich</i> liegen muss, um die Aktion auszulösen.</p>
Vergleichswert	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Geben Sie den Wert der MIB-Variable ein.</p>
Indexvariablen	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in der MIB-Tabelle eindeutig zu kennzeichnen, z.B. <i>ConnIfIndex</i>. Aus der Kombination von Indexvariable (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und Indexwert ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere Indexvariablen mit Hinzufügen an.</p>
Überwachte Schnittstelle	<p>Nur für Ereignistyp <i>Schnittstellenstatus</i> und <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.</p>
Schnittstellenstatus	<p>Nur für Ereignistyp <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Die Schnittstelle ist aktiv. • <i>Inaktiv</i>: Die Schnittstelle ist inaktiv.
Richtung des Datenverkehrs	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>RX</i> (Standardwert): Der eingehende Datenverkehr wird überwacht. • <i>TX</i>: Der ausgehende Datenverkehr wird überwacht.
Bedingung des Schnittstellenverkehrs	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Wählen Sie aus, ob der Wert für Datenverkehr <i>Größer</i> (Standardwert) oder <i>Kleiner</i> dem in <i>Übertragener Datenverkehr</i> angegebenen Wert sein muss, um die Aktion auszulösen.</p>
Übertragener Datenverkehr	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Geben Sie den gewünschten Wert für den Datenverkehr, mit dem verglichen werden soll, in kBytes ein.</p> <p>Der Standardwert ist <i>0</i>.</p>
Ziel-IP-Adresse	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
Quell-IP-Adresse	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das

Feld	Beschreibung
	Eingabefeld ein.
Status	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Wählen Sie aus, ob Ziel-IP-Adresse <i>Erreichbar</i> (Standardwert) oder <i>Nicht erreichbar</i> sein muss, um die Aktion auszulösen.</p>
Intervall	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Der Standardwert ist <i>60</i> Sekunden.</p>
Erfolgreiche Versuche	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p> <p>Der Standardwert ist <i>3</i>.</p>
Fehlgeschlagene Versuche	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie ein, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65536</i>.</p> <p>Der Standardwert ist <i>3</i>.</p>
Überwachtes Zertifikat	<p>Nur für Ereignistyp <i>Lebensdauer eines Zertifikats</i></p> <p>Wählen Sie das Zertifikat aus, dessen Gültigkeit überprüft werden soll.</p>

Feld	Beschreibung
Verbleibende Gültigkeitsdauer	Nur für Ereignistyp <i>Lebensdauer eines Zertifikats</i> Geben Sie den gewünschten Wert für die noch verbleibende Gültigkeit des Zertifikats in Prozent ein.
Status der Funktionstaste	Nur für Ereignistyp <i>Funktionstaste</i> Beim Anlegen des Auslösers können Sie über die Auswahl des Status der Funktionstaste festlegen, bei welchem Zustand der Funktionstaste der Auslöser aktiv sein soll. Setzen Sie den Status auf <i>An</i> , so wird der Auslöser aktiv, wenn der Zustand der Funktionstaste <i>Aktiv</i> ist, und inaktiv, wenn der Zustand der Funktionstaste <i>Inaktiv</i> ist. Setzen Sie ihn auf <i>Aus</i> , so wird der Auslöser aktiv, wenn der Zustand der Funktionstaste <i>Inaktiv</i> ist, und inaktiv, wenn der Zustand der Funktionstaste <i>Aktiv</i> ist. Die Zustandsprüfung erfolgt zyklisch im Abstand des konfigurierten Schedule-Intervalls.

Felder im Menü Zeitintervall auswählen

Feld	Beschreibung
Zeitbedingung	Nur für Ereignistyp <i>Zeit</i> Wählen Sie zunächst die Art der Zeitangabe in Bedingungstyp aus. Mögliche Werte: <ul style="list-style-type: none">• <i>Wochentag</i>: Wählen Sie in Bedingungseinstellungen einen Wochentag aus.• <i>Perioden</i> (Standardwert): Wählen Sie in Bedingungseinstellungen einen bestimmten Turnus aus.• <i>Tag des Monats</i>: Wählen Sie in Bedingungseinstellungen einen bestimmten Tag im Monat aus. Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Wochentag</i> : <i>Montag</i> (Standardwert) ... <i>Sonntag</i> . Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Perioden</i> : <ul style="list-style-type: none">• <i>Täglich</i>: Der Auslöser wird täglich aktiv (Standardwert).

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Montag-Freitag</i>: Der Auslöser wird täglich von Montag bis Freitag aktiv. • <i>Montag-Samstag</i> : Der Auslöser wird täglich von Montag bis Samstag aktiv. • <i>Samstag-Sonntag</i> : Der Auslöser wird Samstag und Sonntag aktiv. <p>Mögliche Werte für Bedingungeinstellungen bei Bedingungstyp = Tag des Monats:</p> <p>1... 31.</p>
Startzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.
Stoppzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine Stoppzeit eingeben oder Stoppzeit = Startzeit setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.

16.6.2 Aktionen

Im Menü **Lokale Dienste->Scheduling->Aktionen** wird eine Liste aller Aktionen angezeigt, die durch die in **Lokale Dienste->Scheduling->Auslöser** konfigurierten Ereignisse oder Ereignisketten ausgelöst werden sollen.

16.6.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Aktionen zu konfigurieren.

Das Menü **Lokale Dienste->Scheduling->Aktionen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Bezeichnung für die Aktion ein.
Befehlstyp	Wählen Sie die gewünschte Aktion aus. Mögliche Werte:

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Neustart</i> (Standardwert): Ihr Gerät wird neu gestartet. • <i>MIB/SNMP</i>: Für eine MIB-Variable wird der gewünschte Wert eingetragen. • <i>Schnittstellenstatus</i>: Der Status einer Schnittstelle wird verändert. • <i>WLAN-Status</i>: Nur für Geräte mit Wireless LAN. Der Status einer WLAN-SSID wird verändert. • <i>Softwareaktualisierung</i>: Es wird ein Software-Update initiiert. • <i>Konfigurationsmanagement</i>: Eine Konfigurationsdatei wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert. • <i>Ping-Test</i>: Die Erreichbarkeit einer IP-Adresse wird überprüft. • <i>Zertifikatverwaltung</i>: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • <i>5 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt. • <i>5,8 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt. • <i>WLC: Neuer Neighbor-Scanvorgang</i>: Nur für Geräte mit WLAN Controller. In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • <i>WLC: VSS-Status</i>: Nur für Geräte mit WLAN Controller. Der Status eines Drahtlosnetzwerkes wird verändert. • <i>Betriebsmodus</i>: Der Betriebsmodus eines WLAN-Radiomoduls wird verändert.
Ereignisliste	Wählen Sie die gewünschte Ereignisliste aus, die in Lokale Dienste->Scheduling->Auslöser angelegt ist.
Bedingung für Ereignisliste	<p>Wählen Sie für die gewählte Ereignisliste aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Eins</i>: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt. • <i>Keiner</i>: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt. • <i>Eins nicht</i>: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.
Neustart des Geräts nach	<p>Nur bei Befehlstyp = <i>Neustart</i></p> <p>Geben Sie die Zeitspanne in Sekunden an, die nach dem Eintreten des Ereignisses gewartet werden soll, bis das Gerät neu gestartet wird.</p> <p>Der Standardwert ist <i>60</i> Sekunden.</p>
Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Tabelle aus, in der die MIB-Variable gespeichert ist, deren Wert verändert werden soll. Wählen Sie zunächst das System aus und dann die MIB-Tabelle. Es werden nur die MIB-Tabellen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
Befehlsmodus	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie aus, auf welche Weise der MIB-Eintrag manipuliert werden soll.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Vorhandenen Eintrag ändern</i> (Standardwert): Ein bestehender Eintrag soll verändert werden. • <i>Neuen MIB-Eintrag erstellen</i>: Ein neuer Eintrag soll angelegt werden.
Indexvariablen	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in MIB-Tabelle eindeutig zu kennzeichnen, z. B. <i>ConnIfIndex</i>. Aus der Kombination von Indexvariable (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und Indexwert ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere Indexvariablen mit Hinzufügen an.</p>

Feld	Beschreibung
Status des Auslösers	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie aus, welchen Status das Ereignis haben muss, um die MIB-Variable wie definiert zu verändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Der Wert der MIB-Variable wird verändert, wenn der Auslöser aktiv ist. • <i>Inaktiv</i>: Der Wert der MIB-Variable wird verändert, wenn der Auslöser inaktiv ist. • <i>Beide</i>: Der Wert der MIB-Variable wird unterschiedlich verändert, wenn der Status des Auslösers sich ändert.
MIB-Variablen	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren Wert, abhängig vom Status des Auslösers, verändert werden soll.</p> <p>Ist der Auslöser aktiv (Status des Auslösers <i>Aktiv</i>), wird die MIB-Variable mit dem in Aktiver Wert eingetragenen Wert beschrieben.</p> <p>Ist der Auslöser inaktiv, Status des Auslösers <i>Inaktiv</i>), wird die MIB-Variable mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (Status des Auslösers <i>Beide</i>), wird sie mit einem aktiven Auslöser mit dem in Aktiver Wert eingetragenen Wert und mit einem inaktiven Auslöser mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Legen Sie weitere Einträge mit Hinzufügen an.</p>
Schnittstelle	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.</p>
Schnittstellenstatus festlegen	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert) • <i>Inaktiv</i> • <i>Zurücksetzen</i>
Lokale WLAN-SSID	<p>Nur bei Befehlstyp = <i>WLAN-Status</i></p> <p>Wählen Sie das gewünschte Drahtlosnetzwerk aus, dessen Status verändert werden soll.</p>
Status festlegen	<p>Nur bei Befehlstyp = <i>WLAN-Status</i> oder <i>WLC: VSS-Status</i></p> <p>Wählen Sie den Status aus, den das Drahtlosnetzwerk erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert) • <i>Deaktivieren</i>
Quelle	<p>Nur bei Befehlstyp = <i>Softwareaktualisierung</i></p> <p>Wählen Sie die gewünschte Quelle für die Software-Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktuelle Software vom Update-Server</i> (Standardwert): Die aktuelle Software wird vom Update-Server geladen. • <i>HTTP-Server</i>: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen. • <i>HTTPS-Server</i>: Die aktuelle Software wird von einem HTTPS-Server geladen, den Sie über die <i>Server-URL</i> festlegen. • <i>TFTP-Server</i>: Die aktuelle Software wird von einem TFTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen.
Server-URL	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i> wenn Quelle nicht <i>Aktuelle Software vom Update-Server</i></p> <p>Geben Sie die URL des Servers ein, von dem die gewünschte Softwareversion geholt werden soll.</p>

Feld	Beschreibung
	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> mit Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Konfigurationsdatei geholt oder auf den die Konfigurationsdatei gesichert werden soll.</p>
Dateiname	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i></p> <p>Geben Sie den Dateinamen der Softwareversion ein.</p> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> mit Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie den Dateinamen der Zertifikatsdatei ein.</p>
Aktion	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Konfiguration importieren</i> (Standardwert) • <i>Konfiguration exportieren</i> • <i>Konfiguration umbenennen</i> • <i>Konfiguration löschen</i> • <i>Konfiguration kopieren</i> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i></p> <p>Wählen Sie aus, welche Aktion Sie auf eine Zertifikatsdatei anwenden möchten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zertifikat importieren</i> (Standardwert) • <i>Zertifikat löschen</i> • <i>SCEP</i>
Protokoll	<p>Nur für Befehlstyp = <i>Zertifikatverwaltung</i> und <i>Konfigurationsmanagement</i> wenn Aktion = <i>Konfiguration</i></p>

Feld	Beschreibung
	<p><i>importieren</i></p> <p>Wählen Sie das Protokoll für die Dateiübertragung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>HTTP</i> (Standardwert) • <i>HTTPS</i> • <i>TFTP</i>
CSV-Dateiformat	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Datei im CSV-Format übertragen werden soll.</p> <p>Das CSV-Format kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Dateiname auf Server	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Für Aktion = <i>Konfiguration importieren</i></p> <p>Geben Sie den Namen der Datei ein, unter dem sie auf dem Server, von dem sie geholt werden soll, gespeichert ist.</p> <p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Geben Sie den Namen der Datei ein, unter dem sie auf dem Server gespeichert werden soll.</p>
Lokaler Dateiname	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i>, <i>Konfiguration umbenennen</i> oder <i>Konfiguration kopieren</i></p> <p>Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.</p>
Dateiname in Flash	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration exportieren</i></p>

Feld	Beschreibung
	<p>Wählen Sie die Datei aus, die exportiert werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration umbenennen</i></p> <p>Wählen Sie die Datei aus, die umbenannt werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration löschen</i></p> <p>Wählen Sie die Datei aus, die gelöscht werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration kopieren</i></p> <p>Wählen Sie die Datei aus, die kopiert werden soll.</p>
Konfiguration enthält Zertifikate/Schlüssel	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Konfiguration verschlüsseln	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Nach Ausführung neu starten	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, ob Ihr Gerät nach der gewünschten Aktion neu gestartet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Versionsprüfung	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i></p> <p>Wählen Sie aus, ob beim Import einer Konfigurationsdatei über-</p>

Feld	Beschreibung
	<p>prüft werden soll, ob auf dem Server eine aktuellere Version der schon geladenen Konfiguration vorhanden ist. Wenn nicht, wird der Datei-Import abgebrochen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Ziel-IP-Adresse	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
Quell-IP-Adresse	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Intervall	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Der Standardwert ist 1 Sekunde.</p>
Versuche	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll.</p> <p>Der Standardwert ist 3.</p>
Serveradresse	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.</p>
Lokale Zertifikatsbe-	<p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion =</p>

Feld	Beschreibung
Beschreibung	<p><i>Zertifikat importieren</i></p> <p>Geben Sie eine Beschreibung für das Zertifikat ein, unter der es im Gerät gespeichert werden soll.</p> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat löschen</i></p> <p>Wählen Sie das Zertifikat aus, das gelöscht werden soll.</p>
Kennwort für geschütztes Zertifikat	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie ein geschütztes Zertifikat verwenden möchten, das ein Passwort benötigt, und geben Sie dieses in das Eingabefeld ein.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Ähnliches Zertifikat überschreiben	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie ein auf Ihrem Gerät schon vorhandenes Zertifikat mit dem neuen überschreiben wollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikat in Konfiguration schreiben	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie das Zertifikat in eine Konfigurationsdatei einbinden wollen, und wählen Sie die gewünschte Konfigurationsdatei aus.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungsbeschreibung	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie eine Beschreibung ein, unter der das SCEP-Zertifikat auf Ihrem Gerät gespeichert werden soll.</p>
SCEP-Server-URL	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie die URL des SCEP-Servers ein, z. B.</p>

Feld	Beschreibung
	<p><code>http://scep.bintec-elmeg.com:8080/scep/scep.dll</code></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Subjektname	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</p> <p>Geben Sie einen Subjektnamen mit Attributen ein.</p> <p>Beispiel: "CN=VPNServer, DC=mydomain, DC=com, c=DE"</p>
CA-Name	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</p> <p>Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Passwort	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</p> <p>Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.</p>
Schlüsselgröße	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</p> <p>Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind <i>1024</i> (Standardwert), <i>2048</i> und <i>4096</i>.</p>
Autospeichermodus	<p>Nur bei Befehlstyp = Zertifikatverwaltung und Aktion = SCEP</p> <p>Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der</p>

Feld	Beschreibung
	<p>Konfiguration Ihres Geräts gespeichert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CRL verwenden	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatssperrlisten-Verteilungspunkt (CDP, CRL Distribution Point) vorhanden ist, soll dieser zusätzlich zu den global im Gerät konfigurierten Sperrlisten ausgewertet werden. • <i>Ja</i>: CRLs werden grundsätzlich überprüft. • <i>Nein</i>: Keine Überprüfung von CRLs.
WLAN-Modul auswählen	<p>Nur bei Befehlstyp = <i>5 GHz-WLAN-Bandscan, 5,8 GHz-WLAN-Bandscan</i> und <i>Betriebsmodus</i></p> <p>Wählen Sie das WLAN-Modul aus, auf dem ein Scan des Frequenzbands durchgeführt werden soll.</p>
WLC-SSID	<p>Nur bei Befehlstyp = <i>WLC: VSS-Status</i></p> <p>Wählen Sie das über den WLAN Controller verwaltete Drahtlosnetzwerk aus, dessen Status verändert werden soll.</p>
Betriebsmodus (Aktiv)	<p>Nur bei Befehlstyp = <i>Betriebsmodus</i></p> <p>Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand <i>Aktiv</i> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.</p>
Betriebsmodus (Inaktiv)	<p>Nur bei Befehlstyp = <i>Betriebsmodus</i></p> <p>Wählen Sie den gewünschten Betriebsmodus des gewählten Radiomoduls aus, wenn sich dieses aktuell im Zustand <i>Inaktiv</i></p>

Feld	Beschreibung
	<i>tiv</i> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.

16.6.3 Optionen

Im Menü **Lokale Dienste->Scheduling->Optionen** konfigurieren Sie das Schedule-Intervall.

Das Menü besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

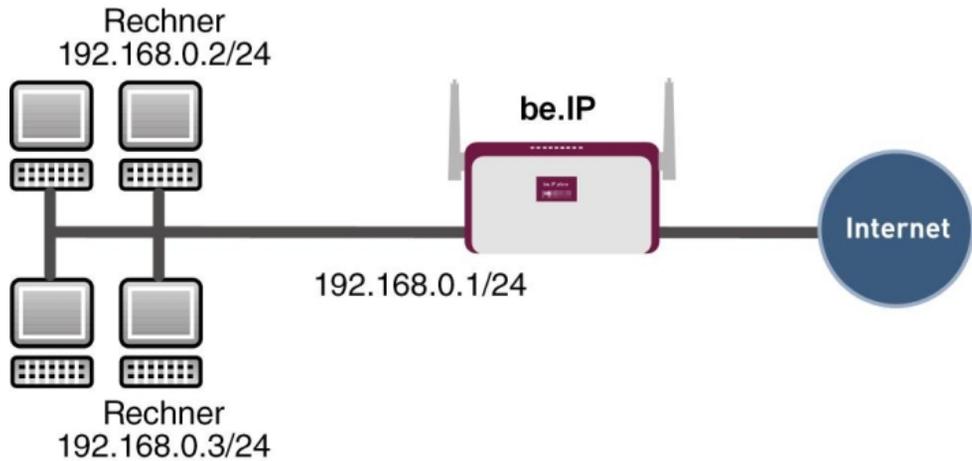
Feld	Beschreibung
Schedule-Intervall	<p>Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll.</p> <p>Standardmäßig ist das Schedule-Intervall nicht aktiv.</p> <p>Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind.</p> <p>Möglich sind Werte zwischen <i>0</i> und <i>65535</i>.</p> <p>Empfohlen wird der Wert <i>300</i> (5 Minuten Genauigkeit).</p>

16.6.4 Konfigurationsbeispiel - Zeitgesteuerte Aufgaben (Scheduling)

Voraussetzungen

- Grundkonfiguration des Gateways

Beispielszenario



Beispielszenario Zeitgesteuerte Aufgaben

Konfigurationsziel

- Das Gateway soll täglich während der Nacht neu starten.
- Am Wochenende soll die WLAN-Schnittstelle abgeschaltet werden.
- Einmal im Monat soll die Konfiguration automatisch auf einen TFTP-Server gesichert werden.

Konfigurationsschritte im Überblick

Täglicher Neustart

Feld	Menü	Wert
Ereignisliste	Lokale Dienste->Scheduling->Auslöser->Neu	Neu
Beschreibung	Lokale Dienste->Scheduling->Auslöser->Neu	z. B. Neustart auslösen
Ereignistyp	Lokale Dienste->Scheduling->Auslöser->Neu	Zeit
Zeitbedingung	Lokale Dienste->Scheduling->Auslöser->Neu	Bedingungstyp = Perioden, Bedingungs-einstellungen = Täglich
Startzeit	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde 02 Minute 00
Beschreibung	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. Neustart des Geräts

Feld	Menü	Wert
Befehlstyp	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Neustart</i>
Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Neustart auslösen</i>
Bedingung für Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Alle</i>
Neustart des Geräts nach	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>60 Sekunden</i>
Schedule-Intervall	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

WLAN-Schnittstelle abschalten

Feld	Menü	Wert
Ereignisliste	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Neu</i>
Beschreibung	Lokale Dienste->Scheduling->Auslöser->Neu	z. B. <i>WLAN-Schnittstelle abschalten auslösen</i>
Ereignistyp	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Zeit</i>
Zeitbedingung	Lokale Dienste->Scheduling->Auslöser->Neu	Bedingungstyp = <i>Perioden</i> , Bedingungseinstellungen = <i>Samstag Sonntag</i>
Startzeit	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde <i>00</i> Minute <i>00</i>
Stopzeit	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde <i>23</i> Minute <i>59</i>
Beschreibung	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>WLAN-Schnittstelle abschalten</i>
Befehlstyp	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Schnittstellenstatus</i>
Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>WLAN-Schnittstelle abschalten auslösen</i>
Bedingung für Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Alle</i>

Feld	Menü	Wert
Schnittstelle	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>vss1-0</i>
Schnittstellenstatus festlegen	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Inaktiv</i>
Schedule-Intervall	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

Konfiguration monatlich sichern

Feld	Menü	Wert
Ereignisliste	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Neu</i>
Beschreibung	Lokale Dienste->Scheduling->Auslöser->Neu	z. B. <i>Konfigurationssicherung auslösen</i>
Ereignistyp	Lokale Dienste->Scheduling->Auslöser->Neu	<i>Zeit</i>
Zeitbedingung	Lokale Dienste->Scheduling->Auslöser->Neu	Bedingungstyp = <i>Tag des Monats</i> , Bedingungseinstellungen = <i>1</i>
Startzeit	Lokale Dienste->Scheduling->Auslöser->Neu	Stunde <i>03</i> Minute <i>00</i>
Beschreibung	Lokale Dienste->Scheduling->Aktionen->Neu	Konfiguration sichern
Befehlstyp	Lokale Dienste->Scheduling->Aktionen->Neu	Konfigurationsmanagement
Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	Konfigurationssicherung auslösen
Bedingung für Ereignisliste	Lokale Dienste->Scheduling->Aktionen->Neu	Alle
Aktion	Lokale Dienste->Scheduling->Aktionen->Neu	Konfiguration exportieren
Server-URL	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>tftp://192.168.2.5</i>
CSV-Dateiformat	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Aktiviert</i>
Dateiname auf Server	Lokale Dienste->Scheduling->Aktionen->Neu	z. B. <i>monthly-backup.cf</i>

Feld	Menü	Wert
Dateiname in Flash	Lokale Dienste->Scheduling->Aktionen->Neu	<i>boot</i>
Konfiguration enthält Zertifikate/Schlüssel	Lokale Dienste->Scheduling->Aktionen->Neu	<i>Aktiviert</i>
Schedule-Intervall	Lokale Dienste->Scheduling->Optionen	<i>Aktiviert, 55 sec</i>

16.7 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Bei Geräten der **bintec WI**-Serie können Sie die Temperatur überwachen lassen.



Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

16.7.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

16.7.1.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Überwachung->Hosts->Neu** besteht aus folgenden Feldern:

Feld im Menü Hostparameter

Feld	Beschreibung
Gruppen-ID	<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 <i>0</i> bis <i>255</i> angelegt. Ist noch kein Eintrag angelegt, wird durch die Option <i>Neue</i></p>

Feld	Beschreibung
	<p>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 Schnittstelle 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
Überwachte IP-Adresse	<p>Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard-Gateway</i> (Standardwert): Das Standard-Gateway wird überwacht. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse des zu überwachenden Hosts ein.
Quell-IP-Adresse	<p>Wählen Sie aus, wie die IP-Adresse ermittelt werden soll, die Ihr Gerät als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse ein.
Intervall	<p>Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 10.</p> <p>Innerhalb einer Gruppe wird das kleinste Intervall der Gruppenmitglieder verwendet.</p>

Feld	Beschreibung
Erfolgreiche Versuche	<p>Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 3.</p>
Fehlgeschlagene Versuche	<p>Geben Sie ein, wieviele Pings unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als nicht erreichbar gilt und stattdessen ein Backup-Gerät verwendet wird.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 3.</p>
Auszuführende Aktion	<p>Nicht für Aktion = Überwachen.</p> <p>Wählen Sie aus, welche Aktion ausgeführt werden soll, wenn der Host als unzugänglich angesehen wird. Für die meisten Aktionen wählen Sie eine Schnittstelle, auf die sich die Aktion 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> <p>Die Aktionen <i>Aktivieren</i> und <i>Deaktivieren</i> werden ebenfalls abgebrochen, wenn die Hosts wieder als zugänglich angesehen werden.</p> <p>Mit Aktion = Überwachen können Sie die IP-Adresse überwachen, die unter Überwachte IP-Adresse angegeben ist. Diese Information kann für andere Funktionen genutzt werden, z. B. für die IP-Adresse zur Nachverfolgung, die beim IP-Lastverteilung verwendet wird.</p>

16.7.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

16.7.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Das Menü **Lokale Dienste->Überwachung->Schnittstellen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
Trigger	Wählen Sie den Status bzw. Statusübergang von Überwachte Schnittstelle aus, der eine bestimmte Schnittstellenaktion auslösen soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Schnittstelle wird aktiviert.</i> (Standardwert) • <i>Schnittstelle wird deaktiviert.</i>
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in Trigger definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in Schnittstelle ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert): Aktivierung der Schnittstelle(n) • <i>Deaktivieren</i>: Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter Schnittstelle festgelegte Aktion ausgeführt werden soll. Wählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle</i>

Feld	Beschreibung
	<i>IPSec-Schnittstellen.</i>

16.7.3 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

16.7.3.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Überwachung->Ping-Generator->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein. Mögliche Werte: <ul style="list-style-type: none"> • <i>Automatisch</i>: Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i> (Standardwert): Geben Sie die IP-Adresse in das nebenstehende Eingabefeld ein, z. B. um eine bestimmte erweiterte Route zu testen.
Intervall	Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in Entfernte IP-Adresse angegebene Adresse abgesetzt werden soll. Mögliche Werte sind 1 bis 65536. Der Standardwert ist 10.
Versuche	Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden sollen. Der Standardwert ist 3.

16.8 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 automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein bintec elmeg Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung**->**Remote Authentifizierung** ->**RADIUS**->**Neu** mit **Gruppenbeschreibung** *Standardgruppe 0*)
- bintec elmeg Hotspot Hosting (Artikelnummer 5510000198 bzw. 5510000197)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

- Gehen Sie auf www.bintec-elmeg.com zu **Service/Support** -> **Services** -> **Online Services**.

- Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

- Sie erhalten daraufhin die Login-Daten des Hotspot Servers.



Hinweis

Die Freischaltung kann etwa 2-3 Werktage in Anspruch nehmen.

Zugangsdaten zur Konfiguration des Gateways

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Wird von bintec elmeg GmbH festgelegt
Domain	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Network	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Server URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Terms & Condition URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt

Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Wird durch bintec elmeg individuell festgelegt

Password

Wird durch bintec elmeg individuell festgelegt

**Hinweis**

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf www.bintec-elmeg.com zum Download zur Verfügung steht.

16.8.1 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.

16.8.1.1 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
Schnittstelle	Wählen Sie die Schnittstelle aus, an der das Hotspot LAN oder WLAN angeschlossen ist. Bei Betrieb über LAN tragen Sie hier die Ethernet-Schnittstelle ein (z. B. die en1-0). Bei Betrieb über WLAN muss die WLAN-Schnittstelle ausgewählt werden, an der der Access Point angeschlossen ist.

**Achtung**

Die Konfiguration Ihres Gerätes ist aus Sicherheitsgründen nicht über eine Schnittstelle möglich, die für den Hotspot konfiguriert ist. Wählen Sie hier daher sorgfältig die Schnittstelle aus, die Sie für den Hotspot nutzen wollen!

Feld	Beschreibung
	<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>
Domäne am Hotspot-Server	<p>Geben Sie den Domännennamen ein, der bei der Einrichtung des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.</p>
Walled Garden	<p>Aktivieren Sie diese Funktion, wenn Sie einen abgegrenzten und kostenfreien Bereich von Webseiten (Intranet) definieren wollen.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>
Walled Network / Netzmaske	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Geben Sie die Netzadresse des Walled Network und die entsprechende Netzmaske des Intranet-Servers ein.</p> <p>Für den aus Walled Network / Netzmaske resultierenden Adressraum benötigen die Clients keine Authentifizierung.</p> <p>Beispiel: Geben Sie 192.168.0.0 / 255.255.255.0 ein, sind alle IP-Adressen von 192.168.0.0 bis 19.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IP-Adresse 192.168.0.1 frei.</p>
Walled Garden URL	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Geben Sie die Walled Garden URL des Intranet-Servers ein. Frei zugängliche Webseiten müssen über diese Adresse erreichbar sein.</p>
Geschäftsbedingungen	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Tragen Sie in das Eingabefeld Geschäftsbedingungen die Adresse der AGB's auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. http://www.webserver.de/agb.htm. Die Seite muss im Adressraum des Walled Garden-Networks liegen.</p>

Feld	Beschreibung
Zusätzliche, frei zugängliche Domännennamen	Nur wenn Walled Garden aktiviert ist. Fügen Sie mit Hinzufügen weitere URLs oder IP-Adressen hinzu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.
Aufzurufende Seite nach Login	Hier können Sie eine URL angeben, zu der ein Benutzer umgeleitet wrd, wenn er sich bei der Hotspot-Lösung angemeldet hat.
Sprache für Anmeldefenster	Hier können Sie die Sprache für die Start/Login-Seite auswählen. Folgende Sprachen werden unterstützt: <i>English, Deutsch, Italiano, Français, Español, Português und Netherlands</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
Tickettyp	Wählen Sie den Tickettyp aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Voucher</i>: Nur der Benutzername muss eingegeben werden. Definieren Sie im Eingabefeld ein Standardpasswort. • <i>Benutzername/Passwort</i> (Standardwert): Benutzername und Passwort müssen eingegeben werden.
Zulässiger Hotspot-Client	Hier legen Sie fest, welche Art von Benutzern sich am Hotspot anmelden dürfen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Alle</i>: Alle Clients werden zugelassen. • <i>DHCP-Client</i>: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.
Geräte pro Ticket	Geben Sie die maximale Anzahl Geräte pro Ticket an.

Feld	Beschreibung
Anmeldefenster	<p>Aktivieren oder deaktivieren Sie das Anmeldefenster.</p> <p>Das Anmeldefenster auf der HTML-Startseite besteht aus zwei Frames.</p> <p>Wenn die Funktion aktiviert ist, wird auf der linken Seite das Anmelde-Formular angezeigt.</p> <p>Wenn die Funktion deaktiviert ist, wird nur die Webseite mit Informationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Pop-Up-Fenster für Statusanzeige	<p>Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Standard-Timeout bei Inaktivität	<p>Aktivieren oder deaktivieren Sie den Standard-Timeout bei Inaktivität Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Der Standardwert ist <i>600</i> Sekunden.</p>

16.8.2 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
Host für mehrere Standorte	<p>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.</p>

16.9 Wake-On-LAN

Mit der Funktion **Wake-On-LAN** können Sie ausgeschaltete Netzwerkgeräte über eine eingebaute Netzwerkkarte starten. Die Netzwerkkarte muss weiterhin mit Strom versorgt werden, auch wenn der Computer ausgeschaltet ist. Sie können die Bedingungen, die zum Versenden des sog. Magic Packets erfüllt sein müssen, über Filter und Regelketten definieren sowie diejenigen Schnittstellen auswählen, die auf die definierten Regelketten hin überwacht werden sollen. Die Konfiguration der Filter und Regelketten entspricht weitgehend der Konfiguration von Filtern und Regelketten im Menü **Zugriffsregeln**.

16.9.1 Wake-on-LAN-Filter

Im Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter** wird eine Liste aller konfigurierten WOL-Filter angezeigt.

16.9.1.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Wake-On-LAN->Wake-on-LAN-Filter ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i>

Feld	Beschreibung
	Der Standardwert ist <i>any</i> .
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Wählen Sie einen Typ aus.</p> <p>Mögliche Werte: <i>Beliebig, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply</i>.</p> <p>Siehe RFC 792.</p> <p>Der Standardwert ist <i>Beliebig</i>.</p>
Verbindungsstatus	<p>Bei Protokoll = <i>TCP</i> können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.
IPv4-Zieladresse/-netzmaske	<p>Geben Sie die IPv4 Ziel-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert): Die Ziel-IP-Adresse/Netzmaske sind nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Ziel-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Ziel-Netzwerk-Adresse und die zugehörige Netzmaske ein.
IPv6-Zieladresse/-länge	<p>Geben Sie die IPv6 Ziel-Adresse der Datenpakete und die Präfixlänge ein.</p> <p>Mögliche Werte:</p>

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

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

16.9.2 WOL-Regeln

Im Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln** wird eine Liste aller konfigurierbaren WOL-Regeln angezeigt.

16.9.2.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Wake-On-LAN->WOL-Regeln->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Wake-On-LAN-Regelkette	<p>Wählen Sie aus, ob Sie eine neue Regelkette anlegen oder eine bestehende bearbeiten wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie eine neue Regelkette an. <i><Name der Regelkette></i>: Zeigt eine bereits angelegte Regelkette, die Sie auswählen und bearbeiten können.
Beschreibung	<p>Nur für Wake-On-LAN-Regelkette = <i>Neu</i></p> <p>Geben Sie die Bezeichnung der Regelkette ein.</p>
Wake-on-LAN-Filter	<p>Wählen Sie ein WOL-Filter aus.</p> <p>Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll.</p> <p>Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll.</p> <p>Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü Lokale Dienste->Wake-On-LAN->WOL-Regeln konfiguriert sein.</p>
Aktion	<p>Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WOL aufrufen, wenn Filter zutrifft</i>: WOL ausführen, wenn der Filter zutrifft. • <i>Aufrufen, wenn Filter nicht zutrifft</i>: WOL ausführen, wenn der Filter nicht zutrifft. • <i>WOL verweigern, wenn Filter zutrifft</i>: WOL nicht ausführen, wenn der Filter zutrifft. • <i>WOL verweigern, wenn Filter nicht zutrifft</i>: WOL nicht ausführen, wenn der Filter nicht zutrifft. • <i>Regel ignorieren und zu nächster Regel springen</i>: Diese Regel wird ignoriert und die in der Kette folgende wird überprüft.
Typ	Wählen Sie aus, ob das Wake on LAN Magic Packet als UDP-Paket oder als Ethernet Frame über die Schnittstelle gesendet werden soll, die in Sende WOL-Paket über Schnittstelle festgelegt wird.
Sende WOL-Paket über Schnittstelle	Wählen Sie die Schnittstelle aus, über die das Wake on LAN Magic Packet gesendet werden soll.
Ziel-MAC-Adresse	<p>Nur für Aktion = <i>WOL aufrufen, wenn Filter zutrifft</i> und <i>Aufrufen, wenn Filter nicht zutrifft</i></p> <p>Geben Sie die MAC-Adresse desjenigen Netzwerkgerätes ein, das mittels WOL aktiviert werden soll.</p>
Passwort	<p>Nur für Aktion = <i>WOL aufrufen, wenn Filter zutrifft</i> und <i>Aufrufen, wenn Filter nicht zutrifft</i></p> <p>Wenn das Netzwerkgerät, das aktiviert werden soll, die Funktion "SecureOn" unterstützt, geben Sie hier das entsprechende Passwort dieses Gerätes ein. Nur wenn MAC-Adresse und Passwort korrekt sind, wird das Gerät aktiviert.</p>

16.9.3 Schnittstellenzuweisung

In diesem Menü werden die konfigurierten Regelketten einzelnen Schnittstellen zugeordnet, die auf diese Regelketten hin überwacht werden.

Im Menü **Lokale Dienste->Wake-On-LAN->Schnittstellenzuweisung** wird eine Liste aller konfigurierten Schnittstellenzuordnungen angezeigt.

16.9.3.1 Bearbeiten oder Neu

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

Das Menü **Lokale Dienste->Wake-On-LAN->Schnittstellenzuweisung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.

16.10 Trace

16.10.1 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
Schnittstellenauswahl	Wählen Sie die Schnittstelle aus, deren Datenverkehr Sie aufzeichnen wollen.
Trace-Modus	Hier können Sie auswählen, auf welchen Ebenen der Datenverkehr der ausgewählten Schnittstelle aufgezeichnet werden soll. Zur Auswahl stehen: <ul style="list-style-type: none"> • <i>Layer 2</i> • <i>PPP</i> • <i>Layer 3</i> • <i>IP</i>

Sobald Sie die Aufzeichnung mit der Schaltfläche **START** beginnen, wird ein Fenster ange-

zeigt, dass 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.

16.10.2 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.

Kapitel 17 Wartung

Im diesem Menü werden Ihnen zahlreiche Funktionen zur Wartung Ihres Geräts zur Verfügung gestellt. So finden Sie zunächst eine Menü zum Testen der Erreichbarkeit innerhalb des Netzwerks. Sie haben die Möglichkeit Ihre Systemkonfigurationsdateien zu verwalten. Falls aktuellere Systemsoftware zur Verfügung steht, kann die Installation über dieses Menü vorgenommen werden. Falls Sie weitere Sprachen der Konfigurationsoberfläche benötigen, können Sie diese importieren. Auch ein System-Neustart kann in diesem Menü ausgelöst werden.

17.1 Benutzer ausloggen

Es kann vorkommen, dass durch eine nicht vollständig abgebaute Konfigurationssitzung Funktionen der Konfigurationsoberfläche beeinträchtigt werden. In diesem Fall können in diesem Menü alle noch bestehenden Verbindungen zum GUI eingesehen und ggf. beendet werden.

17.1.1 Benutzer ausloggen

In diesem Menü sehen Sie zunächst eine Auflistung aller aktiven Konfigurationsverbindungen.

Felder im Menü Benutzer ausloggen

Feld	Beschreibung
Klasse	Zeigt die Benutzerklasse an, der der angemeldete Benutzer angehört.
Benutzer	Zeigt den Benutzernamen an.
Entfernte IP-Adresse	Zeigt die IP-Adresse an, von der die Verbindung aufgebaut wurde. Die kann die Adresse eines PCs sein, aber auch die Adresse eines zwischengelagerten Routers.
Läuft ab	Zeigt an, wann die Verbindung automatisch getrennt wird.
Sofort ausloggen	Wenn sie das Kontrollkästchen aktivieren, wird dieser Benutzer mit einem Klick auf Ausloggen vom System abgemeldet.

17.1.1.1 Logout-Optionen

Nachdem Sie die Auswahl der zu beendenden Verbindungen mit Ausloggen bestätigt haben, können Sie wählen ob und welche Konfigurationen, die mit den entsprechenden Sitzungen zusammenhängen, vor dem Abmelden der Benutzer gespeichert werden.

17.2 Diagnose

Im Menü **Wartung**->**Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

17.2.1 Ping-Test

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind.

Felder im Menü Ping-Test

Feld	Beschreibung
Test-Ping-Modus	Wählen Sie die für den Ping-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none"> • <i>IPv4</i> • <i>IPv6</i>
Ping-Befehl testweise an Adresse senden	Geben Sie die zu testende IP-Adresse ein.
Zu verwendende Schnittstelle	Nur für Test-Ping-Modus = <i>IPv6</i> Wählen Sie für Link-Lokale-Adressen die Schnittstelle, die für den Ping-Test verwendet werden soll. Für globale Adressen kann <i>Standard</i> verwendet werden.

Durch Anklicken der **Los**-Schaltfläche wird der Ping-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an.

17.2.2 DNS-Test

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domännennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

17.2.3 Traceroute-Test

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese erreichbar ist.

Felder im Menü Traceroute-Test

Feld	Beschreibung
Traceroute-Modus	Wählen Sie die für den Traceroute-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none"> • IPv4 • IPv6
Traceroute-Adresse	Geben Sie die zu testende IP-Adresse ein.

Durch Anklicken der **Los**-Schaltfläche wird der Traceroute-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an.

17.3 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

17.3.1 Optionen

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Daher müssen Sie gegebenenfalls ein Software-Update durchführen.

Jede neue Systemsoftware beinhaltet neue Funktionen, bessere Leistung und bei Bedarf Fehlerkorrekturen der vorhergehenden Version. Die aktuelle Systemsoftware finden Sie unter www.bintec-elmeg.com. Hier finden Sie auch aktuelle Dokumentationen.



Wichtig

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörigen Release Notes. Hier sind alle Änderungen beschrieben, die mit der neuen Systemsoftware eingeführt werden.

Die Folge von unterbrochenen Update-Vorgängen (z. B. Stromausfall während des

Updates) könnte sein, dass Ihr Gerät nicht mehr bootet. Schalten Sie Ihr Gerät nicht aus, während die Aktualisierung durchgeführt wird.

In seltenen Fällen ist zusätzlich eine Aktualisierung von BOOTmonitor und/oder Logic empfohlen. In diesem Fall wird ausdrücklich in den entsprechenden Release Notes darauf hingewiesen. Führen Sie bei BOOTmonitor oder Logic nur ein Update durch, wenn bintec elmeg GmbH eine explizite Empfehlung dazu ausspricht.

Flash

Ihr Gerät speichert seine Konfiguration in Konfigurationsdateien im Flash EEPROM (electrically erasable programmable read-only memory). Auch wenn Ihr Gerät ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

RAM

Im Arbeitsspeicher (RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf Ihrem Gerät einstellen. Der Inhalt des RAM geht verloren, wenn Ihr Gerät ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start Ihres Geräts beibehalten wollen, müssen Sie die geänderte Konfiguration im Flash speichern: Schaltfläche **Konfiguration speichern** über dem Navigationsbereich des **GUIs**. Dadurch wird die Konfiguration in eine Datei mit dem Namen *boot* im Flash gespeichert. Beim Starten Ihres Geräts wird standardmäßig die Konfigurationsdatei *boot* verwendet.

Aktionen

Die Dateien im Flash-Speicher können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen Ihrem Gerät und einem Host per HTTP zu transferieren.

Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann 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
BOSS	Zeigt die aktuelle Softwareversion an, die auf Ihrem Gerät geladen ist.
Systemlogik	Zeigt die aktuelle Systemlogik an, die auf Ihrem Gerät geladen ist.
xDSL-Logik	Zeigt die aktuelle Version der xDSL-Logik an, die auf Ihrem Gerät geladen ist.

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	<p>Wählen Sie die Aktion aus, die Sie ausführen möchten.</p> <p>Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine Aktion</i> (Standardwert): • <i>Konfiguration exportieren</i>: Die Konfigurationsdatei Aktueller Dateiname im Flash wird zu Ihrem lokalen Host transferiert. Wenn Sie die Los-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Konfiguration importieren</i>: Wählen Sie in Dateiname eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken auf Los wird die Datei zunächst unter dem Namen <i>boot</i> in den Flash-Speicher des Geräts geladen. Zum Aktivieren müssen Sie das Gerät neu starten. Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben! • <i>Konfiguration kopieren</i>: Die Konfigurationsdatei im Feld Name der Quelldatei wird als Name der Zieldatei gespeichert. • <i>Konfiguration löschen</i>: Die Konfiguration im Feld Datei auswählen wird gelöscht. • <i>Konfiguration umbenennen</i>: Die Konfigurationsdatei im Feld Datei auswählen wird zu Neuer Dateiname umbenannt. • <i>Konfigurationssicherung wiederherstellen</i>: Nur, wenn unter Konfiguration speichern mit der Einstellung <i>Konfiguration speichern und vorhergehende Boot-Konfiguration sichern</i> die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen. • <i>Software/Firmware löschen</i>: Die Datei im Feld Datei auswählen wird gelöscht. • <i>Sprache importieren</i>: Sie können weitere Sprachversionen des GUI auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von www.bintec-elmeg.com auf Ihren PC herunterladen und von dort aus in Ihr Gerät einspielen. • <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware, der DSL-Logik und des BOOTmonitors initiieren. • <i>Konfiguration mit Statusinformationen exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die Los-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. <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"> • <i>Voice Mail Wave-Dateien importieren</i> (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist, sofern von Ihrem Gerät unterstützt): Wählen Sie in Dateiname die Datei <i>vms_wavfiles.zip</i> aus, die Sie importieren wollen. • <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 Dateiname die Datei aus, die Sie laden möchten. • <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!
Aktueller Dateiname im Flash	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.</p>
Zertifikate und Schlüssel einschließen	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Verschlüsselung der Konfiguration	<p>Nur für Aktion = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Passwort eingeben.</p>

Feld	Beschreibung
Dateiname	<p>Nur für Aktion = <i>Konfiguration importieren, Sprache importieren, Systemsoftware aktualisieren</i></p> <p>Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.</p>
Name der Quelldatei	<p>Nur für Aktion = <i>Konfiguration kopieren</i></p> <p>Wählen Sie die Quelldatei aus, die kopiert werden soll.</p>
Name der Zieldatei	<p>Nur für Aktion = <i>Konfiguration kopieren</i></p> <p>Geben Sie den Namen der Kopie ein.</p>
Datei auswählen	<p>Nur für Aktion = <i>Konfiguration löschen, Konfiguration umbenennen</i> oder <i>Software/Firmware löschen</i></p> <p>Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.</p>
Neuer Dateiname	<p>Nur für Aktion = <i>Konfiguration umbenennen</i></p> <p>Geben Sie den neuen Namen der Konfigurationsdatei ein.</p>
Quelle	<p>Nur für Aktion = <i>Systemsoftware aktualisieren</i></p> <p>Wählen Sie die Quelle der Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokale Datei</i> (Standardwert): Die Systemsoftware-Datei ist lokal auf Ihrem PC gespeichert. • <i>HTTP-Server</i>: Die Datei ist auf dem entfernten Server gespeichert, der in der URL angegeben wird. • <i>Aktuelle Software vom Update-Server</i>: Die Datei liegt auf dem offiziellen Update-Server.
URL	<p>Nur für Aktion = <i>Systemsoftware aktualisieren</i> und Quelle = <i>HTTP-Server</i></p> <p>Geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.</p>

Im Menü **Erweiterte Einstellungen** wird die Version der aktuell installierten internen Sys-

tem- Dateien angezeigt.

17.4 Neustart

17.4.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **GUI** neu aufrufen und sich wieder anmelden.

Beobachten Sie dazu die LEDs an Ihrem Gerät. Für die Bedeutung der LEDs lesen Sie bitte in dem Handbuch-Kapitel **Technische Daten**.



Hinweis

Stellen Sie vor einem Neustart sicher, dass Sie Ihre Konfigurationsänderungen durch Klicken auf die Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.

Wenn Sie Ihr Gerät neu starten wollen, klicken Sie auf die **OK**-Schaltfläche. Der Neustart wird ausgeführt.

17.5 Factory Reset

Im Menü **Wartung**->**Factory Reset** können Sie Ihr Gerät über das GUI in den Auslieferungszustand versetzen.

Kapitel 18 Externe Berichterstellung

In diesem Menü legen Sie fest, welche Systemprotokoll-Nachrichten auf welchem Rechner gespeichert werden und ob der Systemadministrator bei bestimmten Ereignissen eine Email erhalten soll. Informationen über den IP-Datenverkehr können - bezogen auf die einzelnen Schnittstellen - ebenfalls gespeichert werden. Darüber hinaus können im Fehlerfall SNMP-Traps an bestimmte Hosts versandt werden.

18.1 Systemprotokoll

Ereignisse in den verschiedenen Subsystemen Ihres Geräts (z. B. PPP) werden in Form von Systemprotokoll-Nachrichten (Syslog) protokolliert. Je nach eingestelltem Level (acht Stufen von *Notfall* über *Information* bis *Debug*) werden dabei mehr oder weniger Meldungen sichtbar.

Zusätzlich zu den intern auf Ihrem Gerät protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf Ihrem Gerät intern gespeicherte Systemprotokoll-Nachrichten gehen bei einem Neustart verloren.



Warnung

Achten Sie darauf, die Systemprotokoll-Nachrichten nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, dass jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

Syslog-Daemon

Die Erfassung der Systemprotokoll-Nachrichten wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (abrufbar im Download-Bereich unter www.bintec-elmeg.com).

18.1.1 Syslog-Server

Konfigurieren Sie Ihr Gerät als Syslog-Server, sodass die definierten Systemmeldungen an geeignete Hosts im LAN geschickt werden können.

In diesem Menü definieren Sie, welche Meldungen mit welchen Bedingungen zu welchem Host geschickt werden.

Im Menü **Externe Berichterstellung ->Systemprotokoll->Syslog-Server** wird eine Liste aller konfigurierten Systemprotokoll-Server angezeigt.

18.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.

Das Menü **Externe Berichterstellung ->Systemprotokoll ->Syslog-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	<p>Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Information</i> (Standardwert) • <i>Debug</i> (niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden an den Host gesendet, d. h. dass beim Syslog-Level <i>Debug</i> sämtliche erzeugten Meldungen an den Host weitergeleitet werden.</p>
Facility	<p>Geben Sie die Syslog Facility auf dem Host an.</p> <p>Dieses ist nur erforderlich, wenn der Log Host ein Unix-Rechner ist.</p> <p>Mögliche Werte: <i>local0</i> - 7 (Standardwert)</p>

Feld	Beschreibung
	<i>local0.</i>
Zeitstempel	<p>Wählen Sie das Format des Zeitstempels im Systemprotokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Keine Systemzeitangabe. • <i>Zeit</i>: Systemzeit ohne Datum. • <i>Datum & Uhrzeit</i>: Systemzeit mit Datum.
Protokoll	<p>Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>UDP</i> (Standardwert) • <i>TCP</i>
Nachrichtentyp	<p>Wählen Sie den Nachrichtentyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System & Accounting</i> (Standardwert) • <i>System</i> • <i>Accounting</i>

18.2 IP-Accounting

In modernen Netzwerken werden häufig aus kommerziellen Gründen Informationen über Art und Menge der Datenpakete gesammelt, die über die Netzwerkverbindungen übertragen und empfangen werden. Für Internet Service Provider, die ihre Kunden nach Datenvolumen abrechnen, ist das von entscheidender Bedeutung.

Aber auch nicht-kommerzielle Zwecke sprechen für ein detailliertes Netzwerk-Accounting. Wenn Sie z. B. einen Server verwalten, der verschiedene Arten von Netzwerkdiensten zur Verfügung stellt, ist es nützlich für Sie zu wissen, wieviel Daten von den einzelnen Diensten erzeugt werden.

Ihr Gerät enthält die Funktion IP-Accounting, die Ihnen die Sammlung vielerlei nützlicher Informationen über den IP-Netzwerkverkehr (jede einzelne IP-Session) ermöglicht.

18.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

Im Menü **Externe Berichterstellung -> IP-Accounting -> Schnittstellen** wird eine Liste aller auf Ihrem Gerät konfigurierten Schnittstellen angezeigt. Für jeden Eintrag kann durch Setzen eines Hakens die Funktion IP-Accounting aktiviert werden. In der Spalte **IP-Accounting** müssen Sie nicht jeden Eintrag einzeln anklicken. Über die Optionen **Alle auswählen** oder **Alle deaktivieren** können Sie die Funktion IP-Accounting für alle Schnittstellen gleichzeitig aktivieren bzw. deaktivieren.

18.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

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]
```

18.3 Benachrichtigungsdienst

Bisher war es schon möglich Syslog-Meldungen vom Router an einen beliebigen Syslog-Host übertragen zu lassen. Mit dem Benachrichtigungsdienst werden dem Administrator je nach Konfiguration E-Mails gesendet, sobald relevante Syslog-Meldungen auftreten.

18.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

18.3.1.1 Neu

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

Das Menü **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungsempfänger->Neu** besteht aus folgenden Feldern:

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungsdienst	<p>Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • E-Mail • SMS
Empfänger	Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des

Feld	Beschreibung
	Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Nachrichtenkompri- mierung	<p>Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse.</p> <p>Aktivieren oder deaktivieren Sie das Feld.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Betreff	Sie können einen Betreff eingeben.
Ereignis	<p>Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar.</p> <p>Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Systemmeldung enthält Zeichenfolge</i> (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. • <i>Neuer Neighbor-AP gefunden</i>: Ein neuer benachbarter AP wurde gefunden. • <i>Neuer Rogue-AP gefunden</i>: Ein neuer Rogue AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • <i>Neuer Slave-AP (WTP) gefunden</i>: Eine neuer unkonfiguriertes AP hat sich beim WLAN Controller gemeldet. • <i>Verwalteter AP offline</i>: Ein managed AP ist nicht mehr erreichbar.
Enthaltene Zeichenfolge	<p>Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms.</p> <p>Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "**") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Sys-</p>

Feld	Beschreibung
	log-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.
Schweregrad	<p>Wählen Sie den Schweregrad aus, auf dem der im Feld Enthaltene Zeichenfolge konfigurierte String vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird.</p> <p>Mögliche Werte:</p> <p><i>Notfall (Standardwert), Alarm, Kritisch, Fehler, Warnung, Benachrichtigung, Information, Debug</i></p>
Überwachte Subsysteme	<p>Wählen Sie die Subsysteme aus, die überwacht werden sollen.</p> <p>Fügen Sie mit Hinzufügen neue Subsysteme hinzu.</p>
Timeout für Nachrichten	<p>Geben Sie ein, wie lange der Router nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Benachrichtigungsmails erzwungen wird.</p> <p>Zur Verfügung stehen Werte von 0 bis 86400. Ein Wert von 0 deaktiviert den Timeout. Der Standardwert ist 60.</p>
Anzahl Nachrichten	<p>Geben Sie die Anzahl der Syslog-Meldungen ein, die erreicht sein muss, ehe eine Benachrichtigungsmail für diesen Fall gesendet werden kann. Wenn Timeout konfiguriert ist, wird die Mail bei dessen Ablauf gesendet, auch wenn die Anzahl an Meldungen noch nicht erreicht ist.</p> <p>Zur Verfügung stehen Werte von 0 bis 99, der Standardwert ist 1.</p>

18.3.2 Benachrichtigungseinstellungen

Das Menü **Externe Berichterstellung** -> **Benachrichtigungsdienst** -> **Benachrichtigungseinstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	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>
Maximale E-Mails pro Minute	<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
E-Mail-Adresse des Senders	Geben Sie die Mailadresse ein, die in das Absenderfeld der E-Mail eingetragen werden soll.
SMTP-Server	<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>
SMTP-Port	<p>Verschlüsselung von E-Mails (SSL/TLS).</p> <p>Das Feld SMTP-Port ist Standardmäßig auf <i>25</i> voreingestellt und SSL Encryption aktiviert.</p>
SMTP-Authentifizierung	<p>Authentifizierung, die der SMTP-Server erwartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung. • <i>ESMTP</i>: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt. • <i>SMTP after POP</i>: Der Server verlangt, dass vor dem Versenden einer Mail Mails per POP3 von der sendenden IP aus mit dem richtigen POP3-Benutzernamen/Passwort abgerufen werden.
Benutzername	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.</p>

Feld	Beschreibung
Passwort	Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i> Geben Sie das Passwort dieses Benutzers an.
POP3-Server	Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i> Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.
POP3-Timeout	Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i> Geben Sie ein, wie lange der Router nach dem POP3-Abruf maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird. Der Standardwert ist <i>600</i> Sekunden.

Felder im Menü SMS Parameter (nur für Geräte mit UMTS)

Feld	Beschreibung
SMS-Gerät	Sie können sich über Systemmeldungen per SMS informieren lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
Maximale SMS pro Tag	Begrenzen Sie hier die Anzahl der an einem Tag versendeten SMS. Die Aktivierung von <i>Uneingeschränkt</i> erlaubt eine beliebige Anzahl an versendeten SMS. Der Standardwert beträgt 10 SMS pro Tag. Hinweis: Die Eingabe des Wertes 0 ist gleichbedeutend mit der Aktivierung von <i>Uneingeschränkt</i> .

18.4 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

18.4.1 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
SNMP Trap Broadcasting	<p>Wählen Sie aus, ob die Übertragung von SNMP-Traps aktiviert werden soll.</p> <p>Ihr Gerät sendet SNMP-Traps dann an die Broadcast-Adresse des LANs.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
SNMP-Trap-UDP-Port	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p> <p>Geben Sie die Nummer des UDP-Ports ein, zu dem Ihr Gerät SNMP-Traps senden soll.</p> <p>Möglich ist jeder ganzzahlige Wert.</p> <p>Der Standardwert ist <i>162</i>.</p>
SNMP-	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p>

Feld	Beschreibung
Trap-Community	<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>

18.4.2 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.

18.4.2.1 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
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

18.5 SIA

18.5.1 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.

Kapitel 19 Monitoring

Dieses Menü enthält Informationen, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten, z. B. an der WAN-Schnittstelle Ihres Geräts, ermöglichen.

19.1 Internes Protokoll

19.1.1 Systemmeldungen

Im Menü **Monitoring->Internes Protokoll->Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die konfigurierten Werte der Felder **Maximale Anzahl der Syslog-Protokolleinträge** und **Maximales Nachrichtenlevel von Systemprotokolleinträgen**. Diese Werte können im Menü **Systemverwaltung->Globale Einstellungen->System** verändert werden.

Werte in der Liste Systemmeldungen

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der System-Meldung an.
Datum	Zeigt das Datum der Aufzeichnung an.
Zeit	Zeigt die Uhrzeit der Aufzeichnung an.
Level	Zeigt die hierarchische Einstufung der Meldung an.
Subsystem	Zeigt an, welches Subsystem Ihres Geräts die Meldung generiert hat.
Nachricht	Zeigt den Meldungstext an.

19.2 IPsec

19.2.1 IPsec-Tunnel

Im Menü **Monitoring->IPsec->IPsec-Tunnel** wird eine Liste aller konfigurierten IPsec-Tunnel angezeigt.

Werte in der Liste IPsec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPsec-Verbindung an.

Feld	Beschreibung
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

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

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

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Peers an.
Lokale IP-Adresse	Zeigt die WAN-IP-Adresse Ihres Geräts an.
Entfernte IP-Adresse	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
Lokale ID	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
Entfernte ID	Zeigt die ID des Peers an.
Aushandlungsmodus	Zeigt den Aushandlungsmodus an.
Authentifizierungsmethode	Zeigt die Authentifizierungsmethode an.
MTU	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
Erreichbarkeitsprüfung	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
NAT-Erkennung	Zeigt die NAT-Erkennungsmethode an.
Lokaler Port	Zeigt den lokalen Port an.
Entfernter Port	Zeigt den entfernten Port an.
Pakete	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
Bytes	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
Fehler	Zeigt die Anzahl der Fehler an.
IKE (Phase-1) SAs (x)	Zeigt die Parameter der IKE (Phase 1) SAs an.

Feld	Beschreibung
Rolle / Algorithmus / Verbleibende Lebensdauer / Status	
IPSec (Phase-2) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

19.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

Das Menü besteht aus folgenden Feldern:

Feld im Menü Lizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (In Verwendung) und die Anzahl der maximal verwendbaren Lizenzen (Maximal) an.

Feld im Menü Peers

Feld	Beschreibung
Status	<p>Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an.</p> <ul style="list-style-type: none"> • Aktiv: Aktuell aktive IPSec-Verbindungen. • Aktivieren: IPSec-Verbindungen, die sich aktuell in der Tunnelaufbau-Phase befinden. • Blockiert: IPSec-Verbindungen, die geblockt sind. • Ruhend: Aktuell inaktive IPSec-Verbindungen. • Konfiguriert: Konfigurierte IPSec-Verbindungen.

Felder im Menü SAs

Feld	Beschreibung
IKE (Phase-1)	Zeigt die Anzahl der aktiven Phase-1-SAs (Hergestellt) zur Gesamtzahl der Phase-1-SAs (Gesamt) an.
IPSec (Phase-2)	Zeigt die Anzahl der aktiven Phase-2-SAs (Hergestellt) zur Gesamtzahl der Phase-2-SAs (Gesamt) an.

Felder im Menü Paketstatistiken

Feld	Beschreibung
Gesamt	Zeigt die Anzahl aller verarbeiteten eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an.
Weitergeleitet	Zeigt die Anzahl der eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an, die im Klartext weitergeleitet wurden.
Verworfen	Zeigt die Anzahl der verworfenen eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an.
Verschlüsselt	Zeigt die Anzahl der durch IPSec geschützten eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an.
Fehler	Zeigt die Anzahl der eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an, bei deren Behandlung es zu Fehlern gekommen ist.

19.3 Schnittstellen

19.3.1 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
Nr.	Zeigt die laufende Nummer der Schnittstelle an.
Beschreibung	Zeigt den Namen der Schnittstelle an.

Feld	Beschreibung
Typ	Zeigt den Schnittstellentyp an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.
Rx-Fehler	Zeigt die Gesamtzahl der erhaltenen Fehler an.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Nicht geändert seit	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

Werte in der Liste Statistik

Feld	Beschreibung
Beschreibung	Zeigt den Namen der Schnittstelle an.
MAC-Adresse	Zeigt die MAC-Adresse an.
IP-Adresse/Netzmaske	Zeigt die IP-Adresse und die Netzmaske an.
NAT	Zeigt an, ob NAT für diese Schnittstelle aktiviert ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.

Feld im Menü TCP-Verbindungen

Feld	Beschreibung
Status	Zeigt den Status einer aktiven TCP-Verbindung an.
Lokale Adresse	Zeigt die lokale IP-Adresse der Schnittstelle für eine aktive TCP-Verbindung an.
Lokaler Port	Zeigt den lokalen Port der IP-Adresse für eine aktive TCP-Verbindung an.
Remote-Adresse	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.

Feld	Beschreibung
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

19.3.2 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.

19.4 WLAN

19.4.1 WLANx

Im Menü **Monitoring->WLAN->WLAN** werden die aktuellen Werte und Aktivitäten der WLAN-Schnittstelle angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

Werte in der Liste WLAN

Feld	Beschreibung
Mbit/s	Zeigt die möglichen Datenraten auf diesem Funkmodul an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete für die in Mbit/s angezeigte Datenrate an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete für die in Mbit/s angezeigte Datenrate an.

Über die Schaltfläche **Erweitert** gelangen Sie in eine Übersicht über weitere Details.

Werte in der Liste Erweitert

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des angezeigten Werts an.
Wert	Zeigt den entsprechenden statistischen Wert an.

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Unicast MSDUs erfolgreich übertragen	Zeigt die Anzahl der erfolgreich an Unicast-Adressen versandten MSDUs seit dem letzten Reset an. Zu jedem dieser Pakete wurde ein Acknowledgement empfangen.
Erfolgreich übertrage-	Zeigt die Anzahl der erfolgreich an Multicast-Adressen

Beschreibung	Bedeutung
ne Multicast-MSDUs	(inklusive der Broadcast MAC-Adresse) versandten MSDUs an.
Übertragene MPDUs	Zeigt die Anzahl der erfolgreich empfangenen MPDUs an.
Erfolgreich empfangene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Multicast-Adresse versandt wurden.
Unicast MPDUs erfolgreich erhalten	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Unicast-Adresse versandt wurden.
MSDUs, die nicht übertragen werden konnten	Zeigt die Anzahl der MSDUs an, die nicht gesendet werden konnten.
Frame-Übertragungen ohne ACK	Zeigt die Anzahl der gesendeten Frames an, für die kein Acknowledgement-Frame empfangen wurde.
Doppelte empfangene MSDUs	Zeigt die Anzahl von doppelt empfangenen MSDUs an.
CTS Frames als Antwort auf RTS empfangen	Zeigt die Anzahl der empfangenen CTS (Clear to send)-Frames an, die als Antwort auf RTS (Request to send) empfangen wurden.
Nicht entschlüsselbare MPDUs erhalten	Zeigt die Anzahl der empfangenen MPDUs an, die nicht entschlüsselt werden konnten. Ein Grund dafür könnte sein, dass kein passender Schlüssel eingetragen wurde.
RTS Frames ohne CTS	Zeigt die Anzahl der RTS-Frames an, für die kein CTS empfangen wurde.
Fehlerhafte Erhaltene Pakete	Zeigt die Anzahl der Frames an, die unvollständig oder fehlerhaft empfangen wurden.

19.4.2 VSS

Im Menü **Monitoring->WLAN->VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.

Werte in der Liste VSS

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1,	Zeigt die Empfangsstärke des Signals in dBm an.

Feld	Beschreibung
RSSI2, RSSI3)	
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	<p>Zeigt die aktuelle Übertragungsrates der von diesem Client empfangenen Daten in Mbit/s an.</p> <p>Folgende Übertragungsrates sind möglich: IEEE 802.11b: 11, 5,5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s.</p> <p>Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5,5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.</p>
Rx Discards	Zeigt die Anzahl der empfangenen Datenpakete, die verworfen wurden, wenn im Menü Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)->  im Feld Rx Shaping die Bandbreite für eingehenden Datenverkehr begrenzt wurde.
Tx Discards	Zeigt die Anzahl der gesendeten Datenpakete, die verworfen wurden, wenn im Menü Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)->  im Feld Rx Shaping die Bandbreite für ausgehenden Datenverkehr begrenzt wurde.

VSS - Details für Verbundene Clients

Im Menü **Monitoring->WLAN->VSS-><Verbundener Client>->**  werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

Werte in der Liste <Verbundener Client>

Feld	Beschreibung
Client-MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen Indikator für die Qualität der Verbindung im Funk dar.

Feld	Beschreibung
	Werte: <ul style="list-style-type: none"> • > 25 dB exzellent • 15 – 25 dB gut • 2 – 15 dB grenzwertig • 0 – 2 dB schlecht.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.
Rate	Zeigt die möglichen Datenraten auf dem Funkmodul an.
Tx-Pakete	Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.
Rx-Pakete	Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.

19.4.3 Client-Verwaltung

Im Menü **Monitoring->WLAN->Client-Verwaltung** wird eine Übersicht des **Client-Verwaltung** angezeigt. Sie sehen für jedes VSS u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die in vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

Werte in der Liste Client-Verwaltung

Feld	Beschreibung
VSS-Beschreibung	Zeigt die eindeutige Beschreibung des Drahtlosnetzwerks (VSS) an.
Netzwerkname (SSID)	Zeigt den Namen des Wireless Netzwerks (SSID) an.
MAC-Adresse	Zeigt die MAC Adresse, die für dieses VSS verwendet wird, an.
Aktive Clients	Zeigt die Anzahl der aktiven Clients.
2,4/5-GHz-Übergang	Zeigt die Anzahl der Clients, die über die Funktion 2,4/5-GHz-Übergang in ein anderes Frequenzband verschoben worden sind.
Abgewiesene Clients soft/hard	Zeigt die Anzahl der abgewiesenen Clients, nachdem die absolute Anzahl an zulässigen Clients erreicht wurde.

19.4.4 Bridge-Links

Im Menü **Monitoring->WLAN->Bridge-Links** werden die aktuellen Werte und Aktivitäten der Bridge-Links angezeigt.

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Tx Data Rate mbps	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link gesendeten Daten in Mbit/s an.
Rx Data Rate mbps	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Bridge-Link aktiv ist.

Bridge-Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Bridge-Links.

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Zuerst gesehen	Zeigt die Zeit des ersten registrierten Kontaktversuchs des Bridge-Link-Partners an.
Zuletzt gesehen	Zeigt die Zeit des letzten registrierten Kontaktversuchs des

Feld	Beschreibung
	Bridge-Link-Partners an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link gesendeten Daten in Mbit/s an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

19.4.5 Client Links

Im Menü **Monitoring->WLAN->Client Links** werden die aktuellen Werte und Aktivitäten der Client Links angezeigt.

Werte in der Liste Client Links

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des Client Links an.
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.

Client Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Client Links.

Werte in der Liste Client Links

Feld	Beschreibung
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Zeigt die Qualität des Signals in dB an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.

19.5 Bridges

19.5.1 br<x>

Im Menü **Monitoring->Bridges->br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

Werte in der Liste br<x>

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adressen der assoziierten Bridges an.
Port	Zeigt den Port an, auf dem die Bridge aktiv ist.

19.6 Hotspot-Gateway

19.6.1 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.
Anmeldung	Zeigt den Zeitpunkt der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

19.7 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

19.7.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

19.8 PIM

19.8.1 Allgemeine Statusangaben

Im Menü **Monitoring->PIM->Allgemeine Statusangaben** wird der Status aller konfigurierten PIM Komponenten angezeigt.

Werte in der Liste Allgemeine Statusangaben

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: <i>Alle, PIM-Schnittstellen, PIM-Nachbarn</i> und <i>Zuordnung Multicast-Gruppen zu RPs</i>

Werte in der Liste PIM-Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der PIM-Schnittstelle an.
IP-Adresse	Zeigt die primäre IP-Adresse der PIM-Schnittstelle an.
Designated Router (DR)	Zeigt die primäre IP-Adresse des Designated Routers auf dieser PIM-Schnittstelle an.

Werte in der Liste PIM-Nachbarn

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, über die der PIM Neighbor erreicht wird.
Generation ID	Zeigt die ID des Nachbar-Gateways an.
IP-Adresse	Zeigt die primäre IP-Adresse des PIM Neighbors an.
Uptime	Zeigt an, wie lange der letzte PIM Neighbor ein Nachbar des lokalen Routers ist.
Expiry Timer	Zeigt an, wann der PIM Neighbor nicht mehr als Nachbar eingetragen ist. Wird der Wert <i>0</i> angezeigt, bleibt der PIM Neighbor immer als Nachbar eingetragen.

Werte in der Liste Zuordnung Multicast-Gruppen zu RPs

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Präfixlänge der Multi-	Zeigt die dazugehörige Netzmaske an.

Feld	Beschreibung
cast-Gruppe	
IP-Adresse des Rendezvous Points	Zeigt die IP-Adresse des Rendezvous Points an.

19.8.2 Nicht-schnittstellen-spezifischer Status

Das Menü **Monitoring->PIM->Nicht-schnittstellen-spezifischer Status** enthält Status-Angaben für alle PIM-Schnittstellen.

Werte in der Liste Nicht-schnittstellen-spezifischer Status

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: <i>Alle, (*,*,RP) Status, (*,G) Status, (S,G) Status</i> und <i>(S,G,RPT) Status</i>

Werte in der Liste (*,*,RP) Status

Feld	Beschreibung
IP-Adresse des Rendezvous Point	Zeigt die IP-Adresse des Rendezvous Point (RP) der Gruppe an.
Upstream Join State	Der Upstream (*,*,RP) Join/Prune Status gibt den Status der Upstream (*,*,RP) State Machine in der PIM-SM Spezifikation wieder.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Upstream Neighbors, oder unknown(0), wenn die Upstream Neighbor IP-Adresse nicht bekannt ist oder es sich nicht um einen PIM Neighbor handelt.
Uptime	Zeigt den Zeitraum an, wie lange der RP besteht.
Upstream Join Timer	Der Join/Prune Timer wird verwendet, um periodisch Join(*,*,RP) Nachrichten zu senden, und um Prune(*,*,RP) Nachrichten von Peers auf einer Upstream LAN Schnittstelle zu korrigieren.

Werte in der Liste (*,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Upstream Nachbar-IP-Adresse	Zeit die primäre IP-Adresse des Neighbors auf pimStarGRPFI-Index an, zu der der lokale Router periodisch (*,G) Join Nach-

Feld	Beschreibung
	richten schickt. Der InetAddressType ist durch das Objekt pimStarGUpstreamNeighborType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF(*,G) genannt.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der Next Hop nicht bekannt ist.
Upstream Join State	Zeigt an, ob der lokale Router dem RP Tree der Gruppe beitreten soll. Dieses entspricht dem Status der Upstream (*,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (*,G) Join Nachricht auf pimStarGRPFIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Upstream Join Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimSGAddressType definiert.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Neighbors auf pimSGRPFIndex an, zu dem der Router periodisch (S,G) Join Nachrichten schickt. Der Wert ist 0, wenn der RPF Next Hop nicht bekannt oder kein PIM Neighbor ist. InetAddressType wird im Objekt pimSGAddressType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF'(S,G) genannt.
Upstream Join State	Zeigt an, ob der lokale Router den Shortest-Path-Tree für die Quelle und die Gruppe, die durch diesen Eintrag dargestellt wird, beitreten soll. Dieses entspricht dem Status der Upstream (S,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (S,G) Join Nachricht auf pimSGRPFIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Upstream Join Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

Feld	Beschreibung
Shortest Path Tree	Zeigt an, ob das Shortest Path Tree Bit gesetzt ist, d.h. ob das Forwarding über den Shortest Path Tree stattfinden soll.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der RPF Next Hop nicht bekannt ist.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Override Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste Triggered (S,G,rpt) Join Nachricht auf pimStarGRPFIIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Upstream Override Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

19.8.3 Schnittstellenspezifische Zustände

Das Menü **Monitoring->PIM->Schnittstellenspezifische Zustände** enthält schnittstellenspezifische Status-Angaben.

Werte in der Liste Schnittstellenspezifische Zustände

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: <i>Alle, (*,G,I) Status, (S,G,I) Status</i> und <i>(S,G,RPT) Status</i>

Werte in der Liste (*,G,I) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (*,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden.

Feld	Beschreibung
	Dieses entspricht dem Status der Downstream Per-Interface (*,G) State Machine in the PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (*,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Join Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFF'h steht für unendlich.
Assert-Status	Zeigt den (*,G) Assert State für diese Schnittstelle. Dieser entspricht dem Status der Per-Interface (*,G) Assert State Machine in der PIM-SM Spezifikation. Wenn pimStarGPimMode 'bidir' ist, muss dieses Objekt 'noInfo' lauten.
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner an, wenn pimStarGIAAssertState 'iAmAssertLoser' lautet. InetAddressType wird durch das Objekt pimStarGIAAssertWinnerAddressType definiert.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (S,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden. Dieser entspricht dem Status der Downstream Per-Interface (S,G) State Machine in der PIM-SM und PIM-DM Spezifikation.
Uptime	Zeigt die Zeit an, die verbleibt, bevor der lokale Router auf eine (S,G) Prune Nachricht reagiert, die auf dieser Schnittstelle empfangen wird. Der Router wartet diese Zeit, um zu prüfen, ob ein anderer Downstream Router die Prune Nachricht korrigiert. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Prune-Pending Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Join Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFF'h steht

Feld	Beschreibung
	für unendlich. Dieser Timer wird in der PIM-DM Spezifikation(S,G) Prune Timer genannt.
Assert-Status	Zeigt den (S,G) Assert State für diese Schnittstelle an. Dieser entspricht dem Status der Per-Interface (S,G) Assert State Machine in der PIM-SM Spezifikation Siehe "I-D.ietf-pim-sm-v2-new section 4.6.1"
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner, wenn pimSGIAssertState 'iAmAssertLoser' lautet. InetAddressType wird durch das Objekt pimSGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Join/Prune-Status	Zeigt an, ob der lokale Router die Quelle des RP Tree abschneiden soll. Dieses entspricht in der PIM-SM Spezifikation dem Status der Upstream (S,G,rpt) State Machine für Triggered Messages.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G,rpt) Prune State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Prune Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation(S,G) Prune Timer genannt.

Glossar

2G	Siehe GSM.
3DES	Siehe DES.
3G	Siehe UMTS.
4G	Siehe LTE.
802.11	Die Norm 802.11 beschreibt Wireless LAN (WLAN). Es existieren verschiedene Erweiterungen: 802.11a: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 5 GHz, 802.11b: Brutto-Datentransferrate: 11 Mbit/s, Frequenzband: 2,4 GHz, 802.11g: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 2,4 GHz, 802.11n: Brutto-Datentransferrate: 600 Mbit/s, Frequenzband: 2,4 GHz (optional: 5 GHz)
Access Client	Der Client Mode ist eine Betriebsart eines Wireless Access Points (AP), bei dem sich dieser gegenüber dem übergeordneten AP wie ein Wireless Adapter verhält. Mit einem im Client Mode betriebenen AP können einzelne Rechner oder ganze Subnetze an übergeordnete Netze angebunden werden.
Access Point	Ein Access Point (AP) ist ein Gerät zur drahtlosen Verbindung von Clients (Computern). Der AP dient somit zum Aufbau eines Funknetzwerks (WLAN) sowie der Verbindung dieses WLANs mit einem kabelgebundenen Ethernet-Netzwerk (Bridging).
Accounting	Beim Accounting werden Verbindungsdaten aufgezeichnet, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.
Activity Monitor	Mithilfe des Activity Monitors kann der Status physikalischer und virtueller Geräteschnittstellen überwacht werden.
Ad-Hoc-Netzwerk	In einem Ad-Hoc-Netzwerk verbinden sich einzelne Clients über einen Wireless Adapter zu einem unabhängiges Wireless LAN. Ad-Hoc-Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer-Basis. Der Ad-Hoc-Modus wird auch als IBSS-Modus (Independent Basic Service Set) bezeichnet und ist in kleinsten Netzen sinnvoll, z. B. bei der Vernetzung zweier Notebooks ohne Access Point.
ADSL	Asymmetric Digital Subscriber Line. Siehe DSL.

AES	Advanced Encryption Standard (AES, Rijndael) ist ein Verschlüsselungsverfahren (siehe Cipher). AES verwendet eine feste Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit. AES ist ein sehr schneller und sicherer Algorithmus.
Aggressive Mode	Beim Aufbau einer IPSec-Verbindung wird der Aggressive Mode zur Realisierung eines Phase-1-Austausches verwendet. Der Aggressive Mode bietet keinen Schutz der Identität für aushandelnde Knoten, da sie ihre Identitäten übertragen müssen, bevor sie einen sicheren Kanal aufbauen können. Siehe auch Main Mode.
AH	Der Authentication Header (AH) wird bei IPSec verwendet, um die Authentizität und Integrität der übertragenen Pakete sicherzustellen sowie den Sender zu authentisieren.
Anlagenanschluss	Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummerblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...) Siehe auch Mehrgeräteanschluss.
Anlagenanschluss-Rufnummer	Siehe Anlagenanschluss.
Annex A	Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.
Annex B	Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.
Annex J	Annex J ist eine DSL-Variante zur reinen Datenübertragung, ohne Sprachinformationen (entbundelter Anschluss). Annex J ist eine Ergänzung zur Spezifikation G.992. Diese DSL-Anschlüsse benötigen keinen Splitter und haben eine höhere Reichweite und eine schnellere Übertragungsgeschwindigkeit.
Annex L	Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrates vergrößert.
Annex M	Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.

ANSI T1.413	ANSI T1.413 ist eine ADSL-Variante.
ARP	Das Address Resolution Protocol (ARP) liefert zu IPv4-Adressen die zugehörigen MAC-Adressen. Die notwendigen Informationen werden zwischen den Netzwerkknoten ausgetauscht, im Cache des Geräts gespeichert und nach Ablauf der ARP Lifetime wieder gelöscht. Für IPv6 wird diese Funktionalität durch das Neighbor Discovery Protocol (NDP) bereitgestellt.
ATM	Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge kodiert und über asynchrones Zeitmultiplexing übertragen wird.
Authentifikation	Überprüfung der Identität des Nutzers (Authentisierung).
Autorisierung	Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
AUX	AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.
B-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.
Backbone Area	Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.
Basisanschluss	Der Basisanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Basic Rate Interface (BRI). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle) mit je 64 kbit/s und einen Steuerkanal (D-Kanal) mit 16 kbit/s. Für den Basisanschluss existieren zwei Betriebsarten: Anlagenanschluss und Mehrgeräteanschluss. Für größere Installationen wird der Primärmultiplexanschluss verwendet.
Beacon	Zum Aufbau eines Wireless LAN im Infrastruktur-Modus versendet der zentrale Access Point Beacons. Diese Mitteilungen enthalten den Netzwerknamen (SSID), eine Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung.
Bit	Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.
Black / White List	Einträge in der Black List werden blockiert, Einträge in der White List werden durchgelassen. (Beispiel: Alle Telefonnummern, die mit 01234 beginnen, werden in der Black List blockiert. Die Telefonnum-

mer 01234987 kann trotzdem in der White List freigegeben werden.)

Blowfish	Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.
BootP	Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Siehe Basisanschluss.
Bridge	Eine Bridge ist eine Netzwerkkomponente zum Verbinden gleichartiger Netze auf Schicht 2 des OSI-Modells. Datenpakete werden anhand von MAC-Adressen übertragen. Durch Bridges wird das Netzwerk aufgeteilt und entlastet.
Broadcast	Bei einem Broadcast werden Datenpakete von einem Punkt an alle Teilnehmer eines Netzes übertragen, z. B. falls der Empfänger noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP und DHCP. Die Kommunikation erfolgt über Broadcast-Adressen: MAC-Netzwerke: FF:FF:FF:FF:FF:FF, IPv4-Netzwerke: 255.255.255.255, IPv6-Netzwerke: ff00::/8
BRRP	BRRP ist eine Implementierung des Virtual Router Redundancy Protocol (VRRP). Ziel des Verfahrens ist es den Ausfall des Standardgateways zu kompensieren. Mehrere Router werden zu einem virtuellen Router zusammengefasst. Fällt einer dieser Router aus, können die Restlichen diesen ersetzen.
CA	Certificate Authority. Siehe Zertifikat.
Cache	Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.
Called Party's Number	Rufnummer des angerufenen Teilnehmers.
Calling Party's Number	Rufnummer des Anrufers.
CAPI	Das Common ISDN Application Programming Interface (CAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch TAPI.

CAPWAP	Das Control And Provisioning of Wireless Access Points Protocol (CAPWAP) dient zur Überwachung von Wireless Access Points (Slaves) durch einen WLAN-Controller (Master). Es verwendet die UDP-Ports 5246 zur Kontrolle und 5247 zur Datenübertragung.
CAST	CAST ist ein Verschlüsselungsverfahren (siehe Cipher). CAST verwendet eine fixe Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 40 und 128 Bit gewählt werden. Alternative Bezeichnungen sind CAST-128 oder CAST5.
CHAP	Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentifizierungsprotokoll für PPP-Verbindungen. Neben dem Standard-CHAP existieren noch die Varianten MS-CHAPv1 und MS-CHAPv2 der Firma Microsoft. Man wählt sich über PPP in ein Netzwerk ein und authentifiziert sich mit Benutzername und Passwort. Benutzername und Passwort werden verschlüsselt übertragen. Siehe auch PAP.
Cipher	Eine Blockchiffre (Block Cipher) ist ein Verschlüsselungsalgorithmus. In diesem Verschlüsselungsverfahren wird ein Datenblock mit fester Größe (normalerweise 64 Bit) mithilfe eines sogenannten Schlüssels zu einem Block derselben Größe umgeschrieben. Je länger der Schlüssel ist, umso sicherer ist der Algorithmus.
Client	Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.
CoS	Der Begriff Class of Service (CoS) hat je nach Anwendungsgebiet verschiedene Bedeutungen. In der Telekommunikation wird unter CoS die dem Benutzer zugewiesene Berechtigungsklasse verstanden. Die Berechtigungsklasse legt die Rechte des Benutzers fest, wie z. B. Amtsberechtigung, nutzbare Leistungsmerkmale, Zugriff auf Anwendungen, ... In der Netzwerktechnologie versteht man unter CoS die Klassifizierung bestimmter Dienste gemäß IEEE 802.1p. CoS ermöglicht eine gezielte Priorisierung, während mit Quality of Service (QoS) explizite Bandbreitengarantien oder -beschränkungen eingerichtet werden. Die Einteilung der Datenpakete erfolgt mittels eines DSCP-Werts (Differentiated Services Code Point).
CRC	Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.
CRL	Siehe Zertifikat.
D-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.

Daemon	Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.
Datagramm	Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.
Datenkompression	Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.
Dead Peer Detection	In IPsec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.
Default Gateway	An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.
Default Route	Siehe Standardroute.
Diffie-Hellman	Diffie-Hellman ist ein Public-Key-Algorithmus zur Aushandlung und Etablierung von Schlüsseln. Da Daten weder verschlüsselt noch signiert werden, ist das Verfahren nur sicher, falls sich die Verbindungspartner über andere Mechanismen, wie RSA oder DSA, authentifizieren.
Denial-Of-Service Attack	Bei einem Denial-of-Service-Angriff (DoS) wird eine Netzwerkkomponente mit Anfragen überflutet, sodass diese völlig überlastet wird. Das System oder ein bestimmter Dienst ist in Folge dessen nicht mehr funktionsfähig.
DES	Data Encryption Standard (DES) ist ein Verschlüsselungsverfahren (siehe Cipher). DES verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge beträgt 56 Bit. Triple-DES oder 3DES basiert auf der dreimaligen Anwendung von DES (drei verschiedene unabhängige Schlüssel).
DFÜ	DFÜ steht für Datenfernübertragung.
DHCP	Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die dynamische Zuweisung von IP-Adressen. Ein DHCP-Server vergibt an jeden Client im Netzwerk eine IP-Adresse aus einem definierten Adress-Pool. Die Clients müssen dazu entsprechend konfiguriert sein.
DIME	Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.
DNS	Mithilfe des Domain Name System (DNS) wird der Domänenname

(z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).

Domäne	Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).
Downstream	Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.
DSA	Mithilfe des Digital Signature Algorithm (DSA) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über Signaturen können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. DSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch RSA. DSA ist schneller in der Schlüsselerzeugung aber langsamer in der Schlüsselverarbeitung als RSA.
DSCP	Datenpakete können mit einem Differentiated Services Codepoint (DSCP) ausgezeichnet werden. DSCP-Werte teilen Datenpakete in Klassen ein, sodass wichtige Pakete schneller durch das Netzwerk geleitet werden können. Siehe auch QoS.
DSL-Modem	Siehe Modem.
DSS1	Digital Subscriber Signalling System No. 1 (DSS1) ist ein Signalisierungsprotokoll für den D-Kanal des ISDN. Es ist auch bekannt als Euro-ISDN.
DTIM	Eine Delivery Traffic Indication Message informiert die Clients über auf dem Access Point vorhandene Multicast- bzw. Broadcast-Daten.
Durchwahl (VoIP)	Beim Durchwahl-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer IP-TK-Anlage. Man erhält eine Basisrufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Basisrufnummer: 1234, Rufnummernblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...)
Durchwahlausnahme	Siehe Anlagenanschluss und Durchwahl (VoIP).
Durchwahlbereich	Siehe Rufnummernblock bei Anlagenanschluss und Durchwahl (VoIP).
Durchwahlnummer	Siehe Anlagenanschluss und Durchwahl (VoIP).

Dynamische IP-Adresse	Im Gegensatz zu einer statischen IP-Adresse wird die dynamische IP-Adresse temporär per DHCP zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
DynDNS	Mithilfe eines DynDNS-Providers kann ein Domänenname auch mit einer dynamisch wechselnden IP-Adresse verknüpft werden.
Einzelrufnummer (VoIP)	Beim Einzelrufnummer-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von VoIP-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Durchwahl (VoIP).
Encapsulation	Encapsulation (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.
Encryption	Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.
ESP	Encapsulating Security Payload (ESP) ist ein Protokoll für IPSec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.
Ethernet	Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.
Euro-ISDN	In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.
Eurofile-Transfer	EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.
Filter	Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Treffen diese Kriterien für ein Datenpaket zu, kann das Datenpaket einer bestimmten Aktion (weiterleiten, ablehnen, ...) unterworfen werden. Dadurch entsteht eine Filterregel.
Filterregel	Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.
Firmware	Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts

bereitgestellt.

Fragmentierung	Falls die Gesamtlänge des Datenpakets größer als die Maximum Transmission Unit (MTU) der Netzwerkschnittstelle ist, muss das Datenpaket durch IP-Fragmentierung auf mehrere physikalische Datenblöcke aufgeteilt werden. Der umgekehrte Prozess wird Reassembly genannt.
Frame	Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells
Frame Relay	Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.
FTP	Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.
Full-Duplex	Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.
G.991.1	Datenübertragungsempfehlung für HDSL.
G.991.2	Datenübertragungsempfehlung für SHDSL.
G.992.1	Datenübertragungsempfehlung für ADSL (G.DMT). Es existieren zwei länderspezifische Ausprägungen G.992.1 Annex A und G.992.1 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.2	Datenübertragungsempfehlung für ADSL (G.LITE / ADSL-Lite). Es existieren zwei Varianten G.992.2 Annex A und G.992.2 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.3	Datenübertragungsempfehlung für xDSL2. Es existieren drei Varianten: G.992.3 Annex A/B (G.DMT bis ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.3 Annex L (RE-ADSL2) mit Datenübertragungsraten von 5 Mbit/s im Downstream und 0,8 Mbit/s im Upstream und G.992.3 Annex M (ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 2,5 Mbit/s im Upstream.
G.992.4	Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)
G.992.5	Datenübertragungsempfehlung für xDSL2+. Es existieren drei Vari-

anten: G.992.5 Annex A/B (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.5 Annex L (RE-ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream und G.992.5 Annex M (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 3,5 Mbit/s im Upstream.

G.993.1	Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)
G.993.2	Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)
G.DMT	Siehe F.992.1.
G.Lite	Siehe F.992.2.
G.SHDSL	Siehe G.991.2.
Gateway	Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.
GPRS	General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.
GRE	Generic Routing Encapsulation (GRE) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. GRE verwendet die Protokollnummer 47.
GSM	Das Global System for Mobile Communications (GSM), auch als 2G bezeichnet, ist ein Mobilfunkstandard. Dieser erreicht zusammen mit GPRS eine spezifizierte max. Datenübertragungsrate von 171,2 kbit/s.
Half-Duplex	Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.
Hash	Zur Sicherstellung der Datenintegrität muss die Information vor unautorisierter Manipulation während der Übertragung geschützt werden. Um dies zu gewährleisten, muss jede empfangene Kommunikation mit der ursprünglich gesendeten Information übereinstimmen. Deshalb werden mathematische Streuwertfunktionen (Hashfunktionen) zur Berechnung von Prüfsummen (Hashwerten) verwendet. Diese werden verschlüsselt und mit der Nachricht als digitale Signatur versendet. Der Empfänger prüft wiederum die Signatur, bevor er das Paket öffnet. Falls sich die Signatur und damit der

Inhalt des Datenpakets geändert hat, wird das Paket verworfen. Die am häufigsten verwendeten Hash-Algorithmen sind Message Digest Version 5 (MD5) und Secure Hash Algorithm (SHA1).

HDSL	High Data Rate Digital Subscriber Line. Siehe DSL.
Heartbeat	Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.
Hop	Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.
Host	Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.
Host-Name	Domänenname eines Host. Siehe DNS.
Hostroute	Eine Hostroute bezeichnet die Route zu einem einzelnen Host.
Hotspot	Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.
HSDPA	High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.
HTTP	Das HyperText Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. Es verwendet standardmäßig den Port 80.
HTTPS	Das HyperText Transfer Protocol Secure (HTTPS) ist ein Protokoll zur abhörsicheren Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. HTTPS ist schematisch identisch zu HTTP. Für die zusätzliche Verschlüsselung der Daten wird SSL / TLS verwendet. Der Standard-Port für HTTPS-Verbindungen ist 443.
Hyperchannel	Beim Hyperchannel haben mehrere Teilnehmer Zugriff auf das Übertragungsmedium. Ein Teilnehmer kann seine Informationen nur übertragen, wenn kein anderer Teilnehmer das Medium belegt. Ein Hyperchannel-Netzwerk dient hauptsächlich für Kurzstreckenbetrieb mit höchsten Datenraten.
ICMP	Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.

IGMP	Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.
IKE	Das Internet-Key-Exchange-Protokoll (IKE) dient der automatischen Schlüsselverwaltung bei IPSec-Verbindungen. Der IKE-Prozess verläuft in zwei Phasen. Während Phase 1 authentifizieren sich die IKE-Teilnehmer gegenseitig und etablieren einen sicheren Kanal. In Phase 2 handeln die beiden IPSec-Teilnehmer die SAs aus. Es existieren zwei Versionen des IKE-Mechanismus.
Infrastruktur-Netzwerk	In einem Infrastruktur-Netz bilden die einzelnen Endgeräte (Clients) über einen zentralen Knotenpunkt (Access Point) ein Wireless LAN. Dieser zentrale Access Point kann dabei auch ein Vermittler in weitere Netze sein.
IP	Das Internet Protocol (IP) ist ein Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es arbeitet auf der Vermittlungsschicht des OSI-Modells. Auf IP bauen die Protokolle TCP und UDP auf. Es existieren zwei Versionen Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6).
IP-Adresse	IP-Adressen werden zur Navigation in einem IP-Netzwerk verwendet, um Quelle und Ziel eindeutig zu bestimmen. IPv4-Adressen bestehen aus 32 Bits, IPv6-Adressen aus 128 Bits. Damit sind bei IPv4 232, also 4.294.967.296 Adressen darstellbar, bei IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen. Für IPv4 wird die Dezimaldarstellung (dotted decimal notation) verwendet, z. B. 192.168.0.250. Für IPv6 wird die Hexadezimaldarstellung verwendet, z. B. 2001:db8:85a3::8a2e:370:7344. Siehe auch Netzmaske.
IPCP	Das Internet Protocol Control Protocol (IPCP) dient, analog zu DHCP, zur Konfiguration eines Host mit IP-Adresse, Gateway und DNS-Server, falls eine PPP-Netzwerkverbindung verwendet wird. Mithilfe der Erweiterung Robust Header Compression over PPP kann der Header für eine schnellere Datenübertragung komprimiert werden. Analog wird in IPv6-Netzwerken die Funktionalität durch das Internet-Protocol-Version-6-Control-Protokoll (IPv6CP) bereitgestellt.
IPSec	IPSec (Internet Protocol Security) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. Die Protokollnummer für IPSec ist dabei vom verwendeten Protokoll abhängig. Der Authentication-Header (AH) verwendet die Protokollnummer 51, das Encapsulating-Security-Payload (ESP) die Nummer 50.

IPv6	Siehe IP.
ISDN	Integrated Services Digital Network (ISDN) ist ein Datenübertragungsstandard, der Telefonie, Telefax und Datenübertragung umfasst. Es existieren zwei ISDN-Anschluss-Varianten: Basisanschluss und Primärmultiplexanschluss.
ISDN-Adresse	Die ISDN-Adresse eines ISDN-Geräts setzt sich zusammen aus einer ISDN-Nummer gefolgt von weiteren Ziffern, die sich auf das spezifische Endgerät beziehen.
ISDN-Login	Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.
ISDN-Nummer	Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.
ISDN-Router	Siehe Router.
ISP	Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.
ITU	Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.
Kanal	Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.
Kanalbündelung	Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.
Keepalive	Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.
Keepalive	Keepalive ist ein Mechanismus zur Aufrechterhaltung der Netzwerkverbindung und zur Überprüfung der Erreichbarkeit der Kommunikationspartner. Dazu werden in der Regel spezifische Pakete ins Netzwerk gesendet.
Konfiguration	Alle Einstellungen des Geräts werden als Konfiguration bezeichnet. Diese Konfiguration ist intern in MIB-Tabellen gespeichert. Diese Informationen können extern gespeichert, von extern geladen oder gelöscht werden. Bearbeitet wird die Konfiguration über die HTTP(S)-Benutzeroberfläche, einen SNMP-Client oder angeschlossene Telefone.

L2TP	Das Layer 2 Tunneling Protocol (L2TP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über verschiedene Protokolle zu transportieren. L2TP verwendet standardmäßig die Protokollnummer 1701. Die Architektur eines L2TP-Netzwerks besteht aus einem L2TP-Access-Concentrator (LAC), der auch fest in den Client integriert sein kann, und dem L2TP-Network-Server (LNS). Der LAC stellt die Verbindungen zum LNS her und verwaltet diese. Die Autorisierung wird über einen Network-Access-Server (NAS), der im LAC oder LNS implementiert sein kann, geregelt. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Die eigentlichen Nutzdaten werden unverschlüsselt ausgetauscht, während Kontrollnachrichten zur Aufrechterhaltung der Erreichbarkeit der Tunnelendpunkte abgesichert übertragen werden.
LAC	Siehe L2TP.
LAN	Ein Local Area Network (LAN) bezeichnet ein räumlich eng begrenztes Netzwerk und umspannt meist ein Gebäude oder einen Firmensitz.
Lastverteilung	Bei der Lastverteilung werden Daten über unterschiedliche Schnittstellen gesendet, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. Im Unterschied zu Multilink funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.
Layer	Ein Layer bezeichnet eine Schicht im OSI-Modell.
LCP	Das Link Control Protocol (LCP) wird in PPP-Verbindungen verwendet, um die Einkapsulierung automatisch auszuhandeln, Grenzen für variierende Paketgrößen zu verarbeiten, den Verbindungspartner zu authentifizieren, einen defekten Link zu bestimmen, Verbindungsfehler zu erkennen und die Verbindung zu beenden.
LDAP	Das Lightweight Directory Access Protocol (LDAP) regelt die Kommunikation zwischen einem Client und dem Directory-Server. LDAP wird für den Austausch und die Aktualisierung von Verzeichnissen, z. B. ein Telefonbuch, verwendet.
Lease Time	Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.
Leased Line	Siehe Standleitung.
LLC	Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.

LNS	Siehe L2TP.
Loopback	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
LTE	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
MAC-Adresse	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
Main Mode	Beim Aufbau einer IPSec-Verbindung wird der Main Mode zur Realisierung eines Phase-1-Austausches verwendet, indem ein sicherer Kanal eingerichtet wird. Siehe auch Aggressive Mode.
Man-in-the-Middle Attack	Im Man-in-the-middle-Angriff befindet sich der Angreifer physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kann somit den Datenverkehr einsehen und sogar manipulieren.
MD5	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Media Gateway	Ein Media Gateway wandelt den Netzwerktyp von digitalen Sprach-, Audio- oder Bildinformationen um. Beispielsweise können die Signale eines ISDN-Netzwerks auf ein IP-Netzwerk umgesetzt werden.
Mehrfachrufnummer (MSN)	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
Mehrgeräteanschluss	Beim Mehrgeräteanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von ISDN-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Anlagenanschluss.
Metrik	Die Metrik ist eine Maß für die Güte der Route. Die schnellste Route weist dabei die geringste Metrik (costs, »Kosten«) auf. Vereinfacht ist dies die Verbindung mit der kleinsten Anzahl an Knotenpunkten (Routern).
MIB	Die Management Information Base (MIB) beschreibt die Informationen, die über ein Netzwerk-Management-Protokoll (z. B. SNMP) abgefragt oder modifiziert werden können. Die MIB ist eine Datenbank, die alle Geräte und Funktionen im Netzwerk beschreibt.

MLP	Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.
Modem	Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.
MPDU	Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.
MPPC	Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.
MPPE	Microsoft Point-To-Point Encryption (MPPE) wird zur Verschlüsselung von Daten, die über PPP übertragen werden, eingesetzt. Es wurde von Microsoft und Cisco entwickelt und als RFC 3078 spezifiziert.
MS-CHAP	Das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) ist ein Authentisierungsverfahren. MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für PPTP-Verbindungen (VPN).
MSDU	Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.
MSN	Siehe Mehrfachrufnummer.
MSS	Die Maximum Segment Size (MSS) definiert die maximale Anzahl an Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Die MSS muss kleiner als die Maximum Transmission Unit (MTU) sein, um eine Fragmentierung der IP-Pakete zu vermeiden.
MSS Clamping	Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.
MTU	Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.
Multicast	Bei einem Multicast werden Datenpakete von einem Punkt an bestimmte Teilnehmer eines Netzes übertragen. In IPv4 wird dies über den Adress-Bereich 224.0.0.0 bis 239.255.255.255 und das Protokoll IGMP gesteuert, in IPv6 über ff00::/8-Adressen und ICMPv6.

Multilink	Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, ...) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.
NAPT	Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.
NAT	Mithilfe von Network Address Translation (NAT) werden die Quell- und Ziel-IP-Adressen eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch PAT.
NBNS	NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.
Netzabschluss	Der Netzabschluss (Network Termination, NT) bezeichnet einen Anschluss bzw. eine Betriebsart. Am NT-Anschluss (Anschlussdose) wird einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt. Beim analogen Anschluss wird die Steckdose TAE genannt, beim ISDN-Basisanschluss NTBA und beim ISDN-Primärmultiplexanschluss NTPMGF. Im NT-Betrieb wird das Gateway am externen S0 der Telefonanlage angeschlossen und stellt für diese einen externen Amtsanschluss dar. Siehe auch TE.
Netzmaske	Die Netzmaske, auch Netzwerkmaske oder Subnetzmaske, definiert bei IPv4 in Verbindung mit der IP-Adresse das Netzwerk, indem sie die IP-Adresse in einen Netzwerk- und einen Geräteanteil aufteilt und somit bestimmt, welche Adressen geroutet werden müssen. Beispiel einer Netzmaske: 255.255.255.0. Bei IPv6 spricht man von der Präfixlänge.
Netzwerkadresse	Eine Netzadresse (Präfix) bezeichnet die Adresse des gesamten Netzwerks. Die Netzwerkmaske bzw. Präfixlänge unterteilt die IP-Adresse in die Netzadresse und Host-Adresse (Geräteadresse). Beispiel für eine Netzadresse: 192.168.0.250/24
Netzwerkroute	Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.
NT	Siehe Netzabschluss.
NTP	Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.
OAM	OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.
OSI-Modell	Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen

physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.

OSPF	OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.
PAP	Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.
PAT	Mithilfe von Port and Address Translation (PAT) werden die Quell- und Ziel-IP-Adressen sowie die Quell- und Ziel-Ports eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch NAT.
Peer	Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.
Phase-1/2	Siehe IKE.
PIM	Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.
Ping	Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist. Daneben wird die Zeitspanne zwischen dem Aussenden eines Datenpakets (ICMP(v6)-Echo-Request-Paket) und dem Empfangen eines daraufhin unmittelbar zurückgeschickten Antwortpakets gemessen. Dadurch kann die Qualität der Verbindung ermittelt werden.
PKCS	Die Public-Key Cryptography Standards (PKCS) beinhalten Standards für Public-Key-Kryptografie. Die PKCS sind konzipiert für binäre und ASCII-Daten und sind kompatibel mit dem X.509-Standard. Die veröffentlichten Standards sind PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, und #15. PKCS #10 beschreibt die Syntax für Zertifizierungsanfragen.
PKI	Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.
PMTU	Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.
Point-to-Multipoint	Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).

Point-to-Point	Siehe Anlagenanschluss und Durchwahl (VoIP).
Pool	Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.
POP3	Das Post Office Protocol Version 3 (POP3) ist ein Übertragungsprotokoll, um den E-Mail-Abruf von einem E-Mail-Server durch einen Client zu steuern.
Port	Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, ...) ein ankommendes Datenpaket weitergeleitet wird.
PPP	Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.
PPPoA	Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.
PPPoE	Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.
PPTP	Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. PPTP verwendet die Protokollnummer 1723. Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP-Access-Concentrator (PAC) und den PPTP-Network-Server (PNS). Der PAC ist üblicherweise in den Windows Client integriert. Er stellt die Verbindung zum PNS her und verwaltet diese. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.
Präfix	Siehe Netzwerkadresse.
Präfixdelegation	In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.
Präfixlänge	Siehe Netzmaske.
Preshared Key	Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.
PRI	Siehe Primärmultiplexanschluss.

Primärmultiplexanschluss	Der Primärmultiplexanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Primary Rate Interface (PRI) oder S2M-Anschluss. Ein Primärmultiplexanschluss bietet in Europa 30 und in den USA 23 Nutzkanäle (B-Kanäle) mit je 64 kbit/s, einen Steuerkanal (D-Kanal) mit 64 kbit/s und einen Synchronisationskanal mit 64 kbit/s in Europa und 8 kbit/s in den USA. Siehe auch Basisanschluss.
Proposal	Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.
Protokoll	Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP
Proxy	Ein Proxy ist eine Netzwerkkomponente. Der Proxy ist ein Vermittler. Er leitet eine Anfrage der Quelle mit seiner eigenen IP-Adresse an das Ziel weiter.
PVID	Der Port VLAN Identifier (PVID) ist die Standard-VLAN-ID des jeweiligen Ports. Ein Paket, das ohne VLAN-Tag diesen Port erreicht, wird mit dieser ID versehen.
Q-SIG	Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.
QoS	Quality of Service (QoS) beschreibt die Qualität (Güte) des Kommunikationsdienstes. Diese wird anhand von Bandbreite, Verzögerung, Paketverlusten und Jitter definiert. Um zeitkritische Datenpakete für VoIP oder Videostreaming möglichst schnell zu übertragen, werden alle Datenpakete bei QoS in Gruppen sortiert und entsprechend ihrer Priorität im Netzwerk schneller oder langsamer weitergeleitet.
Queue	In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen. Der RADIUS-Server authentifiziert den Client z. B. mittels der Überprüfung von Benutzername und Kennwort. Siehe auch TACACS+.
RE-ADSL2	Siehe G.992.5.

Real Time Jitter Control	Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.
Regelkette	In einer Regelkette sind unterschiedliche Filterregeln zusammengefasst. Eine Filterregel wählt einen Teil des Datenverkehrs aufgrund bestimmter Merkmale, z. B. der Quell-IP-Adresse, aus und wendet auf diese Teilmenge eine Aktion an, z. B. blockieren.
Registrar	Der SIP-Server (Registrar) muss eingesetzt werden, falls die Teilnehmer eines VoIP-Gesprächs keine statischen IP-Adressen verwenden. Der SIP-Server registriert die IP-Adressen der Clients und sendet diese Informationen an den SIP-Proxy, der die Anrufe vermittelt. Meistens sind SIP-Proxy und SIP-Registrar identisch.
Repeater	Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.
Reset	Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.
RFC	Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.
Rijndael	Siehe AES.
RIP	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
RJ45	RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.
Roaming	Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.
Router	Ein Router ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze auf der Vermittlungsschicht des OSI-Modells. Datenpakete werden anhand von IP-Adressen übertragen. Über Routing-Tabellen werden die besten Wege (Routen) durch das Netzwerk festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle, z. B. OSPF oder RIP, aus.

Router Advertisement	Router Advertisements sind Nachrichten, die der Router ins Netzwerk sendet. Diese verkünden die Anwesenheit des Routers im Netz. Ferner werden mithilfe von Router Advertisements Präfixe verteilt, die Autokonfiguration organisiert und der Standardrouter festgelegt.
Routing	Routing bezeichnet das Festlegen von Wegen für die Nachrichtenübermittlung.
RSA	Mithilfe des RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über die Signatur können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. RSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch DSA. RSA ist langsamer in der Schlüsselerzeugung aber schneller in der Schlüsselverarbeitung als DSA.
RTP	Mit dem Real-Time Transport Protocol (RTP) werden Audio- und Video-Daten (Streams) über IP-basierte Netzwerke übertragen.
RTS Threshold	Sobald die Anzahl der Frames im Datenpaket über der RTS-Schwelle (RTS Threshold) liegt, wird vor dem Senden eines Datenpakets eine Verbindungsüberprüfung (RTS/CTS-Handshake) durchgeführt.
RTSP	Das Real-Time Streaming Protocol (RTSP) steuert die Übertragung von Audio- und Videodaten (Streams) über IP-basierte Netzwerke. Während das Real-Time Transport Protocol (RTP) zur Übertragung der Nutzdaten dient, besteht die Funktion von RTSP hauptsächlich in der Steuerung der Datenströme.
S2M-Anschluss	Siehe Primärmultiplexanschluss.
SA	Eine sogenannte Sicherheitsverbindungen (Security Associations, SA) enthält Informationen über die Maßnahmen zur Sicherung der Kommunikationsverbindung. Mindestens eine SA ist die Voraussetzung für den Aufbau einer gesicherten Verbindung. Eine SA enthält die IP-Adresse des Teilnehmers, das verwendete Authentifizierungsprotokoll, den verwendeten Verschlüsselungsalgorithmus, den Sicherheits-Parameter-Index (SPI), den Selektor und die Gültigkeitsdauer.
SAD	Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die SAD enthält Informationen über

jede Sicherheitsverbindung. Also welche Verschlüsselungsalgorithmen, Schlüssel, Protokolle, Sitzungsnummern oder Gültigkeitszeiträumen verwendet werden sollen. Für eine ausgehende Verbindung zeigt ein Eintrag der SPD auf einen Eintrag der SAD. Dadurch kann die SPD festlegen, welcher SA für ein bestimmtes Paket verwendet wird. Bei einer eingehenden Verbindung wird die SAD angesprochen, um festzulegen, wie das Paket verarbeitet wird.

SCEP	Das Simple Certificate Enrollment Protocol (SCEP) dient zur Verwaltung digitaler Zertifikate.
Scheduling	Unter Scheduling versteht man einen Aufgabenplan. Bestimmte Aktionen (z. B. Deaktivierung einer Schnittstelle) werden durch Ereignisse (z. B. Zeit oder Änderung einer MIB-Variablen) ausgelöst.
Serielle Schnittstelle	Die serielle Schnittstelle dient dem Datenaustausch zwischen Computern und Peripheriegeräten. Sie kann zur Konfiguration des Geräts oder zur Datenübertragung über eine IP-Infrastruktur verwendet werden (Serial over IP).
Server	Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden.
SFP	Small Form-factor Pluggable (SFP) ist eine Steckverbindung, die für extrem schnelles Ethernet entwickelt wurde.
SHA1	Secure-Hash-Algorithm Version 1 (SHA1) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
SHDSL	Symmetrical High-bit-rate Digital Subscriber Line. Siehe DSL.
Shell	Die Shell ist eine Eingabeschnittstelle (z. B. Kommandozeile oder grafische Benutzerschnittstelle) zwischen Computer und Benutzer.
Shorthold	Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.
SIF	Bei einer Stateful Inspection Firewall (SIF) wird die Weiterleitung eines Datenpakets nicht nur durch Quell- und Zieladressen oder Port bestimmt, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung.
SIP	Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das Protokoll wird für IP-Telefonie (VoIP) verwendet.

SIP-Provider	Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.
SNMP	Mithilfe des Simple Network Management Protocol (SNMP) werden verschiedene Netzwerkkomponenten (z. B. Router, Server, usw.) von einem zentralen System aus konfiguriert, kontrolliert und überwacht. Die änderbaren Einstellungen der Netzwerkkomponenten sind dabei in einer Datenbank gespeichert – der Management Information Base (MIB). SNMP verwendet UDP. Die Netzwerkkomponente empfängt dabei Anfragen (Requests) auf Port 161, während das verwaltende System Bestätigungsmeldungen (TRAPs) auf Port 162 entgegennimmt.
Spatial Streams	Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der Übertragungsrates.
SPD	Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die Security-Policy-Datenbank führt die Formen des Datenverkehrs auf, die gesichert werden sollen. Dazu werden Faktoren wie Quell- und Zieladresse des Datenpakets verwendet.
SRTP	Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die mithilfe von AES verschlüsselte Variante des Real-Time Transport Protocol (RTP).
SSH	Secure Shell (SSH) ist ein Netzwerkprotokoll mit dem man eine verschlüsselte Verbindung zur Shell eines Geräts herstellen kann.
SSID	Der Service Set Identifier (SSID) definiert ein Funknetzwerk, das auf IEEE 802.11 basiert. Der SSID ist der Netzwerkname des Wireless LAN. Alle Access Points und Clients, die zum gleichen Netzwerk gehören, verwenden denselben SSID. Die SSID-Zeichenfolge kann bis zu 32 Zeichen lang sein und wird allen Paketen unverschlüsselt vorangestellt. Mithilfe der SSID ANY kontaktiert ein Client alle erreichbaren Access Points. Dem Anwender werden daraufhin alle verfügbaren WLANs angezeigt und er kann das passende Netz auswählen. Wenn ein Access Point für verschiedene Netze verwendet wird, erhält jedes Funknetzwerk eine eigene MSSID (Multi Service Set Identifier).
SSL	Secure Sockets Layer (SSL) ist ein Protokoll zur Datenverschlüsselung. Seit Version 3.1 wird die neue Bezeichnung Transport Layer

Security (TLS) verwendet. SSL wird hauptsächlich für HTTPS verwendet, um die Datenübertragung zwischen Web-Server und Web-Browser zu verschlüsseln.

STAC	Mithilfe von STAC wird die übertragene Datenmenge verringert (Datenkompression).
Standardroute	Die Standardroute (Default Route) wird verwendet, falls keine andere passende Route vorhanden ist.
Standardrouter	Siehe Default Gateway.
Standleitung	Eine Standleitung (Leased Line) ist eine permanente Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz.
Statische IP-Adresse	Im Gegensatz zu einer dynamischen IP-Adresse wird die statische IP-Adresse fest vom Anwender zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
STUN-Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Ein STUN-Server ermöglicht VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Netzwerk.
Subadressierung	Neben der ISDN-Telefonnummer kann eine Subadresse beim Verbindungsaufbau übertragen werden. Diese Subadresse überträgt eine beliebige Zusatzinformation. Diese kann genutzt werden, um z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt anzusprechen oder bestimmte Programme auf einem PC aufzurufen.
Subnetz	Ein Teilnetz eines IP-Netzes wird als Subnetz bezeichnet. Ein Teilnetz wird wie ein normales Netzwerk über IP-Adresse und (Sub-)Netzmaske (IPv4) bzw. Präfixlänge (IPv6) definiert. Beispiel: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 mögliche IP-Adressen) ist ein Subnetz von 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 mögliche IP-Adressen).
Switch	Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerkkomponenten miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells betrieben werden. Das dem

	Switch vergleichbare Gerät der Bitübertragungsschicht wird als Hub bezeichnet.
SWYX	SwyxWare ist eine softwarebasierte Kommunikationslösung für VoIP.
Syslog	Das Syslog-Protokoll wird zur Übermittlung von Status-Meldungen in einem IP-Netzwerk verwendet. Verschiedene Netzwerkkomponenten können somit von einem zentralen System aus überwacht werden. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP-Port 514 gesendet.
T.38	T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.
TACACS+	Das Terminal Access Controller Access Control System Plus (TACACS+) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern. Der TACACS+-Server authentifiziert den Client mittels der Überprüfung von z. B. Benutzername und Kennwort. Im Gegensatz zum UDP-basierten RADIUS-Protokoll verwendet TACACS+ TCP auf Port 49 und überträgt die gesamte Kommunikation verschlüsselt.
TAPI	Telephony Applications Programming Interface (TAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch CAPI.
TCP	Beim Transmission Control Protocol (TCP) handelt es sich um ein verbindungsorientiertes Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungsorientierten Protokoll wird vor der Übertragung eine logische Verbindung aufgebaut und aufrechterhalten. Dies ermöglicht eine zuverlässige Übertragung der Daten. Allerdings werden ständig Kontrollinformationen neben dem eigentlichen Datenpaketen übertragen. Dies führt zu einem Anstieg des übertragenen Datenvolumens. Siehe auch UDP.
TCP-ACK-Paket	Ein ACK-Signal (Acknowledgement = Bestätigung) wird bei einer Datenübertragung verwendet, um den Erhalt oder die Verarbeitung von Daten oder Befehlen zu bestätigen. TCP verwendet ACK-Signale zur Kommunikation.
TE	Der Endgeräteanschluss (Terminal Equipment, TE) bezeichnet einen Anschluss bzw. eine Betriebsart. Der TE-Anschluss ist der Anschluss eines Endgeräts. Im TE-Betrieb wird das Gateway am internen S0 der Telefonanlage angeschlossen und stellt damit ein

	ISDN-Endgerät dar. Siehe auch NT.
Telnet	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
TFTP	Das Trivial File Transfer Protocol (TFTP) regelt die Übertragung von Dateien. Im Vergleich zu FTP fehlen eine Möglichkeit zur Dateianzeige, eine Rechtevergabe und eine Benutzerauthentifizierung.
Tiger 192	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
TLS	Siehe SSL.
TOS	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
Traceroute	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpakete bis zum abgefragten Ziel-Host vermittelt werden.
Trigger	Unter Trigger versteht man einen Auslöseimpuls.
Triple DES	Siehe DES.
TTL	Die Time to live (TTL) ist die konfigurierte Gültigkeitsdauer eines Datenpakets. Beim Internet Protocol (IP) legt die TTL fest, wie viele Hops ein Datenpaket passieren darf. Der Maximalwert beträgt 255 Hops. Mit jedem Hop wird die TTL um 1 reduziert. Falls ein Datenpaket nach Ablauf seiner TTL noch nicht sein Ziel erreicht hat, wird es verworfen.
Twofish	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) ist eine DSL-Variante. Sie wurde als ANSI T1.413 entwickelt und als G.992.2 standardisiert. U-ADSL erlaubt die parallele Nutzung verschiedener Kommunikationstechniken, z. B. ISDN und POTS, und benötigt keinen Splitter.
Überprüfung der Rückroute	Falls bei einer Schnittstelle "Überprüfung der Rückroute" (Back Route Verify) aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden.

UDP	Beim User Datagram Protocol (UDP) handelt es sich um ein verbindungsloses Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungslosen Protokoll ist keine Kontrolle für die Auslieferung des Pakets integriert. Die Kontrolle muss in der Anwendungsschicht erfolgen. Im Gegenzug ist UDP schneller als verbindungsorientierte Protokolle.
ULA	Unique Local Addresses (ULA) sind IPv6-Adressen, die nicht geroutet werden. Sie können in privaten Netzen (z. B. einem LAN) verwendet werden. ULAs beginnen mit dem Präfix fd.
UMTS	Das Universal Mobile Telecommunications System (UMTS), auch als 3G bezeichnet, ist ein Mobilfunkstandard mit einer spezifizierten max. Datenübertragungsrate von 384 kbit/s bzw. 21 Mbit/s in Verbindung mit HSPA+.
Unicast	Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertragen.
UPnP	Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.
Upstream	Das Gateway leitet die Daten des eigenen Netzwerks weiter.
URL	Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: http://www.example.org/index.htm (Web-Seite im Internet)
V.110	V.110 beschreibt ein Verfahren zur Anpassung von Bitströmen mit 0,6, 1,2, 2,4, 2,8, 7,2, 9,6, 12, 14,4, 19,2 und 38,4 kbit/s in den ISDN-Bitstrom von 64 kbit/s.
VDSL	Very High Speed Digital Subscriber Line. Siehe DSL.
VID	Siehe VLAN.
VLAN	Ein Netzwerk kann in eines oder mehrere logische Teilnetze – sogenannte Virtual-Local-Area-Networks (VLAN) – aufgespalten werden, indem die Netzwerkkomponenten das Datenpaket eines definieren Teilnetzes nicht mehr in andere Teilnetze weiterleiten. Jedem VLAN wird eine eindeutige Nummer zugeordnet. Diese Nummer wird VLAN ID (VID) genannt und den Datenpaketen im VLAN-Tag zugeordnet.
VoIP	Voice over IP (VoIP), auch IP-Telefonie genannt, bezeichnet die Übertragung von Sprache über ein IP-Netzwerk. Der Auf- und Ab-

bau der Telefonverbindung erfolgt dabei über Signalisierungsprotokolle, wie z. B. SIP.

VPN	Mithilfe eines virtuellen privaten Netzwerks (VPN) werden private Datenpakete durch ein öffentliches Netzwerk transportiert. Die Informationen werden dabei durch Einkapselung in neue Protokolle von den öffentlich zugänglichen Daten getrennt, um sie an den vorgesehenen Empfänger zu leiten. Man spricht in diesem Zusammenhang auch von einem Tunnel, der zwischen den privaten Netzen der beiden Verbindungsteilnehmer aufgebaut wird. VPN-Protokolle sind IP-Sec, PPTP, L2TP und GRE.
VSS	Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.
Wählverbindung	Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.
Walled Garden	Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.
WAN	Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausge dehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.
WDS	Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.
Web-Server	Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.
WEP	Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.
WINS	Der Windows Internet Name Service (WINS) ist eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft. Wie DNS dient WINS der zentralen Namensauflösung. Siehe auch DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.
WMM	Wi-Fi Multimedia (WMM) priorisiert die Datenpakete unterschiedlicher Anwendungen und verbessert damit die Übertragung von Sprach-, Musik- und Videodaten in WLAN-Netzwerken. Dazu stellt WMM Quality-of-Service-Merkmale (QoS) für IEEE 802.11-basierte Netzwerke bereit.

WPA	Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.
WPA - Enterprise	WPA - Enterprise bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmer durch das Extensible Authentication Protocol (EAP). Nach erfolgreicher Authentisierung übermittelt der Server dem Client und dem Access Point einen gemeinsamen Schlüssel für die Datenübertragung im WLAN.
WPA - PSK	WPA - PSK bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmern über Preshared Keys. Dabei nutzen Access Point und Client die gleiche Zeichenfolge für die Schlüsselberechnung im WLAN. Diese Zeichenfolge muss von den Anwendern konfiguriert werden.
WPA 2	Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.
X.25	X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.
X.31	Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.
X.500	Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.
X.509	Der X.509-Standard beschreibt die Erstellung der Zertifikate für eine Public-Key-Infrastruktur (PKI).
X.75	X.75 ist eine standardisierte Protokollfamilie für ISDN-Netzwerke mit einer Übertragungsrate von 64 kbit/s.
XAuth	Mithilfe von XAUTH (Extended Authentication) wird IKE um weitere Authentifizierungsmechanismen ergänzt. Nach einer erfolgreichen IKE-Phase-1-Authentifizierung kann der Benutzer noch einmal separat identifiziert werden. Die Identifizierung erfolgt über Benutzername und Passwort, PAP, CHAP oder Hardware-basierte Systeme.
Zeitschlitz	Ein Zeitschlitz ist ein fest zugeordneter Zeitabschnitt innerhalb eines Übertragungsrahmens und entspricht meist einem Übertragungskanal.
Zertifikat	Ein Zertifikat identifiziert eine Person, eine Institution, ein Gerät oder eine Anwendung. Ein Public-Key-Zertifikat ist ein digitales Zertifikat und stellt eine Verbindung zwischen der Identität und einem öffentli-

chen Schlüssel her. Zertifikate mit öffentlichem Schlüssel werden von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt. Nicht mehr vertrauenswürdige Zertifikate können über Zertifikatsperrlisten (Certificate Revocation List, CRL) deaktiviert werden.

Index

- Abfrage Intervall 257
- Address assignment 393
- Admin-Status 217
- Administrative FQDNs 397
- Administrativer Status 289 , 370
- Adressbereich 357
- Adresse/Präfix 357
- Adresse/Subnetz 357
- Adressmodus 112
- Adresstyp 357
- AFTR 278
- Ähnliches Zertifikat überschreiben
405
- Airtime Fairness 129 , 168
- Aktion 148 , 148 , 204 , 242 , 349 ,
351 , 405 , 436
- Aktiver Allgemeiner Präfix 200
- Aktives Funkmodulprofil 165
- Aktiviert 344
- Aktualisierung aktivieren 378
- Aktualisierungsintervall 380
- Aktualisierungspfad 380
- Alle Multicast-Gruppen 261
- Allgemeiner Name 102
- Allgemeiner Präfix 116 , 274
- Ankommende Rufnummer 304
- Ankündigen 116
- Anmeldefenster 430
- Antwort 372
- Antwortintervall (Letztes Mitglied) 257
- Anzahl der Spatial Streams 127 , 168
- Anzahl erlaubter Verbindungen 297
- Anzahl Nachrichten 453
- AP-MAC-Adresse 148
- APN 386
- ARP Lifetime 244
- Art der Einrichtung 116 , 274
- Art des Datenverkehrs 203
- Aufzurufende Seite nach Login 428
- Ausgehende ISDN-Nummer 341
- Ausgehende Rufnummer 304
- Ausgehende Schnittstelle 233
- Ausgewählte Kanäle 132
- Ausgewählte Ports 341
- Ausgewählter Kanal 127
- Auswahl 358
- Auswahl des Client-Bands 141 , 177
- Auszuführende Aktion 422
- Authentifizierung 276 , 282 , 332 ,
338
- Authentifizierungsmethode 289 , 306
- Authentifizierungstyp 85 , 89
- Automatische Subnetzerstellung 116 ,
274
- Autonomous Flag 118
- Autospeichermodus 103
- Autospeichermodus 405
- Bandbreite 127 , 168
- Basierend auf Ethernet-Schnittstelle
111
- Beacon Period 143 , 171
- Bedingung des Schnittstellenverkehrs
399
- Bedingung für Ereignisliste 405
- Befehlsmodus 405
- Befehlstyp 405
- Benachrichtigungsdienst 453
- Benutzer 95 , 320
- Benutzer muss das Passwort ändern
95
- Benutzerdefiniert 102
- Benutzerdefinierte DHCP-Optionen
387
- Benutzerdefinierter Kanalplan 133 ,
171
- Benutzername 269 , 279 , 329 , 335 ,
378
- Benutzter Präfix/Länge 200
- Berichtsmethode 243
- Berücksichtigen 212
- Beschreibung 93 , 97 , 106 , 165 ,
168 , 192 , 203 , 217 , 222 , 226 ,
233 , 238 , 242 , 269 , 278 , 279 ,
289 , 296 , 306 , 314 , 320 , 326 ,
329 , 335 , 344 , 355 , 356 , 357 ,

- 358 , 359 , 361 , 370 , 384 , 388 ,
399 , 405 , 432 , 436
- Beschreibung 195
- Beschreibung des Client Links 148
- Betreff 453
- Betreibermodus 85
- Betriebsmodus 127 , 165 , 168
- Bevorzugte Gültigkeitsdauer 118
- Blockieren nach Verbindungsfehler für
276 , 282 , 332 , 338
- Blockzeit 90 , 311
- Burst-Größe 233
- Burst-Mode 168
- CA-Name 405
- CA-Zertifikat 99
- CA-Zertifikate 311
- Callback 341
- CAPWAP-Verschlüsselung 165
- Client FQDN akzeptieren 397
- Code 359
- COS-Filter (802.1p/Layer 2) 222 , 238
, 432
- CRL verwenden 405
- CSV-Dateiformat 405
- Dateikodierung 104 , 105
- Dateiname 405
- Dateiname auf Server 405
- Dateiname in Flash 405
- Designated-Router-Priorität 262
- DH-Gruppe 306
- DHCP Client an Schnittstelle 244
- DHCP Broadcast Flag 119
- DHCP-Client 113
- DHCP-Client 272
- DHCP-Hostname 119
- DHCP-MAC-Adresse 119
- DHCP-Modus 120
- DHCP-Optionen 385
- DHCP-Server 113 , 159
- Dienst 204 , 217 , 222 , 238 , 349 ,
351 , 432
- DNS-Aushandlung 276 , 282 , 333 ,
340
- DNS-Domänen-Suchliste 394
- DNS-Hostname 372
- DNS-Propagation 120
- DNS-Server 284 , 322 , 343 , 383 ,
395
- DNS-Zuweisung über DHCP 244
- Domäne 374
- Domäne am Hotspot-Server 428
- Drahtloser Modus 129 , 168
- Dropping-Algorithmus 235
- DSCP / Traffic Class Filter (Layer 3)
222 , 238 , 432
- DSCP/TOS-Wert 192
- DSCP/Traffic-Class-Filter setzen (Layer
3) 226
- DTIM Period 143 , 171
- DUID 397
- Durchsatz 183
- Durchsatz/Client 183
- Dynamische Black List 178
- E-Mail 102
- EAP-Vorabauthentifizierung 139 , 175
- Eigene IP-Adresse per ISDN/GSM über-
tragen 304
- Eingehende ISDN-Nummer 341
- Eintrag aktiv 85 , 89
- Empfänger 453
- Entfernte GRE-IP-Adresse 344
- Entfernte PPTP-IP-Adresse 282 , 335
- Entfernte PPTP-IP-Adresse Hostname
335
- Entfernte IP-Adresse 327
- Entfernter Hostname 326
- Entferntes IPv6-Netzwerk 294
- Enthaltene Zeichenfolge 453
- Ereignis 453
- Ereignisliste 399 , 405
- Ereignistyp 399
- Erfolgreiche Versuche 399 , 422
- Erlaubte Adressen 142 , 178
- Erreichbarkeitsprüfung 87 , 311 , 318
- Erzeugungsmethode 117 , 275
- Externer Dateiname 104 , 105
- Facility 450
- Fallback-Proxy-Schnittstelle 1 258

- Fallback-Proxy-Schnittstelle 2 258
- Fehlgeschlagene Versuche 399 , 422
- Fehlversuche per Zeitraum 178
- Filter 226
- Fragmentation Threshold 132 , 171
- Frequenzband 127 , 168
- Gateway 385
- Gateway-Adresse 195
- Gateway-IP-Adresse 191
- GEO Zone Status 399
- Gerät 165
- Geräte pro Ticket 430
- Geschäftsbedingungen 428
- Geschwindigkeitsprofil im 2,4-GHz-Band 180
- Geschwindigkeitsprofil im 5-GHz-Band 144 , 180
- Gewichtung 233
- Größe des Protokoll-Headers unterhalb Layer 3 229
- Gruppen-ID 421
- Gruppenbeschreibung 85 , 212 , 214 , 244
- Gültigkeitsdauer 118
- Hello Hold Time 263
- Hello-Intervall 263 , 328
- Hersteller auswählen 386 , 387
- Hersteller-ID 386 , 387
- Herstellerbeschreibung 386 , 387
- Herstellerspezifische Informationen 386
- Herstellerspezifische Informationen (DHCP-Option 43) 385
- High-Priority-Klasse 226
- Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable 405
- Host 374
- Hostname 378
- IGMP Proxy 258
- IGMP Snooping 143 , 174
- IKE (Internet Key Exchange) 289
- Immer aktiv 269 , 279 , 329 , 335
- Indexvariablen 399 , 405
- Intervall 399 , 405 , 422 , 425
- Intra-cell Repeating 138 , 174
- IP-Adressbereich 159 , 284 , 322 , 343 , 383
- IP-Adresse 388 , 450 , 459
- IP-Adresse / Netzmaske 112
- IP-Adresse zur Nachverfolgung 214
- IP-Adresse/Netzmaske 159
- IP-Adresse/Netzmaske 250
- IP-Adressmodus 271 , 280 , 330 , 336
- IP-Komprimierung 318
- IP-Poolname 284 , 322 , 343 , 383 , 384
- IP-Version 358
- IP-Version 370
- IP-Version des Tunnelnetzwerks 289
- IP-Zuordnungspool 292
- IP-Zuordnungspool (IPCP) 330 , 336
- IPv4 357
- IPv4 Proxy ARP 299
- IPv4-Adresse 372
- IPv4-Adressvergabe 292
- IPv4-Quelladresse/-netzmaske 222 , 238 , 432
- IPv4-Zieladresse/-netzmaske 222 , 238 , 432
- IPv6 113 , 272 , 357
- IPv6-Adresse 372
- IPv6-Adressen 113 , 272
- IPv6-Modus 113 , 272
- IPv6-Quelladresse/-länge 222 , 238 , 432
- IPv6-Schnittstelle 278
- IPv6-Zieladresse/-länge 222 , 238 , 432
- Join/Prune Hold Time 263
- Join/Prune-Intervall 263
- Kanal 127 , 148 , 165
- Kanäle scannen 133
- Kanalplan 132 , 171
- Kenntnis der statischen Schnittstelle 397
- Kennwort für geschütztes Zertifikat 405
- Klassen-ID 226 , 233

- Klassenplan 226
- Komprimierung 338
- Konfiguration verschlüsseln 405
- Konfiguration enthält Zertifikate/Schlüssel 405
- Konfiguration speichern 93
- Konfigurationsmodus 292
- Kontrollmodus 229 , 285
- Land 102
- Layer 4-Protokoll 192
- LCP-Erreichbarkeitsprüfung 276 , 282 , 332 , 338
- LDAP-URL-Pfad 106
- Lease Time 385
- Lebensdauer 306 , 314
- Level 450
- Level Nr. 93
- Link-Präfix 116 , 274
- Lizenzschlüssel 71
- Lizenzseriennummer 71
- Lokale GRE-IP-Adresse 344
- Lokale IP-Adresse 244
- Lokale Zertifikatsbeschreibung 104 , 105 , 405
- Lokale ID 289
- Lokale IP-Adresse 191 , 271 , 280 , 292 , 328 , 330 , 336 , 344
- Lokale PPTP-IP-Adresse 282
- Lokale WLAN-SSID 405
- Lokaler Dateiname 405
- Lokaler Hostname 326
- Lokaler ID-Typ 289 , 306
- Lokaler ID-Wert 306
- Lokales IPv6-Netzwerk 294
- Lokales Zertifikat 306
- Long Retry Limit 171
- MAC-Adresse 111 , 388
- Mail-Exchanger (MX) 380
- Max. Scan-Dauer 133
- Max. Anzahl Clients - Hard Limit 141 , 177
- Max. Anzahl Clients - Soft Limit 141 , 177
- Max. Queue-Größe 235
- Max. Übertragungsrate 171
- Max. Zeitraum aktiver Scan 133
- Max. Zeitraum passiver Scan 133
- Maximale Upload-Geschwindigkeit 229 , 233 , 285
- Maximale Antwortzeit 257
- Maximale Anzahl der erneuten Einwählversuche 276 , 282
- Maximale Anzahl Wiederholungen 328
- Maximale Anzahl der IGMP-Statusmeldungen 257
- Maximale Zeit zwischen Versuchen 328
- Menüs 94
- Metrik 191 , 195 , 292
- Metrik-Offset für Aktive Schnittstellen 250
- Metrik-Offset für Inaktive Schnittstellen 250
- MIB-Variablen 405
- Min. Queue-Größe 235
- Min. Zeitraum aktiver Scan 133
- Min. Zeitraum passiver Scan 133
- Minimale Zeit zwischen Versuchen 328
- Mitglieder 355 , 356 , 361
- MobIKE 299
- Modus 99 , 148 , 192 , 244 , 257 , 304 , 306 , 320
- Modus des D-Kanals 304
- Monitored GEO Zone 399
- MTU 278 , 344
- Multicast-Gruppen-Adresse 261 , 265
- Multicast-Gruppenbereich 265
- Nach Ausführung neu starten 405
- Nachrichtenkomprimierung 453
- Nachrichtentyp 450
- Name 165 , 200 , 320 , 393
- Name des Bridge Links (ID) 149
- NAT-Eintrag erstellen 271 , 280 , 330 , 336
- NAT-Methode 203
- NAT-Traversal 311

- Netzmaske 244
- Netzwerkadresse 244
- Netzwerkkonfiguration 244
- Netzwerkname (SSID) 138 , 146 ,
148 , 174
- Neue Quell-IP-Adresse/Netzmaske
207
- Neue Ziel-IP-Adresse/Netzmaske 207
- Neuer Quell-Port 207
- Neuer Ziel-Port 207
- Neustart des Geräts nach 405
- Nutzungsart 338
- Nutzungsbereich 127
- Öffentliche IPv4-Quelladresse 299
- Öffentliche IPv6-Quelladresse 299
- Öffentliche Schnittstelle 299
- Öffentlicher Schnittstellenmodus 299
- On Link Flag 118
- Organisation 102
- Organisationseinheit 102
- Original Quell-Port/Bereich 204
- Original Ziel-IP-Adresse/Netzmaske
204
- Original Ziel-Port/Bereich 204
- Originale Quell-IP-Adresse/Netzmaske
204
- Ort 102
- OSPF-Modus 333 , 340
- Override Interval 263
- Passwort 95 , 99 , 104 , 105 , 269 ,
279 , 320 , 326 , 329 , 335 , 378 ,
405 , 436
- Peer-Adresse 289
- Peer-ID 289
- PFS-Gruppe verwenden 314
- Phase-1-Profil 297
- Phase-2-Profil 297
- PIM-Modus 262
- PIN 386
- PMTU propagieren 318
- Pool-Verwendung 384
- Pop-Up-Fenster für Statusanzeige
430
- Port 380
- PPPoE-Ethernet-Schnittstelle 269
- PPPoE-Modus 269
- PPPoE-Schnittstelle für Mehrfachlink
269
- PPTP-Adressmodus 282
- PPTP-Ethernet-Schnittstelle 279
- PPTP-Modus 335
- Präfixlänge der Multicast-Gruppe 265
- Preshared Key 139 , 146 , 149 , 175 ,
289
- Primärer IPv4-DNS-Server 370
- Primärer IPv6-DNS-Server 370
- Primärer DNS-Server (IPv4/IPv6) 374
- Priorisierungsalgorithmus 229
- Priorität 85 , 89 , 233 , 370
- Priority Queueing 233
- Privaten Schlüssel generieren 99
- Propagation Delay 263
- Proposals 306 , 314
- Protokoll 204 , 217 , 222 , 238 , 296 ,
359 , 380 , 405 , 432 , 450
- Provider 378
- Providername 380
- Provisioning-Server 387
- Proxy ARP 119
- Proxy-ARP-Modus 333 , 340
- Proxy-Schnittstelle 258
- Quell-IP-Adresse 399 , 405
- Quell-IP-Adresse 422 , 425
- Quell-IP-Adresse/Netzmaske 192 ,
204 , 217 , 296
- Quell-Port 192 , 296
- Quell-Port/Bereich 204 , 217 , 222 ,
238 , 432
- Quelladresse/Länge 195
- Quelle 349 , 351 , 405
- Quellportbereich 359
- Quellschnittstelle 192 , 217 , 261 ,
374
- Queues/Richtlinien 232
- RA-Signierungszertifikat 99
- RA-Verschlüsselungszertifikat 99
- RADIUS-Dialout 87
- RADIUS-Passwort 85

- RADIUS-Server 175
- RADIUS-Server Gruppen-ID 320
- Real Time Jitter Control 229
- Regelkette 242 , 243 , 438
- Rendezvous Point IP-Adresse 265
- Richtlinie 87 , 90
- Richtung 226 , 250
- Richtung des Datenverkehrs 399
- Roaming-Profil 133
- Robustheit 257
- Rolle 149 , 320
- Route aktiv 195
- Routenankündigung 247
- Routeneinträge 271 , 280 , 292 , 330 ,
336 , 344
- Routenklasse 189
- Routenselektor 214
- Routentyp 189 , 195
- Router Advertisement annehmen 113
, 272
- Router-Gültigkeitsdauer 120
- Router-Präferenz 120
- RSSI-Schwellwert 144 , 181
- RTS Threshold 132 , 171
- RTT-Modus (Realtime-Traffic-Modus)
233
- Rx Shaping 143 , 180
- Scan-Intervall 133
- Scan-Schwelle 133
- SCEP-Server-URL 405
- SCEP-URL 99
- Schlüsselgröße 405
- Schlüsselwert 344
- Schnittstelle 75 , 75 , 78 , 189 , 203 ,
214 , 229 , 243 , 250 , 257 , 262 ,
285 , 370 , 378 , 384 , 393 , 405 ,
424 , 428 , 438
- Schnittstellen 226
- Schnittstellenaktion 424
- Schnittstellenauswahl 244
- Schnittstellenmodus 111 , 370
- Schnittstellenstatus 399
- Schnittstellenstatus festlegen 405
- Schweregrad 453
- Sekundärer IPv4-DNS-Server 370
- Sekundärer IPv6-DNS-Server 370
- Sekundärer DNS-Server (IPv4/IPv6)
374
- Sende WOL-Paket über Schnittstelle
436
- Sendeleistung 127 , 165
- Sequenznummern der Datenpakete
328
- Server 380
- Server Timeout 87
- Server-IP-Adresse 85 , 89
- Server-URL 405
- Serveradresse 405
- Setze COS Wert (802.1p/Layer 2)
226
- Short Guard Interval 132 , 171
- Short Retry Limit 171
- Sicherheitsmodus 139 , 146 , 175
- Sicherheitsrichtlinie 112 , 113 , 271 ,
272 , 280 , 292 , 294
- Signal 148
- SNTP-Server 395
- Special Handling Timer 217
- Sperrzeit für Black List 178
- Spezifische Ports 341
- Sprache für Anmeldefenster 428
- Staat/Provinz 102
- Standard-Benutzerpasswort 85
- Standard-Timeout bei Inaktivität 430
- Standardroute 278
- Standardroute 271 , 280 , 292 , 330 ,
336 , 344
- Standardroute erstellen 119
- Standort 165
- Startmodus 297
- Startzeit 404
- Statische Adressen 117 , 275
- Status 399
- Status der Funktionstaste 399
- Status des Auslösers 405
- Status festlegen 405
- Stopzeit 404
- Stub Interface Mode 262

- Subjektnamen 405
- Subnetz-ID 116 , 274
- TACACS+-Passwort 89
- TCP-ACK-Pakete priorisieren 276 ,
282 , 332
- TCP-MSS-Clamping 119
- TCP-Port 90
- Tickettyp 430
- Timeout 90
- Timeout bei Inaktivität 269 , 279 , 329
, 335
- Timeout für Nachrichten 453
- Toleranzzeit 144 , 181
- Traffic Shaping 233
- Traffic Shaping 229
- Transparente MAC-Adresse 75
- Trigger 424
- Triggered-Hello-Intervall 263
- Tunnelprofil 329
- Tx Shaping 143 , 180
- Typ 200 , 222 , 238 , 359 , 432 , 436
- U-APSD 138 , 174
- Überbuchen zugelassen 233
- Überprüfung anhand einer Zertifikatsperlliste (CRL) 97
- Überprüfung der IPv4-Rückroute 299
- Übertragener Datenverkehr 399
- Übertragungsmodus 304
- Übertragungsschlüssel 139 , 146 ,
175
- Überwachte Schnittstelle 399
- Überwachte Subsysteme 453
- Überwachte Variable 399
- Überwachte IP-Adresse 422
- Überwachte Schnittstelle 424
- Überwachtes Zertifikat 399
- UDP-Port 87
- UDP-Quellport 327
- UDP-Zielport 327
- Unveränderliche Parameter 218
- Verbindungsstatus 222 , 238 , 432
- Verbindungstyp 329
- Verbleibende Gültigkeitsdauer 399
- Verbunden 148
- Verbundene Clients 183
- Vergleichsbedingung 399
- Vergleichswert 399
- Vermeidung von Datenstau (RED) 235
- Verschlüsselung 90 , 332 , 338
- Verschlüsselungsmethode 229
- Version in Empfangsrichtung 247
- Version in Senderichtung 247
- Versionsprüfung 405
- Versuche 405 , 425
- Verteilungsmodus 212
- Verteilungsrichtlinie 212 , 214
- Verteilungsverhältnis 214
- Vertrauenswürdigkeit des Zertifikats erzwingen 97
- Verwendeter Kanal 165
- Verwerfen ohne Rückmeldung 243
- VLAN 179 , 269
- VLAN Identifier 123
- VLAN-ID 111 , 159 , 179 , 269
- VLAN-Mitglieder 123
- VLAN-Name 123
- Vom NAT ausnehmen (DMZ) 244
- Von Schnittstelle 200
- Vorrang 265
- Wake-on-LAN-Filter 436
- Wake-On-LAN-Regelkette 436
- Walled Garden 428
- Walled Garden URL 428
- Weiterleiten 374
- Weiterleiten an 374
- Wiederholungen 87
- Wiederkehrender Hintergrund-Scan 168
- Wildcard 380
- Wildcard-MAC-Adresse 75
- Wildcard-Modus 75
- WLAN-Modul auswählen 405
- WLC-SSID 405
- WPA Cipher 139 , 146 , 175
- WPA-Modus 139 , 146 , 175
- WPA2 Cipher 139 , 146 , 175
- XAUTH-Profil 297

- Zeitbedingung 404
- Zeitstempel 450
- Zertifikat in Konfiguration schreiben 405
- Zertifikat ist ein CA-Zertifikat 97
- Zertifikatsanforderungsbeschreibung 99, 405
- Ziel 349, 351
- Ziel-IP-Adresse 399, 405, 425
- Ziel-IP-Adresse/Netzmaske 191, 204, 217, 296
- Ziel-MAC-Adresse 436
- Ziel-Port/Bereich 204, 217, 222, 238, 432
- Zieladresse/Länge 195
- Zielport 192, 296
- Zielportbereich 359
- Zielschnittstelle 261, 374
- Zielschnittstelle 195
- Zugangs-Level 95
- Zugewiesene Drahtlosnetzwerke (VSS) 165
- Zugriffsfiler 242
- Zugriffskontrolle 142, 178
- Zulässiger Hotspot-Client 430
- Zum SNMP Browser wechseln 93
- Zusammenfassend 102
- Zusätzliche, frei zugängliche Domänennamen 428
- Zusätzlicher Filter des IPv4-Datenverkehrs 294, 296
- Zweiter Verwendeter Kanal 127
- 2,4/5-GHz-Übergang 468
- Abgewiesene Clients soft/hard 468
- Aktion 188, 444, 460, 463
- Aktive Clients 468
- Aktualisierungstimer 252
- Aktuelle Ortszeit 66
- Aktueller Dateiname im Flash 444
- Als DHCP-Server 369
- Als IPCP-Server 369
- Alternative Schnittstelle, um DNS-Server zu erhalten 368
- Andere Inaktivität 354
- Angegriffener Access Point 186
- Anmeldung 472
- Ansicht 473, 474, 476
- AP gefunden 182
- AP offline 182
- AP verwaltet 182
- AP-MAC-Adresse 470, 471
- Art des Angriffs 186
- Assert-Status 476, 477
- Aushandlungsmodus 461
- Ausloggen 440
- Authentifizierung für PPP-Einwahl 92
- Authentifizierungsmethode 461
- Benachrichtigungsdienst 455
- Benutzer 440
- Benutzername 456, 472
- Beschreibung 460, 461, 463, 464, 465
- Beschreibung des Client Links 470
- BOSS 444
- Bridge-Link-Beschreibung 469, 469
- Bytes 461
- Cache-Größe 368
- Cache-Treffer 376
- Cache-Trefferrate (%) 376
- Client-MAC-Adresse 467
- CPU-Last [%] 182
- CRLs senden 325
- CTS Frames als Antwort auf RTS empfangen 465
- Datei auswählen 444
- Dateiname 444
- Datenrate Mbit/s 466, 467, 469, 469, 469, 469, 470, 471
- Datum 460
- Datum einstellen 66
- Delete the complete WLAN Controller configuration 160
- Designated Router (DR) 473
- Details 460
- DHCP-Server 160
- DNS-Anfragen 376
- DNS-Domänen-Suchliste 395
- DNS-Server 396

- Domänenname 368
- Doppelte empfangene MSDUs 465
- Dritter Zeitserver 67
- DSL-Logik 444
- Durchsatz 184
- Dynamische RADIUS-Authentifizierung 323
- E-Mail-Adresse 456
- ECDSA-Schlüsselstatus 79
- ED25519-Schlüsselstatus 79
- Empfangene DNS-Pakete 376
- Entfernte IP-Adresse 440
- Entfernte ID 461
- Entfernte IP-Adresse 460 , 461
- Entfernte MAC 469 , 469
- Entfernte Netzwerke 460
- Entfernter Port 461 , 464
- Erfolgreich beantwortete Anfragen 376
- Erfolgreich empfangene Multicast-MS-DUs 465
- Erfolgreich übertragene Multicast-MS-DUs 465
- Erreichbarkeitsprüfung 461
- Erster Zeitserver 67
- Erweiterte Route 197
- Expiry Timer 473 , 476 , 477 , 478
- Fehler 187 , 461 , 463
- Fehlerhafte Erhaltene Pakete 465
- Fertig 187
- Firewall auf Werkseinstellungen zurücksetzen 355
- Frame-Übertragungen ohne ACK 465
- Frames ohne Tag verwerfen 124
- Garbage Collection Timer 252
- Gateway 197
- Generation ID 473
- Gesamt 463
- GRE-Window-Anpassung 342
- GRE-Window-Größe 342
- Größe der Zero Cookies 323
- Hashing-Algorithmen 79
- Herstellernamen anzeigen 61 , 61
- Hold Down Timer 253
- Host für mehrere Standorte 431
- HTTPS-TCP-Port 377
- IGMP-Status 259
- IKE (Phase-1) 462
- IKE (Phase-1) SAs 461
- Image bereits vorhanden. 187
- Importieren 104 , 105
- Initial Contact Message senden 323
- Interface selection 438
- IP-Adressbereich 160
- IP-Adresse 466 , 467 , 472 , 473 , 473
- IP-Adresse des Assert Winner 476 , 477
- IP-Adresse des NetManagers 61
- IP-Adresse des Rendezvous Point 474
- IP-Adresse des Rendezvous Points 473
- IP-Adresse/Netzmaske 464
- IPSec (Phase-2) 462
- IPSec (Phase-2) SAs 461
- IPSec aktivieren 322
- IPSec über TCP 323
- IPSec-Debug-Level 322
- IPSec-Tunnel 462
- ISDN-Zeitserver 67
- Join/Prune-Status 476 , 477 , 478
- Keepalive-Periode 266
- Key Hash Payloads senden 325
- Klasse 440
- Kommunikation mit dem NetManager 61
- Komprimierung 81
- Konfiguration der automatischen Speicherung 61
- Konfigurationsschnittstelle 74
- Kontakt 61
- Läuft ab 440
- LED-Modus 61
- Level 460
- Lokale Adresse 464
- Lokale ID 461
- Lokale IP-Adresse 461

- Lokaler Port 461 , 464
- Lokales Zertifikat 377
- Loopback aktiv 202
- Löschen 186 , 197
- MAC-Adresse 464 , 466 , 468 , 471
- MAC-Adresse des Rogue Clients 186
- Manuelle IP-Adresse des WLAN-Controller 61
- Max. eingehende Kontrollverbindungen über entfernte IP-Adresse 342
- Maximale Anzahl der Accounting-Protokolleinträge 61
- Maximale Anzahl gleichzeitiger Verbindungen 78
- Maximale Anzahl der IGMP-Statusmeldungen 259
- Maximale Anzahl der Syslog-Protokolleinträge 61
- Maximale E-Mails pro Minute 455
- Maximale Gruppen 259
- Maximale Quellen 259
- Maximale SMS pro Tag 457
- Maximale TTL für negative Cacheeinträge 368
- Maximale TTL für positive Cacheeinträge 368
- Maximales Nachrichtenlevel von Systemprotokolleinträgen 61
- Mbit/s 465
- Metrik 197 , 198
- Modus 198 , 259
- Modus / Bridge-Gruppe 74
- MSDUs, die nicht übertragen werden konnten 465
- MTU 461
- Multicast-Gruppen-Adresse 473 , 474 , 475 , 476 , 476 , 477 , 478
- Multicast-Routing 256
- Nachricht 460
- Nachrichten 461
- Name der Quelldatei 444
- Name der Zieldatei 444
- NAT 464
- NAT aktiv 202
- NAT-Erkennung 461
- Negativer Cache 368
- Netzmaske 197
- Netzwerkname (SSID) 186
- Netzwerkname (SSID) 468
- Neuer Dateiname 444
- Nicht entschlüsselbare MPDUs erhalten 465
- Nicht geändert seit 463
- Nicht-Mitglieder verwerfen 124
- Nr. 198 , 460 , 463
- Pakete 461
- Passwort 456
- Passwörter und Schlüssel als Klartext anzeigen 65
- Physische Adresse 472
- PIM-Status 266
- Ping-Befehl testweise an Adresse senden 441
- Poisoned Reverse 251
- POP3-Server 456
- POP3-Timeout 456
- Port 471
- Port-STUN-Server 353
- Portweiterleitungen 202
- Positiver Cache 368
- PPTP-Inaktivität 354
- PPTP-Passthrough 202
- Präfixlänge der Multicast-Gruppe 473
- Primärer DHCP-Server 389
- Protokoll 197 , 198
- Protokollformat 452
- Protokollierte Aktionen 353
- Protokollierungslevel 81
- PVID 124
- QoS-Queue 472
- Quell-IP-Adresse 475 , 476 , 477 , 478
- Quelle 188 , 444
- Queued 472
- Rate 467 , 469 , 471
- Rauschen dBm 466 , 467 , 469 , 469 , 470 , 471
- Region 150 , 160

- Register Suppression Timer 266
- Remote-Adresse 464
- Retransmission Timer 253
- Reverse-Path-Forwarding (RPF) 474
 - , 476
- RFC 2091-Variabler Timer 251
- RFC 2453-Variabler Timer 251
- RIP-UDP-Port 251
- Route 198
- Routentimeout 252
- Routentyp 197
- RSA-Schlüsselstatus 79
- RTS Frames ohne CTS 465
- Rx-Bytes 463 , 464
- Rx-Fehler 463
- Rx-Pakete 463 , 464 , 465 , 466 , 467
 - , 469 , 469 , 470 , 471
- SAs mit dem Status der ISP-
 - Schnittstelle synchronisieren 323
- Schedule-Intervall 417
- Schnittstelle 124 , 160 , 197 , 198 ,
 - 198 , 472 , 472 , 473 , 473 , 476 ,
 - 477 , 478
- Schnittstellenbeschreibung 74
- Sekundärer DHCP-Server 389
- Senden 472
- Server-Priorität 396
- Serverfehler 376
- Shortest Path Tree 475
- Sicherheitsalgorithmus 460
- Signal 184
- Signal dBm 186 , 466
- Slave-AP-LED-Modus 160
- Slave-AP-Standort 160
- SMS-Gerät 457
- SMTP-Authentifizierung 456
- SMTP-Port 456
- SMTP-Server 456
- SNMP multicast discovery 82
- SNMP Read Community 64
- SNMP Trap Broadcasting 458
- SNMP Write Community 64
- SNMP-Listen-UDP-Port 82
- SNMP-Trap-Community 458
- SNMP-Trap-UDP-Port 458
- SNMP-Version 82
- SNR dB 467 , 471
- SNTP-Server 396
- Sofort ausloggen 440
- Speicherverbrauch [%] 182
- SSH-Dienst aktiv 78
- SSH-Port 78
- SSID 186
- Standarddeinstellungen wiederherstellen
 - 77
- Standardmäßige Routenverteilung
 - 251
- Standort 61
- Statische Black List 186
- Status 160 , 460 , 462 , 463 , 464
- Status der IPv4-Firewall 353
- STUN Handler 353
- Subsystem 460
- System als Zeitserver 67
- Systemadministrator-Passwort 64
- Systemadministrator-Passwort bestäti-
 - gen 64
- Systemlogik 444
- Systemname 61
- TCP-Inaktivität 354
- TCP-Keepalives 81
- Test-Ping-Modus 441
- Toleranzzeit beim Login 81
- Trace mode 438
- Traceroute-Adresse 442
- Traceroute-Modus 442
- Tx-Bytes 463 , 464
- Tx-Fehler 463
- Tx-Pakete 463 , 464 , 465 , 466 , 467
 - , 469 , 469 , 470 , 471
- Typ 463
- Überprüfung der Rückroute 198
- Übersicht 183
- Übertragene MPDUs 465
- UDP-Inaktivität 354
- UDP-Quellportauswahl 334
- UDP-Zielpport 334
- Ungültige DNS-Pakete 376

- Unicast MPDUs erfolgreich erhalten 465
- Unicast MSDUs erfolgreich übertragen 465
- Upstream Nachbar-IP-Adresse 474 , 474 , 475
- Upstream Join State 474 , 474 , 475
- Upstream Join Timer 474 , 474 , 475
- Upstream Override Timer 476
- Uptime 466 , 467 , 469 , 470 , 471 , 473 , 474 , 474 , 475 , 476 , 476 , 477 , 478
- URL 188 , 444
- Verbundene Clients/VSS 182
- Verschlüsselt 463
- Verschlüsselung der Konfiguration 444
- Verschlüsselungsalgorithmen 79
- Verwerfen ohne Rückmeldung 202
- Verworfen 463 , 472
- VLAN aktivieren 125
- Vollständige IPsec-Konfiguration löschen 322
- Vollständige IPv4-Filterung 353
- VSS-Beschreibung 468
- Weitergeleitet 463
- Weitergeleitete Anfragen 376
- Wert 465
- WINS-Server 368
- Wird ausgeführt 187
- WLAN Controller: VSS-Durchsatz 182
- Zeit 460
- Zeit einstellen 66
- Zeitaktualisierungsintervall 67 , 69
- Zeitaktualisierungsrichtlinie 67
- Zeitzone 66
- Zero Cookies verwenden 323
- Zertifikate und Schlüssel einschließen 444
- Zertifikatsanforderung 99
- Zertifikatsanforderungs-Payloads senden 325
- Zertifikatsanforderungs-Payloads nicht beachten 325
- Zertifikatsketten senden 325
- Ziel-IP-Adresse 197
- Zu verwendende Schnittstelle 441
- Zuerst gesehen 186 , 469
- Zuletzt gesehen 186 , 469 , 469 , 469
- Zweiter Zeitserver 67
- Adressliste 356
- Aktionen 405
- Aktive Clients 183
- Allgemein 160
- Allgemeine Statusangaben 473
- Auslöser 399
- Benachbarte APs 185
- Benachrichtigungseinstellungen 455
- Benachrichtigungsempfänger 453
- Benutzer 95 , 329
- Benutzer ausloggen 440
- Bridge-Links 148 , 469
- Cache 375
- Client Link 145
- Client Links 470
- Client-Verwaltung 184 , 468
- CRLs 104
- Datum und Uhrzeit 65
- DHCP-Konfiguration 383
- DHCP-Relay-Einstellungen 389
- Dienstliste 359
- DNS-Server 370
- DNS-Test 441
- Domänenweiterleitung 373
- Drahtlosnetzwerke (VSS) 135 , 173 , 184
- Drop-In-Gruppen 244
- Dynamische Hosts 375
- DynDNS-Aktualisierung 378
- DynDNS-Provider 380
- Einstellungen Funkmodul 126
- Firmware-Wartung 187
- Funkmodulprofile 167
- Globale DHCPv6-Optionen 395
- Globale Einstellungen 368
- GRE-Tunnel 344
- Gruppen 358 , 361
- Hosts 421

- Hotspot-Gateway 428
- HTTP 77
- HTTPS 77
- HTTPS-Server 377
- IP Pools 284 , 321 , 342
- IP-Pool-Konfiguration 382
- IP/MAC-Bindung 388
- IPSec-Peers 288
- IPSec-Statistiken 462
- IPSec-Tunnel 460
- IPv4-Filterregeln 348
- IPv4-Gruppen 355
- IPv4-Routing-Tabelle 197
- IPv4/IPv6-Filter 222
- IPv6-Routenkonfiguration 195
- IPv6-Routingtabelle 198
- ISDN-Login 77
- Konfiguration eines Allgemeinen Präfixes 200
- Konfiguration von IPv4-Routen 189
- Konfiguration von zustandsbehafteten Clients 397
- Lastverteilungsgruppen 212
- NAT-Konfiguration 202
- NAT-Schnittstellen 201
- Netzwerk-Status 465
- Nicht-schnittstellen-spezifischer Status 474
- Optionen 91 , 198 , 259 , 322 , 334 , 342 , 353 , 417 , 431 , 442 , 452
- Passwörter 64
- Phase-1-Profile 306
- Phase-2-Profile 314
- PIM-Optionen 266
- PIM-Rendezvous-Punkte 264
- PIM-Schnittstellen 262
- Ping 77
- Ping-Generator 425
- Ping-Test 441
- Portkonfiguration 124
- PPPoE 269
- PPTP 279
- PPTP-Tunnel 335
- QoS-Klassifizierung 226
- QoS-Schnittstellen/Richtlinien 228
- RADIUS 83
- Regelketten 242
- Regulierte Schnittstellen 285
- RIP-Filter 249
- RIP-Optionen 251
- RIP-Schnittstellen 247
- Rogue APs 185
- Rogue Clients 186
- Schnittstellen 74 , 109 , 424 , 452
- Schnittstellenspezifische Zustände 476
- Schnittstellenzuweisung 243 , 437
- Slave Access Points 164 , 183
- SNMP 77 , 82
- SNMP-Trap-Hosts 459
- SNMP-Trap-Optionen 458
- Special Session Handling 216
- SSH 77 , 78
- Statische Hosts 372
- Statistik 376 , 463
- Syslog-Server 449
- System 61
- Systemlizenzen 70
- Systemmeldungen 460
- Systemneustart 448
- TACACS+ 89
- Telnet 77
- Trace-Schnittstelle 438
- Traceroute-Test 442
- Tunnelprofile 326
- Verwaltung 125
- VLANs 123
- VSS 466
- Wake-on-LAN-Filter 432
- WLAN Controller 182
- WOL-Regeln 436
- XAUTH-Profile 319
- Zertifikatsliste 97
- Zertifikatsserver 105
- Zugriffsfiler 238
- Zugriffsprofile 92
- Zustandsbehaftete Clients 393
- Zustandsbehaftete Clients 397

- Administrativer Zugriff 77
- Adressen 356
- Allgemein 256
- Allgemeine IPv6-Präfixe 199
- Benachrichtigungsdienst 453
- Benutzer ausloggen 440
- Bridges 471
- Controller-Konfiguration 160
- DHCP-Server 382
- DHCPv6-Server 392
- Diagnose 441
- Dienste 358
- DNS 366
- Drop-In 244
- DynDNS-Client 377
- Factory Reset 448
- Globale Einstellungen 61
- GRE 343
- Hotspot-Gateway 426 , 471
- HTTPS 376
- IGMP 256
- Internes Protokoll 460
- IP-Accounting 451
- IP-Konfiguration 109
- IPSec 287 , 460
- Konfigurationszugriff 92
- L2TP 326
- Lastverteilung 212
- Monitoring 182
- NAT 201
- Neustart 448
- PIM 261 , 472
- PPTP 335
- QoS 222 , 472
- Real Time Jitter Control 285
- Remote Authentifizierung 83
- Richtlinien 348
- RIP 247
- Routen 189
- Scheduling 398
- Schnittstellen 355 , 463
- Schnittstellenmodus / Bridge-Gruppen
72
- SIA 459
- Slave-AP-Konfiguration 164
- SNMP 457
- Software & Konfiguration 442
- Systemprotokoll 449
- Trace 438
- Überwachung 421
- Umgebungs-Monitoring 184
- Verwaltung 150
- VLAN 123
- Wake-On-LAN 432
- Wartung 187
- Weiterleiten 260
- Wizard 152
- WLAN 126 , 465
- Zertifikate 96
- Zugriffsregeln 236
- Externe Berichterstellung 449
- Firewall 346
- LAN 109
- Multicast 254
- Netzwerk 189
- Wartung 440
- Wireless LAN 126
- Wireless LAN Controller 151
- DHCP-Client (Konfigurationsbeispiel)
389
- DHCP-Relay-Server
(Konfigurationsbeispiel) 389
- DHCP-Server (Konfigurationsbeispiel)
389
- NAT (Konfigurationsbeispiel) 209
- SIF (Konfigurationsbeispiel) 361
- #
- #1#2, #3 103
- A**
- ACCESS_ACCEPT 84
- ACCESS_REJECT 84
- ACCESS_REQUEST 84
- ACCOUNTING_START 84
- ACCOUNTING_STOP 84
- aktiv 267

- Aktive IPSec-Tunnel 60
- Aktuelle Geschwindigkeit / Aktueller Modus 107
- Arbeitsspeichernutzung 60
- Assistenten 58
- B**
- Bedienelemente 48
- Beschreibung - Verbindungsinformation
 - Uptime - Link 60
- Betriebsmodus (Aktiv) 405
- Betriebsmodus (Inaktiv) 405
- blockiert 267
- BOSS-Version 59
- C**
- CPU-Nutzung 60
- E**
- Ethernet-Ports 107
- F**
- Funkmodul1 183
- H**
- Homepage 380
- HTTPS/SSL 378
- I**
- inaktiv 267
- Internet + Einwählen 267
- IP-Version 378
- K**
- Konfigurationsbeispiel - DHCP-Client 389
- Konfigurationsbeispiel - DHCP-Relay-Server 389
- Konfigurationsbeispiel - DHCP-Server 389
- Konfigurationsbeispiel - Lastverteilung 219
- Konfigurationsbeispiel - NAT 209
- Konfigurationsbeispiel - Scheduling 417
- Konfigurationsbeispiel - SIF 361
- Konfigurationsbeispiel - Zeitgesteuerte Aufgaben 417
- Konfigurationsoberfläche aufrufen 48
- Konfigurierte Geschwindigkeit/konfigurierter Modus 107
- L**
- Lastverteilung (Konfigurationsbeispiel) 219
- Letzte gespeicherte Konfiguration 59
- Lokale Dienste 366
- M**
- Monitoring 460
- P**
- Physikalische Schnittstellen 107
- Port 107
- Portkonfiguration 107
- R**
- Routing-Protokolle 247
- ruhend 267
- S**
- Scheduling (Konfigurationsbeispiel) 417
- Schnittstelle 107
- Schnittstelle - Verbindungsinformation - Link 60
- Seriennummer 59
- Server IPv6 380
- Signal dBm (RSSI1, RSSI2, RSSI3) 467 , 469 , 469 , 470 , 471
- Status 59

Supports SSL 380
Systemdatum 59
Systemverwaltung 59

U

Uptime 59

V

VPN 287

W

Walled Network / Netzmaske 428
WAN 267
WEP-Schlüssel 1-4 139 , 146 , 175
WLANx 465

Z

Zeitgesteuerte Aufgaben
(Konfigurationsbeispiel) 417