



Benutzerhandbuch Digitalisierungsbox Premium

Betrieb mit Standardsoftware

Rechtlicher Hinweis

Gewährleistung

Änderungen in dieser Veröffentlichung sind vorbehalten.

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

Copyright © bintec elmeg GmbH

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

Open Source Software in diesem Produkt

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

GEMA

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

Inhaltsverzeichnis

Kapitel 1	Inbetriebnahme	1
1.1	Digitalisierungsbox Premium	1
1.2	Reset	5
1.3	Voreinstellungen	5
1.4	Support-Information	7
Kapitel 2	Montage	8
2.1	Anschluss von Endgeräten	8
2.2	Reset Taster	8
2.3	Wandmontage	8
2.4	Pin-Belegungen	9
Kapitel 3	Grundkonfiguration	12
3.1	Vorbereitungen	12
3.2	Konfiguration des Systems	14
3.3	Internetverbindung einrichten	15
3.4	Benutzerzugang	16
3.5	Softwareaktualisierung Digitalisierungsbox Premium	16
Kapitel 4	Zugang und Konfiguration	18
4.1	Zugang über LAN	18
4.2	Konfiguration	18
Kapitel 5	Assistenten	25
Kapitel 6	Systemverwaltung	26
6.1	Status	26
6.2	Globale Einstellungen	28
6.3	Schnittstellenmodus / Bridge-Gruppen	35
6.4	Administrativer Zugriff	37
6.5	Remote Authentifizierung	38
6.6	Konfigurationszugriff	43
6.7	Zertifikate	48

Kapitel 7	Physikalische Schnittstellen	58
7.1	Ethernet-Ports	58
7.2	ISDN-Ports	60
7.3	DSL-Modem	62
Kapitel 8	LAN	64
8.1	IP-Konfiguration	64
8.2	VLAN	74
Kapitel 9	Wireless LAN	78
9.1	WLAN.	78
9.2	Verwaltung	89
9.3	Konfiguration.	90
Kapitel 10	Wireless LAN Controller	93
10.1	Wizard	93
10.2	Controller-Konfiguration	97
10.3	Slave-AP-Konfiguration	99
10.4	Monitoring	112
10.5	Umgebungs-Monitoring	117
10.6	Wartung.	119
Kapitel 11	Netzwerk	122
11.1	Routen	122
11.2	Allgemeine IPv6-Präfixe	131
11.3	NAT.	132
11.4	Lastverteilung	140
11.5	QoS	148
11.6	Zugriffsregeln	158
Kapitel 12	Multicast.	166
12.1	Allgemein	167
12.2	IGMP	167
12.3	Weiterleiten	170

Kapitel 13	WAN	172
13.1	Internet + Einwählen	172
13.2	ATM	187
13.3	Real Time Jitter Control	196
Kapitel 14	VPN	198
14.1	IPSec	198
Kapitel 15	Firewall	227
15.1	Richtlinien	228
15.2	Schnittstellen.	234
15.3	Adressen	236
15.4	Dienste	237
15.5	Konfiguration.	240
Kapitel 16	VoIP	244
16.1	Application Level Gateway	244
16.2	Einstellungen	247
16.3	Media Gateway	262
16.4	RTSP	268
Kapitel 17	Lokale Dienste	270
17.1	DNS	270
17.2	HTTPS	278
17.3	DynDNS-Client	279
17.4	DHCP-Server	282
17.5	Scheduling.	291
17.6	Überwachung	306
17.7	UPnP	310
Kapitel 18	Wartung	313
18.1	Diagnose	313
18.2	Software &Konfiguration	315
18.3	Neustart	318

Kapitel 19	Externe Berichterstellung.	320
19.1	Systemprotokoll	320
19.2	IP-Accounting	322
19.3	Benachrichtigungsdienst	323
Kapitel 20	Monitoring	328
20.1	Internes Protokoll	328
20.2	IPSec	328
20.3	ISDN/Modem	331
20.4	Schnittstellen.	332
20.5	WLAN.	334
20.6	Bridges	339
20.7	QoS	340
	Index	341

Kapitel 1 Inbetriebnahme

1.1 Digitalisierungsbox Premium

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

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

1.1.1 Aufstellen und Anschließen

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

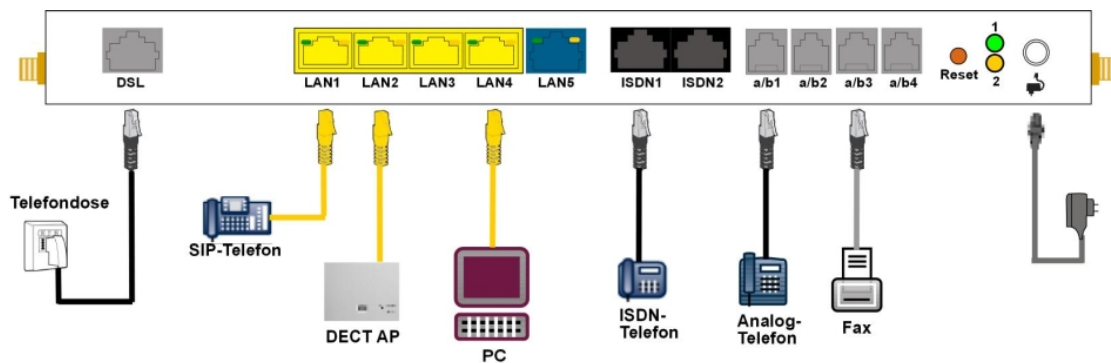


Abb. 1: Basisszenario **Digitalisierungsbox Premium**



Achtung

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



Achtung

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

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

- (1) **Montage**
Um einen störungsfreien Betrieb zu gewährleisten, sollte die **Digitalisierungsbox Premium** aufrecht an einer Wand oder gut belüftet in einem Netzwerkschrank montiert sein (lesen Sie bitte aufmerksam das Kapitel [Montage](#) auf Seite 8).
- (2) **Netzanschluss**
Schließen Sie den Netzanschluss des Geräts mit dem mitgelieferten Steckernetzgerät an eine 230 V~ Steckdose an.
- (3) **Antennen**
Schrauben Sie die mitgelieferten Antennen auf die dafür vorgesehenen Anschlüsse.
- (4) **DSL**
Verbinden Sie den Anschluss **DSL** über das graue Kabel an die TAE-Buchse der Telefondose an.
- (5) **ISDN-Endgeräte**
Schließen Sie ein ISDN-Telefon an den internen ISDN-Anschluss der **Digitalisierungsbox Premium** an.

- (6) Analoge Endgeräte
Verbinden Sie Ihre analogen Endgeräte an den analogen Anschlüssen (a/b1 - a/b4). Verwenden Sie dazu das dem Endgerät beigegefügte Kabel.
- (7) SIP-Telefone
Schliessen Sie Ihre SIP-Telefone an die 10/100/1000 Base-T Ethernet-Schnittstellen an. Einen letzten Schritt müssen Sie am PC ausführen.
- (8) PC
Schließen Sie einen geeigneten PC über ein Ethernet-Kabel an eine der Ethernet-Schnittstellen der **Digitalisierungsbox Premium** an. Sollten Probleme bei der Verbindung zwischen PC und **Digitalisierungsbox Premium** auftreten, lesen Sie bitte die entsprechenden Kapitel zur Grundkonfiguration.
- (9) VoIP
Für einen reinen IP-Anschluss ohne ISDN verwenden Sie die vom Provider bereitgestellte Anleitung.



Hinweis

Mit der "**Automatischen Konfiguration**" der Telekom wird Ihr Gerät automatisch eingerichtet (siehe [Automatische Konfiguration](#) auf Seite 12).

1.1.2 Anschlüsse

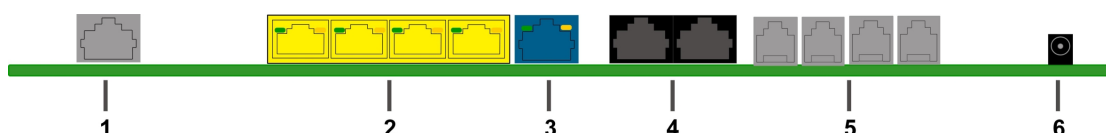


Abb. 2: Anschlüsse

1	DSL-Schnittstelle Annex B/J
2	10/100/1000 Base-T Ethernet-Schnittstellen (LAN 1 - LAN4)
3	Ethernet-WAN-Schnittstelle (LAN5)
4	Schnittstelle für ISDN-Endgeräte (ISDN1, ISDN2)
5	Interne Schnittstelle für analoge Endgeräte (a/b1 - a/b4)
6	Buchse für das Steckernetzteil

1.1.3 Anschlüsse (seitlich)

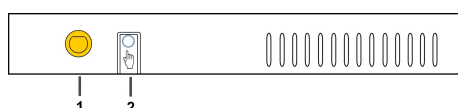


Abb. 3: Seitliche Anschlüsse

1	Antennenanschluss
2	Funktionstaste (ohne Funktion)

1.1.4 Montagewinkel

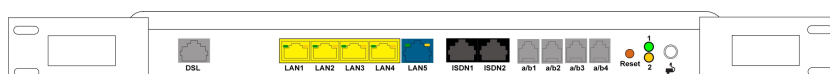



Abb. 4: Montagewinkel

Aufgrund der Platzierung der Geräte im Netzwerkschrank, empfiehlt es sich auf abgesetzte Antennen zurückzugreifen. Montieren Sie die Montagewinkel mit den im Set beiliegenden Schrauben am Gehäus-

se. Die Montagewinkel und die Schrauben sind als Zubehör erhältlich (Artikelnummer MN40285514).



Hinweis

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

1.1.5 LEDs

Anhand der LEDs können Sie den Status Ihres Geräts ablesen.

Die LEDs der **Digitalisierungsbox Premium** sind folgendermaßen angeordnet:

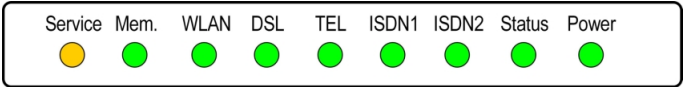


Abb. 5: LEDs

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

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

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

Ethernet-LEDs

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

1.1.6 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

Produktname	Kabelsätze/Sonstiges	Dokumentation
Digitalisierungsbox Premium	ein Ethernet LAN-Kabel (gelb)	Installationsposter
	ein Ethernet WAN-Kabel (blau)	Sicherheitshinweise
	ein DSL-Kabel (grau)	
	zwei FSX-TAE-Adapter (schwarz)	
	ein Netzteil	
	zwei WiFi-Antennen	

1.1.7 Allgemeine Produktmerkmale

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

Allgemeine Produktmerkmale Digitalisierungsbox Premium

Eigenschaft	
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	328 x 193 x 44 mm
Gewicht	ca. 900 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 1800 g
Speicher	128 MB SDRAM,

Eigenschaft	
LEDs	19 (8 x Funktion, 1 x Service, 5x2 Ethernet)
Leistungsaufnahme Gerät	max. 30 W 12 V DC
Spannungsversorgung	12 V DC 2,5 A
Umweltanforderungen:	
Lagertemperatur	-20 °C bis +70 °C
Betriebstemperatur	+5 °C bis +40 °C
Relative Luftfeuchtigkeit	max. 85 %
Raumklassifizierung	Nur in trockenen Räumen betreiben
Verfügbare Schnittstellen:	
DSL-Schnittstelle	Internes DSL-Modem
Ethernet IEEE 802.3 LAN (4-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100/1000 MBit/s, autosensing, MDIX
ISDN-Schnittstellen	2 interne ISDN-Schnittstellen, ISDN-Terminierung
FXS	4 FXS-Schnittstellen (a/b1 - a/b4)
Vorhandene Buchsen:	
WLAN Antennen	R-SMA-Buchsen
Ethernet-Schnittstellen 1 - 4 (LAN)	RJ45-Buchse
Ethernet-Schnittstelle 5 (WAN)	RJ45-Buchse
ISDN-Schnittstelle (ISDN1, ISDN2)	RJ45-Buchse
FXS-Schnittstelle (a/b1 bis a/b4)	RJ12-Buchse
DSL-Schnittstelle	RJ45-Buchse
Hohlsteckerbuchse für Stromversorgung	

1.2 Reset

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

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

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

1.3 Voreinstellungen

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

**Hinweis**

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

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

Konfigurationsoberfläche

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

- **IP-Adresse:** *192.168.2.1*
- **Netzmaske:** *255.255.255.0*

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

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

**Hinweis**

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

Betriebsmodus wählen

Bei der **Digitalisierungsbox Premium** haben Sie die Möglichkeit zwischen den Betriebsmodus als Telefonanlage und den Betriebsmodus als Media Gateway zu wählen.

Fall 1: Wenn das Passwort noch nicht geändert worden ist, haben Sie nach dem Login die Möglichkeit den **Betriebsmodus** zu wählen.

Fall 2: Wenn das Passwort schon geändert ist, ist das Gerät ab Werk als Telefonanlage konfiguriert. Sie können im Menü **Assistenten+Erste Schritte->Betriebsmodus** den **Betriebsmodus** ändern. Beachten Sie, dass dann nicht mehr alle Leistungsmerkmale zur Verfügung stehen. Die Montage und die Grundkonfiguration sind identisch.

**Achtung**

Beim Umschalten von Telefonanlage auf Media Gateway oder von Media Gateway auf Telefonanlage, führt das Gerät einen Factory Reset durch. Das bedeutet, dass das Gerät in den Auslieferungszustand versetzt wird. Die Konfiguration wird gelöscht und alle Passwörter werden zurückgesetzt.

Software-Update

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt.

Dank der "**Automatischen Konfiguration**" der Telekom wird die Systemsoftware Ihres Geräts auf dem neuesten Stand gehalten (siehe [Automatische Konfiguration](#) auf Seite 12).

Wie Sie den Softwarestand Ihres Geräts prüfen und ggf. eine Aktualisierung selbst durchführen, wird im **Handbuch-Kapitel „Wartung“** beschrieben.

1.4 Support-Information

Ergänzende Beratung zu Ihrer Digitalisierungsbox erhalten Sie während der üblichen Geschäftszeiten unter der kostenfreien Rufnummer 0800 330 1300 oder unter 0800 330 2870 (für Großkunden). Weitere Hinweise finden Sie auch im Internet unter <http://hilfe.telekom.de>. Vermuten Sie eine Störung Ihres Anschlusses, wenden Sie sich bitte unter der entsprechenden Nummer an den Technischen Kundendienst oder informieren Sie sich unter <http://hilfe.telekom.de>.

Kapitel 2 Montage



Warnung

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



Achtung

Um einen störungsfreien Betrieb zu gewährleisten, sollte die **Digitalisierungsbox Premium** aufrecht an einer Wand oder gut belüftet in einem Netzwerkschrank montiert sein. Das Gerät darf keiner direkten Sonneneinstrahlung oder anderen Wärmequellen ausgesetzt sein. Beachten Sie auch die einzuhaltenden Abstände (siehe [Wandmontage](#) auf Seite 8).

2.1 Anschluss von Endgeräten

2.1.1 Interner ISDN-Anschluss

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

2.1.2 Terminierung der ISDN-Schnittstellen

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

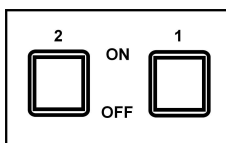


Abb. 6: Schalter für die Terminierung

2.2 Reset Taster

An der Anschlussseite des Geräts befindet sich der Reset-Taster, mit dem Sie einen Neustart des Geräts erzwingen oder den Auslieferungszustand wieder herstellen können (siehe [Reset](#) auf Seite 5).

2.3 Wandmontage

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

- (1) Suchen Sie einen Montageort aus, der max. 1,5 Meter von einer 230 V ~ Netzsteckdose und 2,5 Meter vom Übergabepunkt des Netzbetreibers entfernt ist.
- (2) Um eine gegenseitige Beeinträchtigung auszuschließen, montieren Sie das Gerät nicht in unmittelbarer Nähe von elektronischen Geräten wie z. B. HiFi-Geräten, Bürogeräten oder Mikrowellengeräten. Vermeiden Sie auch einen Aufstellort in der Nähe von Wärmequellen, z. B. Heizkörpern oder in feuchten Räumen.

- (3) Halten Sie die Abstände ein, die auf der Rückseite des Geräts eingeprägt sind.
- (4) Markieren Sie die Bohrlöcher an der Wand.
- (5) Überprüfen Sie die feste Auflage aller Befestigungspunkte der **Digitalisierungsbox Premium** an der Wand. Vergewissern Sie sich, dass im Bereich der markierten Bohrlöcher keine Versorgungsleitungen, Kabel o. ä. verlegt sind.
- (6) Bohren Sie die Befestigungslöcher an den markierten Stellen (bei Montage mit den Dübeln verwenden Sie einen 5 mm Steinbohrer). Setzen Sie die Dübel ein.
- (7) Schrauben Sie die beiden Schrauben so ein, dass zwischen Schraubenkopf und Wand noch ein Abstand von ca. 5 mm verbleibt.
- (8) Hängen Sie die **Digitalisierungsbox Premium** mit den rückseitigen Halterungen von oben hinter den Schraubenköpfen ein.
- (9) Installieren Sie, wenn erforderlich, die Anschlussdosen für die Endgeräte. Verbinden Sie die Installation der Anschlussdosen mit der des Geräts. Die Anschlussdosen dienen der festen Installation, beispielsweise im Flur. Wenn diese installiert sind, werden die Anschlusskabel mit den Anschlüssen des Geräts verbunden.
- (10) Stecken Sie die Anschlüsse der Endgeräte in die Anschlussdosen.
- (11) Verbinden Sie die **Digitalisierungsbox Premium** mit dem externen xDSL-Anschluss. Sie können dazu so verfahren, wie auf dem beigelegten Installationsposter beschrieben.
- (12) Stecken Sie das Steckernetzgerät in die 230 V~ Steckdose.
- (13) Stecken Sie den Hohlstecker des Steckernetzgeräts in die entsprechende Buchse an Ihrem Gerät.
- (14) Sie können das Gerät in Betrieb nehmen.

2.4 Pin-Belegungen

2.4.1 Ethernet-Schnittstellen

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

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

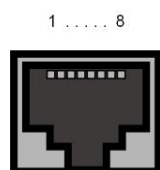


Abb. 7: Ethernet-10/100/1000 Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

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

2.4.2 ISDN-Schnittstelle

Der Anschluss erfolgt über eine RJ45-Buchse:

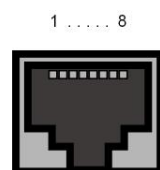


Abb. 8: ISDN-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

2.4.3 Analoge Schnittstellen (FXS / a/b)

Die Endgeräte werden an die a/b-Schnittstellen (RJ12-Buchse) mit einem RJ11-Stecker angeschlossen.

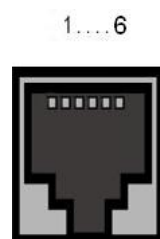


Abb. 9: a/b-Schnittstelle (RJ12)

Die Pin-Zuordnung für die a/b-Schnittstelle (RJ12-Buchse) ist wie folgt:

RJ12-Buchse für FXS-Anschluss

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	FXS
4	FXS
5	Nicht genutzt
6	Nicht genutzt

2.4.4 xDSL-Schnittstelle

Die **Digitalisierungsbox Premium** verfügt über eine xDSL-Schnittstelle. Die xDSL-Schnittstelle wird mittels eines RJ45-Steckers verbunden.

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

1 8

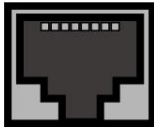


Abb. 10: xDSL-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für xDSL-Anschluss

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

Kapitel 3 Grundkonfiguration

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

3.1 Vorbereitungen

Ihr Gerät ist werksseitig als DHCP-Server eingerichtet, es übermittelt also PCs in Ihrem LAN, die über keine IP-Konfiguration verfügen, alle für eine Verbindung notwendigen Einstellungen. Wie Sie den PC, mit dem Sie die Grundkonfiguration durchführen wollen, für den automatischen Bezug einer IP-Konfiguration einrichten, ist in [PC einrichten](#) auf Seite 14 beschrieben.



Hinweis

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

3.1.1 Automatische Konfiguration

Die Automatische Konfiguration ist ein Service für Kunden der Telekom, den Sie mit Ihrer **Digitalisierungsbox Premium** nutzen können.

Verbinden Sie die **Digitalisierungsbox Premium** mit dem Stromnetz. Schließen Sie die Kabel an die dafür vorgesehenen Dosen/Buchsen an. Warten Sie, bis die Service-LED nicht mehr leuchtet.

Starten Sie einen Internet-Browser, geben Sie www.telekom.de in die Adresszeile ein und bestätigen Sie mit der Eingabetaste. Sie werden auf die Autokonfigurationsseite der Telekom weitergeleitet.

Geben Sie Ihre Zugangskennung und Ihr Passwort ein und klicken Sie auf **Konfiguration starten**. Während der Konfiguration leuchtet die Service-LED. Warten Sie, bis Sie die Bestätigung angezeigt bekommen, dass die Konfiguration erfolgreich war. Die Service-LED ist nun aus.

3.1.2 Systemsoftware

Das Gerät wird mit der zum Zeitpunkt der Produktion aktuellen Systemsoftwareversion betrieben. Die Systemsoftware wird fortwährend weiterentwickelt, um die Sicherheit und Funktionsvielfalt des Geräts zu erhöhen. Dank der "**Automatischen Konfiguration**" der Telekom wird die Systemsoftware Ihres Gerätes auf dem neuesten Stand gehalten (siehe [Automatische Konfiguration](#) auf Seite 12).

Alternativ können Sie eine Software-Aktualisierung im Menü **Wartung->Software & Konfiguration->Optionen** vornehmen. Eine Beschreibung der Vorgehensweise finden Sie in [Softwareaktualisierung Digitalisierungsbox Premium](#) auf Seite 16.

3.1.3 System-Voraussetzungen

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

- geeignetes Betriebssystem (Windows, Linux, MAC OS)
- ein Web-Browser (Internet Explorer, Firefox, Chrome) in der jeweils aktuellen Version
- installierte Netzwerkkarte (Ethernet)
- installiertes TCP/IP-Protokoll
- hohe Farbanzeige für die korrekte Darstellung der Grafiken

3.1.4 Daten sammeln

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

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

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

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

Grundkonfiguration

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

Netzwerkeinstellungen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	192.168.2.1	
Netzmaske Ihres Gateways	255.255.255.0	

SIP-Provider

Zugangsdaten	Beispielwert	Ihre Werte
Beschreibung	Geben Sie den Namen Ihres SIP-Providers an, z.B. <i>Telekom</i> .	
Authentifizierungsname/Benutzername	Geben Sie Ihre ID ein, z.B. Ihre Email-Adresse	
Passwort	Geben Sie Ihr Passwort ein, das Sie vom SIP-Provider erhalten haben.	
Registrar	Geben Sie den entsprechenden Registrar ein, z. B. <i>tel.t-online.de</i> .	
Rufnummer	z. B. 123456	

Daten für den Internetzugang über xDSL

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

3.1.5 PC einrichten

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

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

TCP/IP-Protokoll prüfen

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

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

TCP/IP-Protokoll installieren

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

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

Windows PC als DHCP-Client konfigurieren

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

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

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



Hinweis

Zur Konfiguration können Sie nun die Konfigurationsoberfläche aufrufen, indem Sie in einem unterstützten Browser die vorkonfigurierte IP-Adresse Ihres Gerätes eingeben (192.168.2.1) und sich mit den voreingestellten Anmeldedaten (**User:** *admin*, **Password:** *admin*) anmelden.

3.2 Konfiguration des Systems

3.2.1 Systempasswort ändern

Alle Geräte werden mit gleichen Benutzernamen und Passwörtern ausgeliefert. Nach dem ersten Login werden Sie daher aufgefordert, ein sicheres Passwort einzugeben. Bitte beachten Sie folgende Regeln für sichere Passwörter:

- Das Passwort muss mindestens acht Zeichen lang sein.
- Nehmen Sie Zeichen aus mindestens drei der folgenden vier Zeichengruppen:
 - Kleinbuchstaben [a-z]
 - Großbuchstaben [A-Z]
 - Zahlen [0-9]
 - Sonderzeichen.

**Hinweis**

Drücken Sie am Ende des Konfigurationsvorgangs die Schaltfläche **Konfiguration speichern**! Ansonsten geht auch das neue sichere Passwort nach einem Neustart verloren.

3.2.2 Netzwerkeinstellung (LAN)

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

3.2.3 SIP-Provider eintragen

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

3.3 Internetverbindung einrichten

Sie können mit Ihrem Gerät eine Internetverbindung aufbauen.

3.3.1 Internetverbindung über das interne VDSL-Modem

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

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

3.3.2 Andere Internetverbindungen

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

3.3.3 Konfiguration prüfen

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

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

- (1) Testen Sie die Verbindung von einem beliebigen Gerät im lokalen Netzwerk zum Gerät. Klicken Sie im Windows-Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihres Geräts ein (z. B. `192.168.2.1`). Es erscheint ein Fenster mit dem Hinweis "Antwort von...".
- (2) Testen Sie den Internetzugang, indem Sie im Internet Browser <http://www.telekom.de> eingeben.



Hinweis

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

3.4 Benutzerzugang

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



Hinweis

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

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

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

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

3.5 Softwareaktualisierung Digitalisierungsbox Premium

Die Funktionsvielfalt der **Digitalisierungsbox Premium** wird permanent erweitert. Dank der "**Automatischen Konfiguration**" der Telekom wird die Systemsoftware Ihres Gerätes auf dem neuesten Stand gehalten (siehe [Automatische Konfiguration](#) auf Seite 12).

Alternativ kann die Softwareaktualisierung über das **GUI** vorgenommen werden. Voraussetzung für ein automatisches Update ist eine bestehende Internetverbindung.

Gehen Sie folgendermaßen vor:

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

Optionen

Aktuell Installierte Software	
BOSS	V.10.1 Rev. 2 IPv6, IPSec, MGW from 2015/01/23 00:00:00
Systemlogik	1.4
Optionen zu Software und Konfiguration	
Aktion	Systemsoftware aktualisieren ▼
Quelle	Aktuelle Software vom Update-Server ▼

Start

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

**Achtung**

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

Kapitel 4 Zugang und Konfiguration

4.1 Zugang über LAN

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

4.1.1 HTTP/HTTPS

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

- `http://192.168.2.1`

oder

`https://192.168.2.1`

4.2 Konfiguration

Die Konfiguration wird mit der HTML-Konfigurationsoberfläche durchgeführt.

4.2.1 Konfigurationsoberfläche

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

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

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

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen						
Systeminformationen						
Uptime	0 Tag(e) 0 Stunde(n) 7 Minute(n)					
Systemdatum	Mittwoch, 08 Mär 2000, 22:31:34					
Seriennummer	TO2CBA014450029					
BOSS-Version	V.10.1 Rev. 2 IPv6, IPSec, MGW from 2015/01/23 00:00:00					
Letzte gespeicherte Konfiguration	Mittwoch, 08 Mär 2000, 22:24:27					
Ressourceninformationen						
CPU-Nutzung	0%					
Arbeitsspeichernutzung	35.6/127.9 MByte (27%)					
Interner Speicher	0.057/3.963 GByte (1%)					
ISDN Verwendung Intern	0 / 4 B-Kanäle					
Aktive Sitzungen (SIF, RTP, etc....)	0					
Aktive IPSec-Tunnel	0 / 0					
Module						
DSP-Modul	LANTIQ (0/5)					
Physikalische Schnittstellen						
Schnittstelle	Verbindungsinformation	Link				
en1-4	192.168.0.254 255.255.255.0					
en1-0	br0:10.0.0.164 255.0.0.0					
WLAN1	Access-Point / Verwendeter Kanal 6 / 0 Clients					
bri-0	Nicht konfiguriert					
bri-1	Nicht konfiguriert					
fxs4-0	Konfiguriert					
fxs4-1	Konfiguriert					
fxs4-2	Konfiguriert					
fxs4-3	Konfiguriert					
VDSL	<table border="1"> <tr> <td>0</td> <td>kbit/s Downstream</td> </tr> <tr> <td>0</td> <td>kbit/s Upstream</td> </tr> </table>	0	kbit/s Downstream	0	kbit/s Upstream	
0	kbit/s Downstream					
0	kbit/s Upstream					
WAN-Schnittstellen						
Beschreibung	Verbindungsinformation	Link				
Initial_Contact						

Weiterführende Produkt- und Serviceinformationen finden Sie unter: <http://hilfe.telekom.de>

Abb. 11: Konfigurationsoberfläche Startseite

4.2.1.1 Die Konfigurationsoberfläche aufrufen

- (1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind.
- (2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten.
- (3) Öffnen Sie einen Webbrowser.
- (4) Geben Sie `http://192.168.2.1` in das Adressfeld des Webbrowsers ein.
- (5) Geben Sie in das Feld **User** `admin` und in das Feld **Password** `admin` ein und klicken Sie auf **LOGIN**.

Sie werden zur Änderung des Administrator-Passworts aufgefordert. Ändern Sie das Login-Passwort.

Sie befinden sich nun im Statusmenü der Konfigurationsoberfläche Ihres Geräts.

4.2.1.2 Bedienelemente

Fenster der Konfigurationsoberfläche

Das Fenster der Konfigurationsoberfläche ist in drei Bereiche geteilt:

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

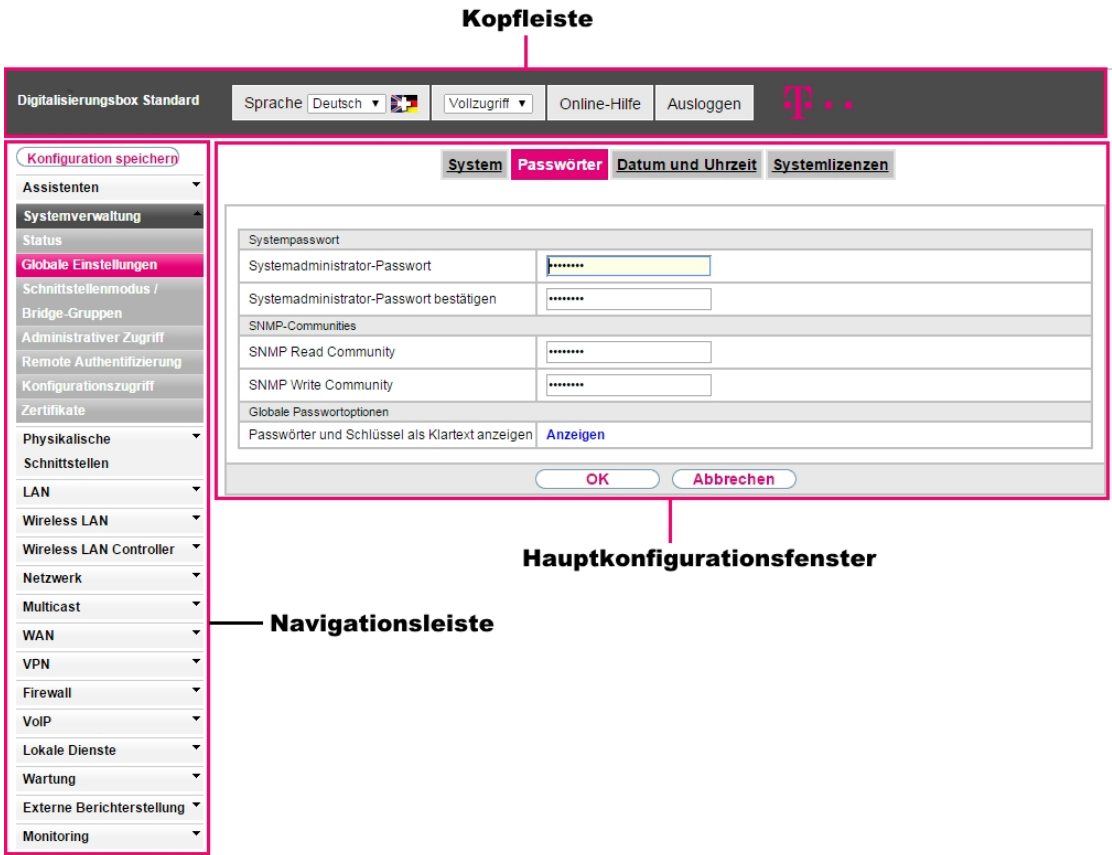


Abb. 12: Bereiche der Konfigurationsoberfläche

Kopfleiste

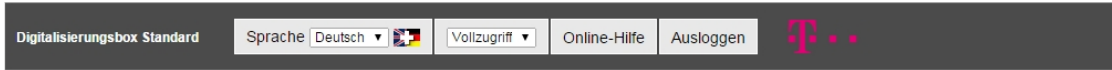


Abb. 13: Konfigurationsoberfläche Kopfleiste

Konfigurationsoberfläche Kopfleiste

Menü	Funktion
<div>Sprache: Deutsch</div>	Sprache: Wählen Sie in dem Dropdown-Menü 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>English</i> .
<div>Ansicht: Vollzugriff</div>	Ansicht: Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl steht <i>Vollzugriff</i> , <i>Experte</i> und <i>Benutzer</i> . Auch den Schnellstart können Sie von hier aus erneut aufrufen.
<div>Online-Hilfe</div>	Online-Hilfe: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Die Beschreibung des Untermenüs, in dem Sie sich gerade befinden, wird angezeigt.
<div>Ausloggen</div>	Ausloggen: Wenn Sie die Konfiguration beenden möchten, klicken Sie auf diese Schaltfläche, um sich von Ihrem Gerät abzumelden. Es wird ein Fenster geöffnet, in dem Ihnen folgende Optionen angeboten werden: <ul style="list-style-type: none">mit der Konfiguration fortfahren,die Konfiguration speichern und das Fenster schließen,die Konfiguration ohne Speichern verlassen.

Navigationsleiste



Abb. 14: Konfiguration speichern Schaltfläche

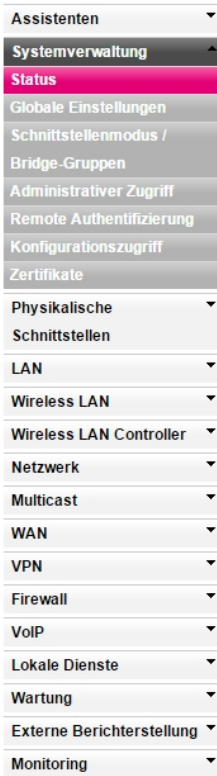


Abb. 15: Menüs

Über der Navigationsleiste ist die Schaltfläche **Konfiguration speichern** zu finden. Wenn Sie eine aktuelle Konfiguration speichern, können Sie diese als Start-Konfiguration speichern oder Sie können zusätzlich die vorhergehende Boot-Konfiguration als Backup archivieren. Wenn Sie auf die Schaltfläche **Konfiguration speichern** klicken, erscheint die Frage: "Möchten Sie die aktuelle Konfiguration wirklich als Boot-Konfiguration speichern?"

Die Navigationsleiste enthält weiterhin die Hauptkonfigurationsmenüs und deren Untermenüs. Klicken Sie auf das gewünschte Hauptmenü. Es öffnet sich das jeweilige Untermenü. Wenn Sie auf das gewünschte Untermenü klicken, wird der gewählte Eintrag in roter Schrift angezeigt. Alle anderen Untermenüs werden geschlossen. So können Sie stets mit einem Blick erkennen, in welchem Untermenü Sie sich befinden.

Hauptkonfigurationsfenster





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

Konfigurationselemente







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

Schaltflächen


Schaltfläche	Funktion
Übernehmen	Aktualisiert die Ansicht.
Abbrechen	Wenn Sie einen neu konfigurierten Listeneintrag nicht sichern wollen, machen Sie diesen und die evtl. getätigten Einstellungen durch Abbre-




Schaltfläche	Funktion
	chen rückgängig.
	Bestätigt die Einstellungen eines neuen Eintrags und die Parameteränderungen in einer Liste.
	Startet die konfigurierte Aktion sofort.
	Ruft das Untermenü zum Anlegen eines neuen Eintrags auf.
	Fügt einen Eintrag zu einer internen Liste hinzu.

Symbole

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

Listenoptionen

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

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


Automatisches Aktualisierungsintervall Sekunden 

Abb. 16: Konfiguration des Aktualisierungsintervalls




Ansicht pro Seite   Filtern in Keiner ▼ gleich ▼ 

Abb. 17: Liste filtern

Struktur der Konfigurationsmenüs

Die Menüs enthalten folgende Grundstrukturen:





Menüstruktur

Menü	Funktion
Basis-Konfigurationsmenü / Liste	<p>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.</p> <p>Das Menü enthält entweder eine Liste aller konfigurierten Einträge oder die Grundeinstellungen für die jeweilige Funktion.</p>
Untermenü 	<p>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.</p>
Untermenü 	<p>Klicken Sie auf diese Schaltfläche, um den bestehenden Listeneintrag zu bearbeiten. Sie gelangen in das Konfigurationsmenü.</p>
Menü 	<p>Klicken Sie auf diesen Reiter, um erweiterte Konfigurationsoptionen anzuzeigen.</p>

Für die Konfiguration stehen folgende Optionen zur Verfügung:


Konfigurationselemente

Menü	Funktion
Eingabefelder	<p>z. B. leeres Textfeld</p> <div><input type="text"/></div> <p>Textfeld mit verdeckter Eingabe</p> <div><input type="password"/></div> <p>Geben Sie entsprechende Daten ein.</p>
Radiobuttons	<p>z. B.</p> <div><input type="checkbox"/> IP-Adressmodus <input checked="" type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen</div>

Menü	Funktion												
	Wählen Sie die entsprechende Option aus.												
Checkboxes	<p>z. B. Aktivieren durch Auswahl der Checkbox</p> <div><input checked="" type="checkbox"/> Aktiviert</div> <p>Auswahl verschiedener möglicher Optionen</p> <table><tr><td>Verschlüsselungsalgorithmen</td><td><input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256</td></tr><tr><td>Hashing-Algorithmen</td><td><input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD 160</td></tr></table>	Verschlüsselungsalgorithmen	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256	Hashing-Algorithmen	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD 160								
Verschlüsselungsalgorithmen	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256												
Hashing-Algorithmen	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD 160												
Dropdown-Menüs	<p>z. B.</p> <div><div>Vollständige automatische Aushandlung ▼</div><div>Vollständige automatische Aushandlung ▼</div><div>Vollständige automatische Aushandlung ▼</div><div>Vollständige automatische Aushandlung ▼</div></div> <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> <table><tr><td>Entfernte IP-Adresse</td><td>Netzmaske</td><td>Metrik</td><td></td></tr><tr><td><input type="text"/></td><td><input type="text"/></td><td>1 ▼</td><td></td></tr><tr><td colspan="4"><input type="button" value="Hinzufügen"/></td></tr></table> <p>Klicken Sie auf die Schaltfläche <input type="button" value="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>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	1 ▼		<input type="button" value="Hinzufügen"/>			
Entfernte IP-Adresse	Netzmaske	Metrik											
<input type="text"/>	<input type="text"/>	1 ▼											
<input type="button" value="Hinzufügen"/>													

Darstellung von Optionen, die nicht zur Verfügung stehen

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




Wichtig

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

4.2.1.3 Menüs

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



Hinweis

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

Kapitel 5 Assistenten

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

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

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

Kapitel 6 Systemverwaltung

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

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

6.1 Status

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

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

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



Hinweis

Unterbrechen Sie weder die Internetverbindung noch die Stromversorgung.

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

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

Sie erhalten einen Überblick über folgende Daten:

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

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



Achtung

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

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen						
Systeminformationen						
Uptime	0 Tag(e) 0 Stunde(n) 7 Minute(n)					
Systemdatum	Mittwoch, 08 Mär 2000, 22:31:34					
Seriennummer	TO2CBA014450029					
BOSS-Version	V.10.1 Rev. 2 IPv6, IPSec, MGW from 2015/01/23 00:00:00					
Letzte gespeicherte Konfiguration	Mittwoch, 08 Mär 2000, 22:24:27					
Ressourceninformationen						
CPU-Nutzung	0%					
Arbeitsspeichernutzung	35.6/127.9 MByte (27%)					
Interner Speicher	0.057/3.963 GByte (1%)					
ISDN Verwendung Intern	0 / 4 B-Kanäle					
Aktive Sitzungen (SIF, RTP, etc....)	0					
Aktive IPSec-Tunnel	0 / 0					
Module						
DSP-Modul	LANTIQ (0/5)					
Physikalische Schnittstellen						
Schnittstelle	Verbindungsinformation	Link				
en1-4	192.168.0.254 255.255.255.0					
en1-0	br0:10.0.0.164 255.0.0.0					
WLAN1	Access-Point / Verwendeter Kanal 6 / 0 Clients					
bri-0	Nicht konfiguriert					
bri-1	Nicht konfiguriert					
fxs4-0	Konfiguriert					
fxs4-1	Konfiguriert					
fxs4-2	Konfiguriert					
fxs4-3	Konfiguriert					
VDSL	<table border="1"> <tr> <td>0</td> <td>kbit/s Downstream</td> </tr> <tr> <td>0</td> <td>kbit/s Upstream</td> </tr> </table>	0	kbit/s Downstream	0	kbit/s Upstream	
0	kbit/s Downstream					
0	kbit/s Upstream					
WAN-Schnittstellen						
Beschreibung	Verbindungsinformation	Link				
Initial_Contact						

Weiterführende Produkt- und Serviceinformationen finden Sie unter: <http://hilfe.telekom.de>

Abb. 18: Systemverwaltung -> Status

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

Felder im Menü Systeminformationen

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

Felder im Menü Ressourceninformationen

Feld	Wert
CPU-Nutzung	Zeigt die CPU-Auslastung in Prozent an.
Arbeitsspeichernutzung	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtarbeitsspeicher in MByte an. Die Auslastung wird außerdem in Klammern in Prozent angezeigt.
Interner Speicher	Zeigt den Status eines internen Speichers und die Speichergröße in GByte oder MByte an.

Feld	Wert
ISDN Verwendung Intern	Zeigt die Anzahl der aktiven B-Kanäle und die maximale Anzahl an zur Verfügung stehenden B-Kanäle für interne Verbindungen.
Aktive Sitzungen (SIF, RTP, etc...)	Zeigt die Summe aller SIF, TDRC und IP-Lastverteilung Sessions an.
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Felder im Menü Module

Feld	Wert
DSP-Modul	Zeigt den Typ des DSP-Moduls und die aktuell belegten DSP-Kanäle (belegt / vorhanden) an.

Felder im Menü Physikalische Schnittstellen

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

Felder im Menü WAN-Schnittstellen

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

6.2 Globale Einstellungen

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

6.2.1 System

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

System
Passwörter
Datum und Uhrzeit
Systemlizenzen

Grundeinstellungen	
Systemname	Digitalisierungsbox
Standort	
Kontakt	Telekom Deutschland
Maximale Anzahl der Syslog-Protokolleinträge	50
Maximales Nachrichtenlevel von Systemprotokolleinträgen	Information ▼
Maximale Anzahl der Accounting-Protokolleinträge	20
LED-Modus	Status ▼

OK
Abbrechen

Abb. 19: **Systemverwaltung->Globale Einstellungen->System**

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

Felder im Menü Grundeinstellungen

Feld	Wert
Systemname	<p>Geben Sie den Systemnamen Ihres Geräts ein.</p> <p>Möglich ist eine Zeichenkette mit max. 255 Zeichen.</p> <p>Als Standardwert ist der Gerätetyp voreingestellt.</p>
Standort	Geben Sie an, wo sich Ihr Gerät befindet.
Kontakt	<p>Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden.</p> <p>Möglich ist eine Zeichenkette mit max. 255 Zeichen.</p> <p>Der Standardwert ist <i>Telekom Deutschland</i>.</p>
Maximale Anzahl der Syslog-Protokolleinträge	<p>Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000</i>.</p> <p>Der Standardwert ist <i>50</i>. Sie können die gespeicherten Meldungen in Monitoring->Internes Protokoll anzeigen lassen.</p>
Maximales Nachrichtenlevel von Systemprotokolleinträgen	<p>Wählen Sie die Priorität der Systemmeldungen aus, ab der protokolliert werden soll.</p> <p>Nur Systemmeldungen mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass bei der Priorität <i>Debug</i> sämtliche erzeugten Meldungen aufgezeichnet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i>: Es werden nur Meldungen mit der Priorität Notfall aufgezeichnet. • <i>Alarm</i>: Es werden Meldungen mit der Priorität Notfall und Alarm aufgezeichnet. • <i>Kritisch</i>: Es werden Meldungen mit der Priorität Notfall, Alarm und Kritisch aufgezeichnet. • <i>Fehler</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch und Fehler aufgezeichnet. • <i>Warnung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler und Warnung aufgezeichnet. • <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.
Maximale Anzahl der Accounting-Protokolleinträge	<p>Geben Sie die maximale Anzahl an Einträgen an, die für Login-Vorgänge auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000</i>.</p> <p>Der Standardwert ist <i>20</i>.</p>
LED-Modus	<p>Diese Funktion wird nicht unterstützt.</p> <p>Wählen Sie das Leuchtverhalten der LEDs.</p>

Feld	Wert
	<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.

6.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

Abb. 20: **Systemverwaltung ->Globale Einstellungen->Passwörter**



Hinweis

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

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

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

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

Felder im Menü Systempasswort

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

Felder im Menü SNMP-Communities

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

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

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. Nach Anklicken von OK oder erneutem Aufruf des Menüs werden sie als Sternchen angezeigt.</p>

6.2.3 Datum und Uhrzeit

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

System
Passwörter
Datum und Uhrzeit
Systemlizenzen

Grundeinstellungen	
Zeitzone	Europe/Berlin ▼
Aktuelle Ortszeit	Freitag, 24 Apr 2015, 12:05:18
Manuelle Zeiteinstellung	
Datum einstellen	<div style="display: flex; justify-content: space-between;"> <div>Tag <input type="text"/></div> <div>Monat <input type="text"/></div> <div>Jahr <input type="text"/></div> </div>
Zeit einstellen	<div style="display: flex; justify-content: space-between;"> <div>Stunde <input type="text"/></div> <div>Minute <input type="text"/></div> </div>
Automatische Zeiteinstellung (Zeitprotokoll)	
ISDN-Zeitserver	<input type="checkbox"/> Aktiviert
Erster Zeitserver	ntp1.t-online.de SNTP ▼
Zweiter Zeitserver	ptbtime1.ptb.de SNTP ▼
Dritter Zeitserver	<input type="text"/> SNTP ▼
Zeitaktualisierungsintervall	1440 Minute(n)
Zeitaktualisierungsrichtlinie	Normal ▼
System als Zeitserver	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 21: **Systemverwaltung -> Globale Einstellungen -> Datum und Uhrzeit**

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

Manuell

Die Umschaltung der Uhrzeit von Sommer- auf Winterzeit (und zurück) erfolgt automatisch. Die Umschaltung erfolgt unabhängig von der Zeit der Vermittlungsstelle oder von einem ntp-Server. Die Sommerzeit beginnt am letzten Sonntag im März durch die Umschaltung von 2 Uhr auf 3 Uhr. Die in der feh-

lenden Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt. Die Winterzeit beginnt am letzten Sonntag im Oktober durch die Umschaltung von 3 Uhr auf 2 Uhr. Die in der zusätzlichen Stunde anstehenden kalender- oder zeitplanbedingten Umschaltungen im Gerät werden anschließend durchgeführt.

Zeitserver

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



Hinweis

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

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
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. Nur für Kompaktsysteme: Der Standardwert ist <i>Europe/Berlin</i> .
Aktuelle Ortszeit	Hier werden das aktuelle Datum und die aktuelle Systemzeit angezeigt. Der Eintrag kann nicht verändert werden.

Felder im Menü Manuelle Zeiteinstellung

Feld	Beschreibung
Datum einstellen	Geben Sie ein neues Datum ein. Format: <ul style="list-style-type: none"> • Tag: dd • Monat: mm • Jahr: yyyy
Zeit einstellen	Geben Sie eine neue Uhrzeit ein. Format: <ul style="list-style-type: none"> • Stunde: hh • Minute: mm

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
Erster Zeitserver	Geben Sie den ersten Zeitserver an, entweder mit Domännennamen oder IP-Adresse. Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus. Mögliche Werte:

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zweiter Zeitserver	<p>Geben Sie den zweiten Zeitserver an, entweder mit Domännennamen oder IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeitservers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
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 Zeitservers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol über UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst über UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst über TCP-Port 37. • <i>Keiner</i>: Dieser Zeitserver wird momentan nicht für die Zeitabfrage benutzt.
Zeitaktualisierungsintervall	<p>Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird.</p> <p>Der Standardwert ist <i>1440</i>.</p>
Zeitaktualisierungsrichtlinie	<p>Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeitserver erneut zu erreichen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Normal</i> (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeitserver zu erreichen. • <i>Aggressiv</i>: Zehn Minuten lang wird versucht, den Zeitserver zuerst 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 nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen.

Feld	Beschreibung
	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> .
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 aktiv. Zeitanfragen der Clients im LAN werden beantwortet.</p>

6.2.4 Systemlizenzen

In diesem Kapitel werden die im Auslieferungsstand aktivierten Software-Lizenzen angezeigt.


Die Optionen zum Bearbeiten, Neueintragen und Wiederherstellen werden in der Regel nicht benötigt.

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 System nicht unterstützt.

Außerdem wird die **Systemlizenz-ID** oberhalb der Liste angezeigt.

6.2.4.1 Bearbeiten oder Neu

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

System

Passwörter

Datum und Uhrzeit

Systemlizenzen

Grundeinstellungen

Lizenzseriennummer

Lizenzschlüssel

OK

Abbrechen

Abb. 22: **Systemverwaltung->Globale Einstellungen->Systemlizenzen->Neu**

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

Felder im Menü Grundeinstellungen

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

6.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

Mit Bridging werden gleichartige Netze verbunden. Im Gegensatz zum Routern arbeiten Bridges auf Schicht 2 (Sicherungsschicht) 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 der virtuellen Schnittstelle, die an einen Ethernet-Port gebunden ist, setzt sich aus den folgenden Bestandteilen zusammen:

- (a) Abkürzung für den Schnittstellentyp
- (b) Nummer des Ethernet-Ports

- (c) Nummer der Schnittstelle, die an den Ethernet-Port gebunden ist
- (d) Nummer der virtuellen Schnittstelle

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

6.3.1 Schnittstellen

Sie definieren für jede Schnittstelle separat, ob diese im Routing- oder im Bridging-Modus arbeiten soll.
Wenn Sie den Bridging-Modus setzen wollen, können Sie zwischen bestehenden Bridge-Gruppen und dem Erstellen einer neuen Bridge-Gruppe wählen.

Schnittstellen

#	Schnittstellenbeschreibung	Modus / Bridge-Gruppe		
1	en1-0	br0 (192.168.2.1) ▼		
2	en1-4	Routing-Modus ▼		
3	efm35-60	Routing-Modus ▼		
4	ethoa35-5	Routing-Modus ▼		
5	vss7-10	br0 (192.168.2.1) ▼		

Konfigurationsschnittstelle

Eine auswählen ▼

HinzufügenOKAbbrechen

Abb. 23: Systemverwaltung->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen

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

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstellenbeschreibung	Zeigt den Namen der Schnittstelle an.
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><Schnittstellennamen></i>: Legen Sie die Schnittstelle fest, die zur Konfiguration benutzt wird. Wenn diese Schnittstelle Mitglied einer Bridge-Gruppe ist, übernimmt sie deren IP-Adresse, wenn sie aus der Bridge-Gruppe herausgenommen wird.

6.3.1.1 Hinzufügen

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



Abb. 24: **Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen -> Hinzufügen**

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.

6.4 Administrativer Zugriff

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

6.4.1 Zugriff

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



Abb. 25: **Systemverwaltung -> Administrativer Zugriff -> Zugriff**


Für eine Ethernet-Schnittstelle sind die Zugangsparameter *HTTP*, *HTTPS* und *Ping* auswählbar.

Nur für Telefonanlagen: Weiterhin können Sie Ihr Gerät für Wartungsarbeiten durch den Telekom-Kundenservice freischalten. Hierzu aktivieren Sie je nach angeforderter Service-Leistung die Option **Service Call Ticket (SSH Web-Access)** oder **Automatische Konfiguration (TR-069)** und wählen die Schaltfläche **OK**. Folgen Sie den Anweisungen des Telekom-Kundenservice!

Service Call Ticket (SSH Web-Access) ist standardmäßig nicht aktiv, **Automatische Konfiguration (TR-069)** ist standardmäßig aktiv.

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

Felder im Menü Erweiterte Einstellungen

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

6.4.1.1 Hinzufügen

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

Abb. 26: **Systemverwaltung->Administrativer Zugriff->Zugriff->Hinzufügen**

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

Felder im Menü Zugriff

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

6.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

6.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete

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


Pakettypen

Feld	Wert
ACCESS_REQUEST	Client -> Server Wenn ein Verbindungs-Request auf Ihrem Gerät empfangen wird, wird

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

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

6.5.1.1 Bearbeiten oder Neu

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

RADIUS

Optionen

Basisparameter

Authentifizierungstyp

PPP-Authentifizierung

Server-IP-Adresse

RADIUS-Passwort

Standard-Benutzerpasswort

Priorität

0

Eintrag aktiv

☒ Aktiviert

Gruppenbeschreibung

Standardgruppe 0

Erweiterte Einstellungen

Richtlinie

Verbindlich

UDP-Port

1812

Server Timeout

1000

Millisekunden

Erreichbarkeitsprüfung

☒ Aktiviert

Wiederholungen

1

RADIUS-Dialout:

☐ Aktiviert

Neulade-Intervall

0

Sekunden

OK

Abbrechen

Abb. 27: Systemverwaltung ->Remote Authentifizierung ->RADIUS->Neu

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>In Standardanwendungen belassen Sie den Wert bei <i>Standard</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>France Telecom</i>: Für Anwendungen der France Telecom
Server-IP-Adresse	<p>Geben Sie die IP-Adresse des RADIUS-Servers ein.</p>

Feld	Wert
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 aus. • <i><Gruppenname></i>: Wählen Sie aus der Liste eine schon definierte Gruppe aus.

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

Felder im Menü Erweiterte Einstellungen

Feld	Wert
Richtlinie	<p>Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Verbindlich</i> (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. • <i>Nicht verbindlich</i>: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS-Server wird angefragt, bis Ihr Gerät eine Antwort von einem als autoritativ konfigurierten Server erhält.
UDP-Port	<p>Geben Sie den zu verwendenden UDP-Port für RADIUS-Daten ein.</p> <p>Gemäß RFC 2138 sind die Standard-Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Gebührenerfassung (1646 in älteren RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können</p>

Feld	Wert
	<p>Sie entnehmen, welcher Port zu verwenden ist.</p> <p>Der Standardwert ist <i>1812</i>.</p>
Server Timeout	<p>Geben Sie die maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden ein.</p> <p>Nach Ablauf dieser Zeit wird die Anfrage gemäß Wiederholungen wiederholt bzw. der nächste konfigurierte RADIUS-Server angefragt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>50</i> und <i>50000</i>.</p> <p>Der Standardwert ist <i>1000</i> (1 Sekunde).</p>
Erreichbarkeitsprüfung	<p>Wählen Sie eine Überprüfung der Erreichbarkeit eines RADIUS-Servers im Status <i>Inaktiv</i>.</p> <p>Es wird regelmäßig (alle 20 Sekunden) ein Alive-Check durchgeführt, in dem ein ACCESS_REQUEST an die IP-Adresse des RADIUS-Servers gesendet wird. Bei erneuter Erreichbarkeit wird der Status wieder auf <i>aktiv</i> gesetzt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Wiederholungen	<p>Geben Sie die Anzahl der Wiederholungen für den Fall ein, dass eine Anfrage nicht beantwortet wird. Falls nach diesen Versuchen dennoch keine Antwort erhalten wurde, wird der Status auf <i>inaktiv</i> gesetzt. bei Erreichbarkeitsprüfung = <i>Aktiviert</i> versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird Status wieder auf <i>aktiv</i> zurückgesetzt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>0</i> und <i>10</i>.</p> <p>Der Standardwert ist <i>1</i>. Um zu verhindern, dass Status auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf <i>0</i>.</p>
RADIUS-Dialout	<p>Nur für Authentifizierungstyp = <i>PPP-Authentifizierung</i> und <i>IP-Sec-Authentifizierung</i>.</p> <p>Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiv ist, können Sie folgende Optionen eingeben:</p> <ul style="list-style-type: none"> • <i>Neulade-Intervall</i>: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. <p>Standardmäßig ist hier <i>0</i> eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>

6.5.2 Optionen

Aufgrund der hier möglichen Einstellung führt Ihr Gerät bei eingehenden Rufen eine Authentifizierungs-verhandlung 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 er-haltenen Daten (Passwort, Partner PPP ID) mit den Daten einer eingetragenen Gegenstelle oder eines RADIUS-Benutzers übereinstimmen, akzeptiert Ihr Gerät den ankommenden Ruf.



Abb. 28: Systemverwaltung ->Remote Authentifizierung->Optionen

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

Felder im Menü Globale RADIUS-Optionen


Feld	Beschreibung
Authentifizierung für PPP-Einwahl	<p>Standardmäßig wird folgende Reihenfolge bei der Authentisierung für eingehende Verbindungen unter Berücksichtigung von RADIUS ange-wendet: zunächst CLID, danach PPP und daraufhin PPP mit RADIUS.</p> <p>Optionen:</p> <ul style="list-style-type: none">• <i>Inband</i>: Nur Inband-RADIUS-Anfragen (PAP, CHAP, MS-CHAP V1 & V2) (d. h. PPP-Anfragen ohne Rufnummernidentifizierung) werden zum in Server-IP-Adresse definierten RADIUS-Server geschickt.• <i>Outband (CLID)</i>: Nur Outband-RADIUS-Anfragen (d. h. Anfragen zur Rufnummernidentifizierung) werden zum RADIUS-Server geschickt (CLID = Calling Line Identification). <p>Standardmäßig ist <i>Inband</i> aktiviert, <i>Outband (CLID)</i> deaktiviert.</p>



6.6 Konfigurationszugriff

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

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

6.6.1 Zugriffsprofile

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

Standardmäßig sind die Zugriffsprofile *EXPERT* und *USER* bereits angelegt. Diese können Sie mithilfe des Symbols  ändern sowie über das Symbol  auf die Standardeinstellungen zurücksetzen.

Zugriffsprofile Benutzer

Ansicht 20 pro Seite << >> Filtern in Keiner gleich Los


Level Nr.	Beschreibung		
29	EXPERT		
30	USER		

Seite: 1, Objekte: 1 - 2

Neu Zurücksetzen

Abb. 29: Systemverwaltung -> Konfigurationszugriff -> Zugriffsprofile

6.6.1.1 Bearbeiten oder Neu

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

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

ZugriffsprofileBenutzer

Grundeinstellungen

Beschreibung

Level Nr.

2

Schaltflächen

Konfiguration speichern

☐ Aktiviert

Navigationseinträge

Assistenten

▲

✕

Betriebsart

▼

✕

Erste Schritte

▼

✕

Internetzugang

▼

✕

VPN

▼

✕

Wireless LAN

▼

✕

SWYX

▼

✕

VoIP PBX im LAN

▼

✕

Telefonie

▼

✕

Systemverwaltung

▼

✕

Physikalische Schnittstellen

▼

✕

LAN

▼

✕

Wireless LAN

▼

✕

Wireless LAN Controller

▼

✕

Netzwerk

▼

✕

Multicast

▼

✕

WAN

▼

✕

VPN

▼

✕

Firewall

▼

✕

VoIP

▼

✕

Lokale Dienste

▼

✕

Wartung

▼

✕

Externe Berichterstellung

▼

✕

Monitoring

▼

✕

OK

Abbrechen

Abb. 30: Systemverwaltung->Konfigurationszugriff->Zugriffsprofile->Neu


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

Felder im Menü Grundeinstellungen








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

Felder im Menü Schaltflächen


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

Feld	Beschreibung
	<div>  Hinweis Beachten Sie, dass die Passwörter in der gespeicherten Datei im Klartext eingesehen werden können. </div> <p>Aktivieren oder deaktivieren Sie Konfiguration speichern.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Navigationseinträge

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

6.6.2 Benutzer

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

Es sind keine Benutzer vorkonfiguriert.

Zugriffsprofile **Benutzer**

Ansicht 20

pro Seite << >>

Filtern in: Keiner ▼ gleich ▼

Los


Name ▲
🔍 🗑️ ✎

user1

Seite: 1, Objekte: 1 - 1

Neu

Abb. 31: **Systemverwaltung -> Konfigurationszugriff -> Benutzer**




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

Zugriffsprofile **Benutzer**

Grundeinstellungen	
Benutzer	user1
Benutzer muss das Passwort ändern	Deaktiviert
Schaltflächen	
Konfiguration speichern	Deaktiviert
Zum SNMP Browser wechseln	Deaktiviert
Navigationseinträge	
Assistenten	▲ 🔒 🔒
Betriebsart	▼ 🔒 🔒
Erste Schritte	▼ 🔒 🔒
Internetzugang	▼ 🔒 🔒
VPN	▼ 🔒 🔒
Wireless LAN	▼ 🔒 🔒
SWYX	▼ 🔒 🔒
VoIP PBX im LAN	▼ 🔒 🔒
Telefonie	▼ 🔒 🔒
Systemverwaltung	▼ 🔒 🔒
Physikalische Schnittstellen	▼ 🔒 🔒
LAN	▼ 🔒 🔒
Wireless LAN	▼ 🔒 🔒
Wireless LAN Controller	▼ 🔒 🔒
Netzwerk	▼ 🔒 🔒
Multicast	▼ 🔒 🔒
WAN	▼ 🔒 🔒
VPN	▼ 🔒 🔒
Firewall	▼ 🔒 🔒
VoIP	▼ 🔒 🔒
Lokale Dienste	▼ 🔒 🔒
Wartung	▼ 🔒 🔒
Externe Berichterstellung	▼ 🔒 🔒
Monitoring	▼ 🔒 🔒


Abbrechen

Abb. 32: **Systemverwaltung -> Konfigurationszugriff -> Benutzer -> **

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

gesperrte Einträge.

6.6.2.1 Bearbeiten oder Neu

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

ZugriffsprofileBenutzer

Grundeinstellungen

Benutzer

Passwort

Benutzer muss das Passwort ändern

☐ Aktiviert

Zugangs-Level

Zugangs-LevelNur lesen

Hinzufügen

OK

Abbrechen

Abb. 33: Systemverwaltung ->Konfigurationszugriff ->Benutzer->Neu

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

Felder im Menü Grundeinstellungen

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

6.7 Zertifikate

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

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

nanntes digitales Zertifikat benötigt.

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

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

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


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

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

6.7.1 Zertifikatsliste

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

6.7.1.1 Bearbeiten

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

ZertifikatslisteCRLsZertifikatsserver

Parameter bearbeiten

Beschreibung

test

Zertifikat ist ein CA-Zertifikat

☒ Wahr

Überprüfung anhand einer Zertifikatsperrliste (CRL)

☐ Deaktiviert

☐ Immer

☒ Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist

☐ Einstellungen des übergeordneten Zertifikates benutzen

Vertrauenswürdigkeit des Zertifikats erzwingen

☐ Wahr

Details anzeigen

Certificate =
SerialNumber = 1
SubjectName = <MAILTO=mboehmer@bintec.de, CN=Windows XP,
OU=Development,
O=FEC, L=Nuernberg, ST=Bayern, C=DE>
IssuerName = <MAILTO=mboehmer@bintec.de, CN=openssl ca, OU=Development,
O=FEC,
L=Nuernberg, ST=Bayern, C=DE>
Signature algorithm = rsa-pkcs1-md5
Validity =
NotBefore = 2005 Feb 4th, 09:50:11 GMT
NotAfter = 2006 Feb 4th, 09:50:11 GMT
PublicKeyInfo =
Algorithm name (X.509) : rsaEncryption
Modulus n (1024 bits) :

1049357175555193943755033604156717547796569837243619843433661910785954650

0873086401038448934139427553386997798691156631654067109218748316889198617

MD5-Fingerabdruck

EE:AB:21:CB:4A:82:02:44:6C:A2:F6:5E:0D:0C:65:34

SHA1-Fingerabdruck

77:5A:14:BC:60:17:66:56:8C:F7:CC:90:C0:4E:25:19:3B:D3:7B:F7

Verwendet

OK

Abbrechen

Abb. 34: Systemverwaltung ->Zertifikate->Zertifikatsliste->

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

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

Felder im Menü Parameter bearbeiten

Feld	Beschreibung
Beschreibung	Zeigt den Namen des Zertifikats, des Schlüssels oder der Anforderung.
Zertifikat ist ein CA-Zertifikat	<p>Markieren Sie das Zertifikat als Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (CA).</p> <p>Zertifikate, die von dieser CA ausgestellt wurden, werden bei der Authentifizierung akzeptiert.</p> <p>Mit <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Überprüfung anhand einer Zertifikatsperrliste (CRL)	<p>Nur für Zertifikat ist ein CA-Zertifikat = 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</i>

Feld	Beschreibung
	<p><i>vorhanden ist</i> (Standardwert): Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden.</p> <ul style="list-style-type: none"> • <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.

6.7.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

ZertifikatslisteCRLsZertifikatsserver

Zertifikatsanforderung

Zertifikatsanforderungsbeschreibung

Modus

☒ Manuell ☐ SCEP

Privaten Schlüssel generieren

RSA1024Bits

Subjektnamen

Benutzerdefiniert

☐ Aktiviert

Allgemeiner Name

E-Mail

Organisationseinheit

Organisation

Ort

Staat/Provinz

Land

Erweiterte Einstellungen

Subjekt-Alternativnamen

#1

Keiner

#2

Keiner

#3

Keiner

Optionen

Autospeichermodus

☒ Aktiviert

OK

Abbrechen

Abb. 35: Systemverwaltung ->Zertifikate->Zertifikatsliste->Zertifikatsanforderung

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

Felder im Menü Zertifikatsanforderung

Feld	Beschreibung
Zertifikatsanforderungsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Modus	<p>Wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"><i>Manuell</i> (Standardwert): Ihr Gerät erzeugt für den Schlüssel eine PK-CS#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 ein-</p>

Feld	Beschreibung
	gestuft 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.
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. <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 Subjektnamen

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

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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IP</i>: Es wird eine IP-Adresse eingetragen. • <i>DNS</i>: Es wird ein DNS-Name eingetragen. • <i>E-Mail</i>: Es wird eine E-Mail-Adresse eingetragen. • <i>URI</i>: Es wird ein Uniform Resource Identifier eingetragen. • <i>DN</i>: Es wird ein Distinguished Name (DN) eingetragen. • <i>RID</i>: Es wird eine Registered Identity (RID) eingetragen.

Feld im Menü Optionen

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

6.7.1.3 Importieren

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

Zertifikatsliste CRLs Zertifikatsserver

Importieren

Externer Dateiname	<input type="button" value="Datei auswählen"/> Keine ausgewählt
Lokale Zertifikatsbeschreibung	<input style="width: 90%;" type="text"/>
Dateikodierung	<div style="display: inline-block; border: 1px solid #ccc; padding: 2px 5px;">Auto ▼</div>
Passwort	<input style="width: 90%;" type="password"/>

Abb. 36: **Systemverwaltung -> Zertifikate -> Zertifikatsliste -> Importieren**

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

Felder im Menü Importieren

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen des Zertifikats ein, welches importiert werden soll oder wählen Sie die Datei mit Datei auswählen über den Dateibrowser aus.
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Dateikodierung	<p>Wählen Sie die Art der Kodierung, so dass Ihr Gerät das Zertifikat dekodieren kann.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Aktiviert die automatische Kodiererkennung. Falls der Zertifikat-Download im Auto-Modus fehlschlägt, versuchen

Feld	Beschreibung
	<p>Sie es mit einer bestimmten Kodierung.</p> <ul style="list-style-type: none"> • <i>Base64</i> • <i>Binär</i>
Passwort	<p>Um Zertifikate für Ihre Schlüssel zu erhalten, benötigen Sie möglicherweise ein Passwort.</p> <p>Tragen Sie das Passwort hier ein.</p>

6.7.2 CRLs

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

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

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

6.7.2.1 Importieren

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

Abb. 37: **Systemverwaltung->Zertifikate->CRLs->Importieren**

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

Felder im Menü CRL-Import

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

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

6.7.3 Zertifikatsserver

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

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

6.7.3.1 Neu

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

ZertifikatslisteCRLsZertifikatsserver

Basisparameter

Beschreibung

LDAP-URL-Pfad

ldap://

OK

Abbrechen

Abb. 38: **Systemverwaltung ->Zertifikate->Zertifikatsserver->Neu**

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

Felder im Menü Basisparameter

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

Kapitel 7 Physikalische Schnittstellen

7.1 Ethernet-Ports

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

Die Ethernet-Ports **LAN1** bis **LAN4** sind im Auslieferungszustand einer einzigen logischen Ethernet-Schnittstelle zugeordnet. Die logische Ethernet-Schnittstelle `en1-0` ist zugewiesen und mit **IP-Adresse** `192.168.2.1` und **Netzmaske** `255.255.255.0` vorkonfiguriert.



Hinweis

Um die Erreichbarkeit Ihres Systems zu gewährleisten, achten Sie beim Aufteilen der Ports darauf, dass die Ethernet-Schnittstelle `en1-0` mit der vorkonfigurierten IP-Adresse und Netzmaske einem Port zugewiesen wird, der per Ethernet erreichbar ist.

ETH1 - ETH4

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

VLANs für Routing-Schnittstellen

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

7.1.1 Portkonfiguration

Portseparation

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

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

Portkonfiguration

Automatisches Aktualisierungsintervall Sekunden
Übernehmen

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

OK
Abbrechen

Abb. 39: **Physikalische Schnittstellen->Ethernet-Ports->Portkonfiguration**

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

Felder im Menü Switch-Konfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Switch-Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Ethernet-Schnittstellenauswahl	<p>Ordnen Sie dem jeweiligen Switch-Port eine logische Ethernet-Schnittstelle zu.</p> <p>Zur Auswahl stehen vier Schnittstellen, <i>en1-0</i> bis <i>en1-3</i>. In der Grundeinstellung ist Switch Port 1-4 die Schnittstelle <i>en1-0</i> zugeordnet.</p>
Konfigurierte Geschwindigkeit/konfigurierter Modus	<p>Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vollständige automatische Aushandlung</i> (Standardwert) • <i>Auto 1000 Mbit/s only</i> • <i>Auto 100 Mbit/s only</i> • <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 jeweiligen Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>1000 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Half Duplex</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • 10 Mbit/s / Full Duplex • 10 Mbit/s / Half Duplex • Inaktiv
Flusskontrolle	<p>Wählen Sie aus, ob auf der entsprechenden Schnittstelle eine Flusskontrolle vorgenommen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i> (Standardwert): Es wird keine Flusskontrolle vorgenommen. • <i>Aktiviert</i>: Es wird eine Flusskontrolle durchgeführt. • <i>Auto</i>: Es wird eine automatische Flusskontrolle durchgeführt.

7.2 ISDN-Ports

In diesem Menü konfigurieren Sie die ISDN-Schnittstelle Ihres Geräts. Um die ISDN-BRI-Schnittstelle zu konfigurieren, müssen Sie zwei Schritte durchführen:

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

7.2.1 ISDN-Konfiguration




Hinweis

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


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

7.2.1.1 Bearbeiten

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

ISDN-Konfiguration MSN-Konfiguration

Basisparameter	
Portname	bri-0 (NT)
Port-Verwendung	Dialup (Euro-ISDN) ▼
ISDN-Konfigurationstyp	<input type="radio"/> Punkt-zu-Mehrpunkt <input checked="" type="radio"/> Punkt-zu-Punkt
Erweiterte Einstellungen	
X.31 (X.25 im D-Kanal)	<input type="checkbox"/> Aktiviert
OK Abbrechen	

Abb. 40: **Physikalische Schnittstellen->ISDN-Ports->ISDN-Konfiguration->** 

Das Menü **Physikalische Schnittstellen->ISDN-Ports->ISDN-Konfiguration->**  besteht aus folgen-

den Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Port-Verwendung	<p>Nur wenn Automatische Konfiguration beim Start deaktiviert ist.</p> <p>Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht verwendet</i>: Der ISDN-Anschluss wird nicht genutzt. • <i>Dialup (Euro-ISDN)</i> • <i>Q-SIG</i>
ISDN-Konfigurationstyp	<p>Nur wenn Automatische Konfiguration beim Start deaktiviert ist und für Port-Verwendung = <i>Dialup (Euro-ISDN)</i> gesetzt ist.</p> <p>Wählen Sie die ISDN-Anschlussart aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Punkt-zu-Mehrpunkt</i> (Standardwert): Mehrgeräteanschluss. • <i>Punkt-zu-Punkt</i>: Anlagenanschluss.

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	<i>Packet Switch</i> stellen Sie ein, wenn Sie den X.31-TEI für das X.25-Gerät nutzen möchten.

7.3 DSL-Modem

Das DSL-Modem eignet sich für den High-Speed Internetzugang und den Remote-Access-Einsatz in kleinen bis mittleren Unternehmen oder Remote-Offices.

7.3.1 DSL-Konfiguration

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

DSL-Konfiguration

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

Abb. 41: Physikalische Schnittstellen->DSL-Modem->DSL-Konfiguration

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

Felder im Menü DSL-Portstatus

Feld	Beschreibung
DSL-Chipsatz	Zeigt die Kennung des eingebauten Chipsatzes an.
Physikalische Verbindung	<p>Zeigt den aktuellen DSL-Betriebsmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Unbekannt</i>: Der Link ist nicht aktiv. • <i>ADSL1</i>: ADSL classic, G.DMT, ITU-T G.992.1 • <i>ADSL2</i>: G.DMT.Bis, ITU-T G.992.3 • <i>ADSL2 Plus</i>: ADSL2 Plus, ITU-T G.992.5 • <i>ADSL2+ Annex J</i>: ITU-T G.992.5 • <i>VDSL2</i>: ITU-T G.993.2

Felder im Menü Aktuelle Leitungsgeschwindigkeit

Feld	Beschreibung
Downstream	Zeigt die Datenrate in Empfangsrichtung (Richtung von CO/DSLAM zu CPE/Router) in Bits pro Sekunde an.

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

Felder im Menü DSL Parameter

Feld	Beschreibung
DSL-Modus	<p>Zeigt den gewählten DSL-Betriebsmodus an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>: Der Link ist nicht aktiv. • <i>ETSI T1.413</i>: ETSI T1.413 • <i>ADSL1</i>: ADSL classic, G.DMT, ITU-T G.992.1 • <i>Automatischer Modus (ADSL)</i> (Standardwert, wenn das Gerät als Telefonanlage betrieben wird): Automatische Erkennung des ADSL-Modus <i>ADSL1</i>, <i>ADSL2</i> oder <i>ADSL2 Plus</i> • <i>ADSL2</i>: G.DMT.Bis, ITU-T G.992.3 • <i>ADSL2 Plus</i>: ADSL2 Plus, ITU-T G.992.5 • <i>VDSL</i>: VDSL2 (ITU-T G.993.2) • <i>VDSL/ADSL Multimodus</i> (Standardwert, wenn das Gerät als Media Gateway betrieben wird): Automatische Erkennung des DSL-Modus <i>ADSL1</i>, <i>ADSL2</i>, <i>ADSL2 Plus</i> oder <i>VDSL</i>
Transmit Shaping	<p>Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DSLAMs notwendig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard (Leitungsgeschwindigkeit)</i> (Standardwert): Die Datenrate in Senderichtung wird nicht reduziert. • <i>128.000 Bit/s bis 2.048.000 Bit/s</i>: Die Datenrate in Senderichtung wird reduziert auf maximal 128.000 bit/s bis 2.048.000 bit/s in festgesetzten Schritten. • <i>Benutzerdefiniert</i>: Die Datenrate wird reduziert auf den in Maximale Upstream-Bandbreite eingegebenen Wert.
Maximale Upstream-Bandbreite	<p>Nur für Transmit Shaping = <i>Benutzerdefiniert</i></p> <p>Geben Sie die maximale Datenrate in Senderichtung in Bits pro Sekunde ein.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
ADSL-Leitungsprofil	<p>Wählen Sie den gewünschten Internet-Service-Provider und damit implizit den von diesem Provider verwendeten Modem-Parametersatz aus.</p> <p><i>Deutsche Telekom</i> ist als Standardwert voreingestellt.</p> <p>Wenn Sie Ihren Provider in der Liste nicht finden, verwenden Sie die Einstellung <i>Standard</i>.</p>

Kapitel 8 LAN


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

8.1 IP-Konfiguration

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



8.1.1 Schnittstellen


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

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

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

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

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

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



Hinweis

Beachten Sie bei IPv4:

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

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

Beispiel Teilnetze

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

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

IPv6-Adressen konfigurieren

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

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

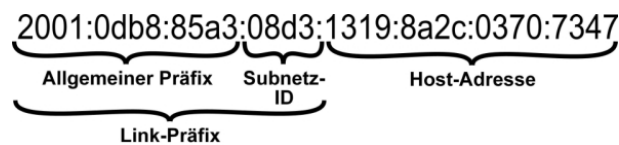


Abb. 42: IPv6-Adresse (Beispiel)

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 Zeitervers, 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 Zeitervers können per DHCP bezogen werden. Verwenden Sie dazu im Menü **LAN->IP-Konfiguration->Schnittstellen->Neu** die Einstellungen **IPv6-Modus** = *Client*, **Router Advertisement annehmen** *Aktiviert* und **DHCP-Client** = *Aktiviert*.

8.1.1.1 Bearbeiten oder Neu

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

Schnittstellen

(VLAN-ID3)

Basisparameter

Basierend auf Ethernet-Schnittstelle

Eine auswählen

Schnittstellenmodus

Untagged

Tagged (VLAN)

VLAN-ID

1

MAC-Adresse

00:a0:f9

☒ Voreingestellte verwenden

Grundlegende IPv4-Parameter

Sicherheitsrichtlinie

Nicht Vertrauenswürdig

Vertrauenswürdig

Adressmodus

Statisch

DHCP

IP-Adresse / Netzmaske

IP-Adresse

Netzmaske

Hinzufügen

Grundlegende IPv6-Parameter

IPv6

☐ Aktiviert

Erweiterte Einstellungen

Erweiterte IPv4-Einstellungen

Proxy ARP

☐ Aktiviert

TCP-MSS-Clamping

☐ Aktiviert

OK

Abbrechen

Abb. 43: LAN->IP-Konfiguration->Schnittstellen->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	<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">Untagged (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet.Tagged (VLAN): Diese Option gilt nur für Routing-Schnittstellen. <p>Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu. Dies geschieht über die VLAN-ID, die in diesem Modus angezeigt wird und konfiguriert werden kann. Die Definition einer MAC-Adresse in MAC-Adresse ist in diesem Modus optional.</p>
VLAN-ID	<p>Nur für Schnittstellenmodus = Tagged (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</p>

Feld	Beschreibung
	<p>können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde, wenn Sie Voreingestellte verwenden aktivieren. Die VLAN IDs müssen sich jedoch unterscheiden. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt (sie können jedoch geändert werden).</p> <p>Wenn Voreingestellte verwenden aktiv ist, wird die voreingestellte MAC-Adresse der zugrunde liegenden physikalischen Schnittstelle verwendet.</p> <p>Standardmäßig ist Voreingestellte verwenden aktiv.</p>

Felder im Menü Grundlegende IPv4-Parameter

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Vertrauenswürdig</i> (Standardwert): Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <i>Nicht Vertrauenswürdig</i>: Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 227 konfigurieren.</p>
Adressmodus	<p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse / Netzmaske zugewiesen. <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse / Netzmaske	<p>Nur für Adressmodus = <i>Statisch</i></p> <p>Fügen Sie mit Hinzufügen einen neuen Adresseintrag hinzu und geben Sie die IP-Adresse und die entsprechende Netzmaske der virtuellen Schnittstelle ein.</p>

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

Feld	Beschreibung
	<p>durchgelassen, außer denen, die explizit verboten sind.</p> <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <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 227 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</i> (Standardwert): Die Schnittstelle wird im Router-Modus betrieben. • <i>Host</i>: Die Schnittstelle wird im Host-Modus betrieben.
Router Advertisement übertragen	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <i>Router</i></p> <p>Wählen Sie, ob Router Advertisements über die gewählte Schnittstelle gesendet werden sollen.</p> <p>Mithilfe der Router Advertisements wird z.B. die Präfix Liste übertragen und der Router propagiert sich als Standard-Gateway.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
DHCP-Server	<p>Nur für IPv6 = <i>Aktiviert</i> und IPv6-Modus = <i>Router</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 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 zu-</p>

Feld	Beschreibung
	<p>sätzliche Adressen eintippen.</p> <p>Wenn Ihr Gerät im Router-Modus arbeitet (IPv6-Modus = <i>Router</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 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.

Schnittstellen

en1-4

Basisparameter

Schnittstellenmodus

Untagged

Tagged (VLAN)

MAC-Adresse

Grundlegende IP

Sicherheitsricht

Adressmodus

IP-Adresse / N

Grundlegende IP

IPv6

Sicherheitsricht

IPv6-Modus

Router Adverti

DHCP-Server

IPv6-Adressen

Basisparameter

Ankündigen

Aktiviert

Link-Präfix

Art der Einrichtung

Von Allgemeinem Präfix

Statisch

Allgemeiner Präfix

Eine auswählen

Host-Adresse

Erzeugungsmethode

Auto eui-64

Statische Adressen

Adresse

Länge

Hinzufügen

Erweitert

Übernehmen

Schließen

DHCP-Server

Aktiviert

Link-Präfix

Host-Adresse

Ankündigen

Hinzufügen

Erweiterte Einstellungen

OK

Abbrechen

Abb. 44: LAN->IP-Konfiguration->Schnittstellen->Neu->Hinzufügen

Felder im Menü Basisparameter

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

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

Felder im Menü Link-Präfix


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

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 <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Autonomous Flag	<p>Wählen Sie, ob das Autonomous Address Configuration Flag (A-Flag) gesetzt werden soll.</p> <p>Dadurch nutzt ein Host das Präfix und eine Schnittstellen-ID, um daraus seine Adresse abzuleiten.</p> <p>Mit Auswahl von <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Bevorzugte Gültigkeitsdauer	<p>Geben Sie eine Zeitspanne in Sekunden ein. Während dieser Zeit werden die Adressen, die mit Hilfe des Präfix per SLAAC 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>  Hinweis <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> <p>Wählen Sie aus, ob in den DHCP-Anfragen Ihres Gerätes das BROADCAST Bit gesetzt werden soll oder nicht. Einige DHCP-Server, die IP-Adressen mittels UNICAST vergeben, reagieren nicht auf DHCP-Anfragen mit gesetztem BROADCAST Bit. In diesem Falle ist es nötig, DHCP-Anfragen zu versenden, in denen dieses Bit nicht gesetzt ist. Deaktivieren Sie in diesem Fall diese Option.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für definierte Gegenstellen beantworten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-MSS-Clamping	<p>Wählen Sie aus, ob Ihr Gerät das Verfahren MSS Clamping anwenden soll. Um die Fragmentierung von IP-Paketen zu verhindern, wird hierbei vom Gerät automatisch die MSS (Maximum Segment Size) auf den hier einstellbaren Wert verringert.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Bei Aktivierung ist im Eingabefeld der Standardwert <i>1350</i> eingetragen.</p>

Felder im Menü Erweiterte IPv6-Einstellungen

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

Feld	Beschreibung
	<p>ist und nicht in die Default Router List eingetragen werden soll.</p> <div data-bbox="563 219 1348 436">  Hinweis 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. </div>
Router-Präferenz	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die Präferenz Ihres Routers für die Wahl des Standardrouters. Dies ist in Fällen nützlich, in denen ein Knoten Advertisements von mehreren Routern erhält oder in Back-Up-Szenarien.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hoch</i> • <i>Mittel</i> (Standardwert) • <i>Niedrig</i>
DHCP-Modus	<p>Nur für IPv6 = Aktiviert, IPv6-Modus = Router und Router Advertisement übertragen = Aktiviert</p> <p>Wählen Sie die an den DHCP-Client weitergeleiteten Informationen aus.</p> <div data-bbox="563 1086 1348 1209">  Hinweis Der Router muss nicht als DHCP-Server eingerichtet sein. </div> <p>Mit Auswahl von <i>Andere - DNS-Server, SIP-Server</i> (Standardwert) werden nicht-adressbezogene Informationen, wie z. B. DNS, VoIP, usw. durchgeleitet.</p> <p>Aktivieren Sie diese Option, wenn die Hosts im Netzwerk ihre IP-Adresse über SLAAC automatisch bilden sollen. Der Router sendet in diesem Fall ausschließlich nicht-adressbezogene Daten über DHCP.</p> <p>Mit Auswahl von <i>Verwaltet - IPv6-Adressverwaltung</i> werden sowohl die IPv6-Adressen als auch alle nicht adressbezogenen Daten vom Host per DHCP bezogen.</p>
DNS-Propagation	<p>Nur für IPv6-Modus = Router und Router Advertisement übertragen Aktiviert</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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Sonstige</i>: Die statisch konfigurierten und die dynamisch gelernten DNS-Server-Einträge werden gemäß ihrer Priorität propagiert. Sind keine Einträge vorhanden, werden keine Adressen propagiert.

8.2 VLAN

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

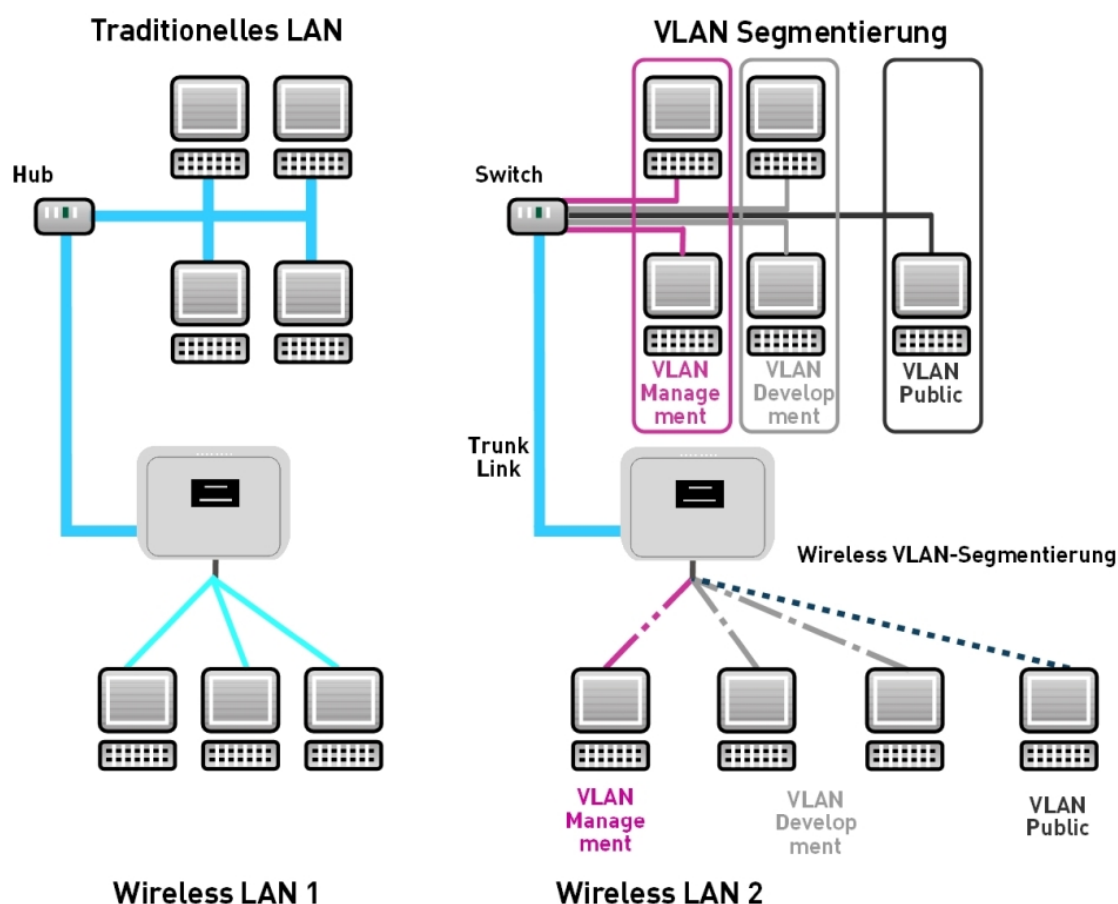


Abb. 45: VLAN-Segmentierung

VLAN für Bridging und VLAN für Routing

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




Achtung

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

8.2.1 VLANs

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

8.2.1.1 Bearbeiten oder Neu

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

VLANsPortkonfigurationVerwaltung

VLAN konfigurieren

VLAN Identifier1

VLAN-NameManagement

VLAN-Mitglieder

Schnittstelle

Ausgehende Regel

Löschen

en1-0

Untagged


OK

Abbrechen

Abb. 46: LAN->VLAN->VLANs->Neu

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

Felder im Menü VLAN konfigurieren

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

8.2.2 Portkonfiguration

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

VLANs Portkonfiguration Verwaltung

Ansicht 20
pro Seite << >>
Filtern in Keiner gleich
Los

Schnittstelle	PVID	Frames ohne Tag verwerfen	Nicht-Mitglieder verwerfen
en1-0	1 - Management	<input type="checkbox"/>	<input type="checkbox"/>

Seite: 1, Objekte: 1 - 1

OK Abbrechen

Abb. 47: LAN->VLANs->Portkonfiguration

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

Felder im Menü Portkonfiguration

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

8.2.3 Verwaltung

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

VLANs Portkonfiguration Verwaltung

Bridge-Gruppe br0 VLAN-Optionen

VLAN aktivieren	<input type="checkbox"/> Aktiviert
Verwaltungs-VID	1 - Management

OK Abbrechen

Abb. 48: LAN->VLANs->Verwaltung

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

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

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

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

Kapitel 9 Wireless LAN

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

Netzwerkfunktionen

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

Derzeit gültiger Standard: IEEE 802.11

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

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

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

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

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

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

9.1 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.

Konkrete Hinweise für die Konfiguration von Wireless LAN finden Sie am Ende des Kapitels unter [WLAN - Konfigurationsbeispiel](#) auf Seite 90.

9.1.1 Einstellungen Funkmodul

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

Einstellungen Funkmodul

Einstellungen Funkmodul						
MAC-Adresse	Betriebsmodus	Frequenzband	Verwendeter Kanal	Sendeleistung	Status	
00:a0:f9:ff:a4:fb	Aus	2,4 GHz	6	Max.		

Abb. 49: Wireless LAN->WLAN->Einstellungen Funkmodul

9.1.1.1 Einstellungen Funkmodul->

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie das Symbol um die Konfiguration zu bearbeiten.

Einstellungen Funkmodul

WLAN-Einstellungen

Betriebsmodus	Access-Point ▼
Frequenzband	2,4 GHz In/Outdoor ▼
Kanal	Auto ▼
Ausgewählter Kanal	6
Anzahl der Spatial Streams	2 ▼
Sendeleistung	Max. ▼

Performance-Einstellungen

Drahtloser Modus	802.11b/g/n ▼
Airtime Fairness	<input type="checkbox"/> Aktiviert

Erweiterte Einstellungen

Kanalplan	Alle ▼
RTS Threshold	Immer inaktiv ▼
Short Guard Interval	<input checked="" type="checkbox"/> Aktiviert
Fragmentation Threshold	2346 Bytes

OK

Abbrechen

Abb. 50: Wireless LAN->WLAN->Einstellungen Funkmodul-> für Betriebsmodus *Access-Point* / *Bridge Link Master*

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

Felder im Menü WLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	<p>Legen Sie fest, in welchem Modus das Funkmodul Ihres Geräts betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><i>Aus</i> (Standardwert): Das Funkmodul ist nicht aktiv.<i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk.
Frequenzband	<p>Wählen Sie das Frequenzband und ggf. den Einsatzbereich des Funkmoduls aus.</p> <p>Für Betriebsmodus = <i>Access-Point</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

Feld	Beschreibung
	<p>(Mode 802.11b und Mode 802.11g) innerhalb oder außerhalb von Gebäuden betrieben.</p> <ul style="list-style-type: none"> • <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb von Gebäuden betrieben. • <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) außerhalb von Gebäuden betrieben. • <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb oder außerhalb von Gebäuden betrieben.
Kanal	<p>Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.</p> <p>Access-Point-Modus:</p> <p>Durch das Einstellen des Netzwerknamens (SSID) im Access-Point-Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens 4 Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt.</p> <p>Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden Clients diese Kanäle auch unterstützen.</p> <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</i> bis <i>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</i>, <i>40</i>, <i>44</i>, <i>48</i> und <i>Auto</i> (Standardwert)</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Outdoor</i> <p>Hier ist nur die Option <i>Auto</i> möglich.</p>
Ausgewählter Kanal	Zeigt den verwendeten Kanal an.
Bandbreite	<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.
Anzahl der Spatial Streams	<p>Nur für Drahtloser Modus = <i>802.11b/g/n</i>, <i>802.11g/n</i> und <i>802.11n</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.
Sendeleistung	Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die

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

Feld	Beschreibung
	<p>sourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.</p>


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

Felder im Menü Erweiterte Einstellungen für Betriebsmodus = Access-Point

Feld	Beschreibung
Kanalplan	<p>Nur für Betriebsmodus = <i>Access-Point</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	<p>Hier wählen Sie aus, wie der RTS/CTS-Mechanismus ein- bzw. ausgeschaltet werden soll.</p> <p>Wählen Sie <i>Benutzerdefiniert</i> aus, können Sie in das Eingabefeld den Schwellwert in Bytes (1 - 2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch unabhängig von der Datenpaketlänge ein- bzw. ausgeschaltet werden, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.</p>
Short Guard Interval	<p>Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.</p>
Fragmentation Threshold	<p>Geben Sie die maximale Größe an, ab der Datenpakete fragmentiert (d.</p>

Feld	Beschreibung
	h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert.
	Möglich Werte sind 256 bis 2346.
	Der Standardwert ist 2346 Bytes.

9.1.2 Drahtlosnetzwerke (VSS)

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



Hinweis

Das voreingestellte Drahtlosnetzwerk default verfügt im Auslieferungszustand über folgende Sicherheitseinstellungen:

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

Einstellen von Netzwerknamen

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

Absicherung von Funknetzwerken

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

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

WEP

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

IEEE 802.11i

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

WPA

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

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

WPA 2

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

Zugangskontrolle

Sie können kontrollieren, welche Clients über Ihr Gerät auf Ihr Wireless LAN zugreifen dürfen, indem Sie eine Access Control List anlegen (**Zugriffskontrolle** oder **MAC-Filter**). In der Access Control List tragen Sie die MAC-Adressen der Clients ein, die Zugriff auf Ihr 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 88).

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

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
WMM	<p>Wählen Sie aus, ob für das Drahtlosnetzwerk Sprach- oder Videodaten-Priorisierung mittels WMM (Wireless Multimedia) aktiviert sein soll, um stets eine optimale Übertragungsqualität bei zeitkritischen Anwendungen zu erreichen. Es wird Datenpriorisierung nach DSCP (Differentiated Services Code Point) oder IEEE802.1d unterstützt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
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>

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, z. B. <i>hallo</i> für <i>WEP 40</i>, <i>wep1</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA und WPA 2</i> (Standardwert): WPA und WPA 2 können angewendet werden. • <i>WPA</i>: Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA 2 wird angewendet.

Feld	Beschreibung
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>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</i> und <i>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 black; padding: 10px; margin-top: 10px;"> <p> Hinweis</p> <p>Ändern Sie unbedingt den Standard Preshared Key! Solange der Schlüssel nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p> </div>
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>

Feld	Beschreibung
	<p>Mögliche Werte sind ganze Zahlen von 1 bis 254.</p> <p>Der Standardwert ist 32.</p>
Max. Anzahl Clients - Soft Limit	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Um eine vollständige Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehnt. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des Max. Anzahl Clients - Hard Limit werden Anfragen strikt abgelehnt.</p> <p>Der Wert der Max. Anzahl Clients - Soft Limit muss gleich oder kleiner sein als der Max. Anzahl Clients - Hard Limit.</p> <p>Der Standardwert ist 28.</p> <p>Sie können diese Funktion deaktivieren, indem Sie Max. Anzahl Clients - Soft Limit und Max. Anzahl Clients - Hard Limit auf den gleichen Wert einstellen.</p>
Auswahl des Client-Bands	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Diese Funktion erfordert eine Konfiguration mit zwei Radiomodulen, bei der das gleiche Drahtlosnetzwerk auf beiden Modulen, aber in unterschiedlichen Frequenzbändern konfiguriert ist.</p> <p>Die Option Auswahl des Client-Bands ermöglicht es, Clients von dem ursprünglich ausgewählten in ein weniger ausgelastetes Frequenzband zu verschieben, sofern dieses vom Client unterstützt wird. Dazu wird ein Verbindungsversuch des Clients ggf. zunächst abgelehnt, damit dieser sich in einem anderen Frequenzband erneut anzumelden versucht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert, optimiert für Fast Roaming</i> (Standardwert): Die Funktion wird für dieses VSS 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-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.</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</i> (Standardwert) • <i>1 Mbit/s, 1 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>1 Mbit/s, 1 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 Erweiterte Einstellungen

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 Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten.</p> <p>Mögliche Werte sind <i>1 bis 255</i>.</p> <p>Der Standardwert ist <i>2</i>.</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>

9.2 Verwaltung

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

9.2.1 Grundeinstellungen

Abb. 52: **Wireless LAN->Verwaltung->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>

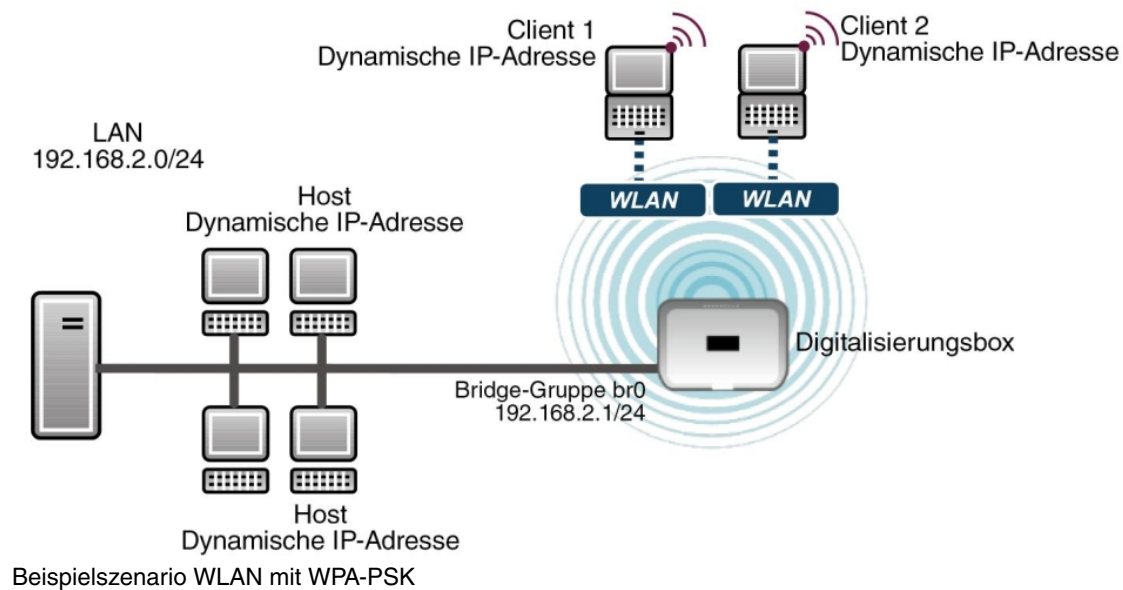
9.3 Konfiguration

9.3.1 WLAN - Konfigurationsbeispiel

Voraussetzungen

- Ihr LAN ist über die erste Ethernet-Schnittstelle (Port **1**) Ihres Geräts angeschlossen
- Ein Client mit geeignetem Betriebssystem und WLAN
- Im LAN verteilt ein DHCP-Server IP-Adressen aus dem Netz *192.168.2.0/24* für Clients aus dem LAN und WLAN.
- Eine z. B. mit dem Assistenten **Schnellstart** im Abschnitt **Internet** konfigurierte Verbindung zum WAN, z. B. *WAN_VDSL_Telekom*.

Beispielszenario



Konfigurationsziel

Konfiguration eines zusätzlichen WLANs (Gaeeste-WLAN)

Konfigurationsschritte im Überblick

Gaeeste-WLAN einrichten

Feld	Menü	Wert
Netzwerkname (SSID)	Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu	z. B. <i>Gaeeste-WLAN</i>
Sichtbar	Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu	Aktiviert
Sicherheitsmodus	Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu	<i>WPA-PSK</i>
WPA-Modus	Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu	<i>WPA2</i>
Preshared Key	Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS) -> Neu	z. B. <i>Super-Secret-2</i>

Gaeeste-WLAN aktivieren

Feld	Menü	Wert
Aktion	Wireless LAN -> WLAN -> Drahtlosnetzwerke (VSS)	

IP-Pool zuordnen

Feld	Menü	Wert
Adressmodus	LAN -> IP-Konfiguration -> Schnittstellen -> vss7-11	<i>Statisch</i>
IP-Adresse / Netzmaske	LAN-> IP-Konfiguration-> Schnittstellen-> vss7-11 -> Hinzufügen	z. B. <i>192.168.0.10 / 255.255.255.0</i>
IP-Poolname	Lokale Dienste -> DHCP-Server-> IP-Pool-Konfiguration-> Neu	z. B. <i>Pool Gaeeste</i>
IP-Adressbereich	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>192.168.0.50 - 192.168.0.99</i>
Schnittstelle	Lokale Dienste -> DHCP-Server -> DHCP-Konfiguration -> Neu	<i>vss7-11</i>
IP-Poolname	Lokale Dienste -> DHCP-Server -> DH-	z. B. <i>Pool Gaeeste</i>

Feld	Menü	Wert
	CP-Konfiguration -> Neu	

Firewall-Regeln einrichten

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>WLAN_VSS7-11</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>z. B. WAN_VDSL_TELEKOM</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Zugriff</i>
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>WLAN_VSS7-11</i>
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>z. B. WAN</i>
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>any</i>
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>Verweigern</i>

Kapitel 10 Wireless LAN Controller

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

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

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

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

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

10.1 Wizard

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

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



Hinweis

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

10.1.1 Grundeinstellungen

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

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

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

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

Schnittstelle

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

DHCP-Server

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

Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen

APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü **Systemverwaltung->Globale Einstellungen->System** im Feld **Manuelle IP-Adresse des WLAN-Controller** eintragen.

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

Wenn Sie z. B. eine **Digitalisierungsbox** 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.

10.1.2 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.

10.1.3 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.

10.1.3.1 Drahtlosnetzwerke ändern oder hinzufügen

Zum Bearbeiten eines vorhandenen Eintrags klicken Sie auf .

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

Folgende Parameter stehen zur Verfügung

Netzwerkname (SSID)

Geben Sie den Namen des Drahtlosnetzwerks (SSID) ein.

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

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

Sicherheitsmodus

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

Hinweis: *WPA-Enterprise* bedeutet 802.11x.

WPA-Modus

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

Preshared Key

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

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



Wichtig

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

RADIUS-Server

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

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

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

EAP-Vorabauthentifizierung

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

VLAN

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

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




Hinweis

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

10.1.4 Automatische Installation starten

Sie sehen eine Liste der gefundenen Access Points.

Wenn Sie die Einstellungen eines gefundenen APs ändern wollen, klicken Sie im entsprechenden Ein-

trag auf .

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

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

Standort

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

Zugewiesene Drahtlosnetzwerke (VSS)

Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

Folgende Parameter stehen im Menü Funkmodul 1 zur Verfügung:

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

Betriebsmodus

Wählen Sie den Betriebsmodus des Funkmoduls.

Mögliche Werte:

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

Aktives Funkmodulprofil

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

Kanal

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

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



Hinweis

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

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

Sendeleistung

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

Mit **OK** übernehmen Sie die Einstellungen.

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

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

10.2 Controller-Konfiguration

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

10.2.1 Allgemein

Allgemein

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

Abb. 53: **Wireless LAN Controller->Controller-Konfiguration->Allgemein**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Region	<p>Wählen Sie das Land, in welchem der Wireless LAN Controller betrieben werden soll.</p> <p>Mögliche Werte sind alle auf dem Wirelessmodul des Geräts vorkonfigurierten Länder.</p>

Feld	Beschreibung
	<p>Der Bereich der verwendbaren Kanäle variiert je nach Ländereinstellung.</p> <p>Der Standardwert ist <i>Germany</i>.</p>
Schnittstelle	Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.
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. eine Digitalisierungsbox 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 <i>CAPWAP Controller</i> und tragen Sie im Feld Wert die IP-Adresse des WLAN Controllers ein.</p> <p>Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü Systemverwaltung->Globale Einstellungen->System im Feld Manuelle IP-Adresse des WLAN-Controller eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Extern oder statisch</i> (Standardwert): Ein externer DHCP-Server mit aktiver CAPWAP Option 138 vergibt die IP-Adressen an die APs oder Sie vergeben statische IP-Adressen an die APs. • <i>Intern</i>: Ihr Gerät, auf dem CAPWAP Option 138 aktiv ist, vergibt die IP-Adressen an die APs.
IP-Adressbereich	<p>Nur für DHCP-Server = <i>Intern</i></p> <p>Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein. Diese IP-Adressen und Ihr Gerät müssen aus demselben Netz stammen.</p>
Slave-AP-Standort	<p>Wählen Sie aus, ob sich die APs, die der Wireless LAN Controller verwalten soll, im LAN oder im WAN befinden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal (LAN)</i> (Standardwert) • <i>Entfernt (WAN)</i> <p>Die Einstellung <i>Entfernt (WAN)</i> ist nützlich, wenn zum Beispiel ein Wireless LAN Controller in der Zentrale installiert ist und seine APs auf verschiedene Filialen verteilt sind. Wenn die 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>

Feld	Beschreibung
	<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.

10.3 Slave-AP-Konfiguration

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

10.3.1 Slave Access Points

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

Automatisches Aktualisierungsintervall Sekunden Übernehmen

Ansicht pro Seite << >> Filtern in Keiner gleich Los

Standort	Name	IP-Adresse	LAN-MAC-Adresse	Kanal	Kanalsuche	Status	Aktion
1:	W2003n-ext	10.0.0.231	00:a0:f9:0b:cf:d8	auto (Ch.1)/auto (Ch.0)		Managed	

Seite: 1, Objekte: 1 - 1

Aktionen

Neue Kanalfestlegung START

Abb. 54: Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points

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

Für jeden Access Point sehen Sie einen Eintrag mit einem Parametersatz (**Standort**, **Name**, **IP-Adresse**, **LAN-MAC-Adresse**, **Kanal**, **Kanalsuche**, **Status**, **Aktion**). 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 bzw. ohne Stromversorgung o.ä.

10.3.1.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.


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

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

Access-Point-Einstellungen							
Gerät	W2003n-ext						
Standort	1:						
Name	W2003n-ext						
Beschreibung							
CAPWAP-Verschlüsselung	<input checked="" type="checkbox"/> Aktiviert						
Funkmodul1							
Betriebsmodus	<input checked="" type="radio"/> Ein <input type="radio"/> Aus						
Aktives Funkmodulprofil	2.4 GHz Radio Profile ▼						
Kanal	Auto ▼						
Verwendeter Kanal	1						
Sendeleistung	Max. ▼						
Zugewiesene Drahtlosnetzwerke (VSS)	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Profil</th> <th style="width: 40%;">MAC-Adresse</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td>vss-2.default</td> <td>00:a0:f9:0b:cf:e0</td> <td></td> </tr> </tbody> </table>	Profil	MAC-Adresse		vss-2.default	00:a0:f9:0b:cf:e0	
Profil	MAC-Adresse						
vss-2.default	00:a0:f9:0b:cf:e0						
Funkmodul2							
Betriebsmodus	<input type="radio"/> Ein <input checked="" type="radio"/> Aus						
Aktives Funkmodulprofil	Eine auswählen ▼						
Kanal	Kein Profil ausgewählt!						
Verwendeter Kanal	0						
Sendeleistung	Max. ▼						
Zugewiesene Drahtlosnetzwerke (VSS)	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Profil</th> <th style="width: 40%;">MAC-Adresse</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td>vss-2.default</td> <td>00:a0:f9:0b:cf:e1</td> <td></td> </tr> </tbody> </table>	Profil	MAC-Adresse		vss-2.default	00:a0:f9:0b:cf:e1	
Profil	MAC-Adresse						
vss-2.default	00:a0:f9:0b:cf:e1						

OK
Abbrechen

Abb. 55: Wireless LAN Controller->Slave-AP-Konfiguration->Slave Access Points->

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

Das Menü besteht aus folgenden Feldern:

Felder im Menü Access-Point-Einstellungen

Feld	Beschreibung
Gerät	Zeigt den Gerätetyp des APs.
Standort	Zeigt den Standort des APs. Wenn kein Standort angegeben ist, werden die Standorte nummeriert. Sie können einen anderen Standort eingeben.
Name	Zeigt den Namen des APs. Sie können den Namen ändern.
Beschreibung	Geben Sie eine eindeutige Bezeichnung für den AP ein.
CAPWAP-Verschlüsselung	Wählen Sie aus, ob die Kommunikation zwischen Master und Slaves verschlüsselt werden soll.

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




Felder im Menü Funkmodul 1 oder im Menü Funkmodul 2

Feld	Beschreibung
Betriebsmodus	<p>Zeigt, in welchem Modus das Funkmodul betrieben werden soll. Sie können den Modus ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ein</i> (Standardwert): Das Funkmodul dient als Access Point in Ihrem Netzwerk. • <i>Aus</i>: Das Funkmodul ist nicht aktiv.
Aktives Funkmodulprofil	<p>Zeigt das aktuell gewählte Funkmodulprofil. Sie können ein anderes Funkmodulprofil aus der Liste wählen, wenn mehrere Funkmodulprofile angelegt sind.</p>
Kanal	<p>Zeigt den zugewiesenen Kanal. Sie können einen anderen Kanal wählen.</p> <p>Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.</p> <p>Access Point Modus</p> <p>Durch das Einstellen des Netzwerknamens (SSID) im Access Point Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens vier Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt.</p> <p>Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden APs diese Kanäle auch 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</i> bis <i>13</i> und <i>Auto</i> (Standardwert). • Für Aktives Funkmodulprofil = <i>5 GHz Radio Profile</i> Mögliche Werte sind <i>36</i>, <i>40</i>, <i>44</i>, <i>48</i> und <i>Auto</i> (Standardwert)
Verwendeter Kanal	<p>Nur für Managed APs.</p> <p>Zeigt den aktuell benutzten Kanal.</p>
Sendeleistung	<p>Zeigt die Sendeleistung. Sie können eine andere Sendeleistung wählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet. • <i>5 dBm</i> • <i>8 dBm</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • 11 dBm • 14 dBm • 16 dBm • 17 dBm
Zugewiesene Drahtlosnetzwerke (VSS)	Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

10.3.2 Funkmodulprofile

Slave Access Points	Funkmodulprofile	Drahtlosnetzwerke (VSS)
-------------------------------------	-------------------------	---

Funkmodulprofile	Konfigurierte Funkmodule	Frequenzband	Drahtloser Modus		
2.4 GHz Radio Profile	0	2,4 GHz In/Outdoor	802.11b/g/n		
5 GHz Radio Profile	0	5 GHz Indoor	802.11a/n		


Neu

Abb. 56: **Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile**

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

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

10.3.2.1 Bearbeiten oder Neu

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

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

Funkmodulprofil-Konfiguration	
Beschreibung	<input style="width: 100%;" type="text"/>
Betriebsmodus	Aus ▼
Frequenzband	2,4 GHz In/Outdoor ▼
Anzahl der Spatial Streams	3 ▼
Performance-Einstellungen	
Drahtloser Modus	802.11b/g/n ▼
Max. Übertragungsrate	Auto ▼
Burst-Mode	<input type="checkbox"/> Aktiviert
Airtime Fairness	<input checked="" type="checkbox"/> Aktiviert

Erweiterte Einstellungen	
Kanalplan	Alle ▼
Beacon Period	100 ms
DTIM Period	2
RTS Threshold	2347
Short Guard Interval	<input type="checkbox"/> Aktiviert
Short Retry Limit	7
Long Retry Limit	4
Fragmentation Threshold	2346 Bytes
Wiederkehrender Hintergrund-Scan	<input type="checkbox"/> Aktiviert

OK
Abbrechen

Abb. 57: Wireless LAN Controller->Slave-AP-Konfiguration->Funkmodulprofile->Neu

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

Felder im Menü Funkmodulprofil-Konfiguration

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung des Funkmodulprofils ein.
Betriebsmodus	<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 (Mode 802.11b, Mode 802.11g und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb von Gebäuden betrieben. <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) außerhalb von Gebäuden betrieben. <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h und Mode 802.11n) innerhalb oder außerhalb von Gebäuden betrieben. <i>5,8 GHz Outdoor</i>: Nur für so genannte Broadband Fixed Wireless

Feld	Beschreibung
	Access (BFWA) Anwendungen. Die Frequenzen im Frequenzbereich von 5 755 MHz bis 5 875 MHz dürfen nur in Verbindung mit gewerblichen Angeboten für öffentliche Netzzugänge genutzt werden und bedürfen einer Anmeldung bei der Bundesnetzagentur.
Bandbreite	<p>Nicht für Frequenzband = 2,4 GHz In/Outdoor</p> <p>Wählen Sie aus, wieviele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • 20 MHz (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • 40 MHz: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal.
Anzahl der Spatial Streams	<p>Wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • 3: Drei Datenströme werden verwendet. • 2: Zwei Datenströme werden verwendet. • 1: Ein Datenstrom wird verwendet.

Felder im Menü Performance-Einstellungen

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>802.11a</i>: Ihr Gerät arbeitet ausschließlich nach 802.11a. • <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. • <i>802.11a/n</i>: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n.
Max. Übertragungsrate	<p>Wählen Sie die Übertragungsgeschwindigkeit aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt. • <i><Wert></i>: Je nach Einstellung für Frequenzband, Bandbreite, Anzahl der Spatial Streams und Drahtloser Modus stehen verschiedene feste Werte in MBit/s zur Auswahl.
Burst-Mode	<p>Aktivieren Sie diese Funktion, um die Übertragungsgeschwindigkeit für 802.11g durch Frame Bursting zu erhöhen. Dabei werden mehrere Pakete nacheinander ohne Wartezeiten verschickt. Dies ist besonders effektiv im 11b/g Mischbetrieb.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion nicht aktiv sein.</p>
Airtime Fairness	<p>Diese Funktion ist nicht für alle Geräte verfügbar.</p> <p>Mit der Airtime Fairness -Funktion wird gewährleistet, dass Sendersourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.</p>

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

Felder im Menü Erweiterte Einstellungen

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.

Feld	Beschreibung
Benutzerdefinierter Kanalplan	<p>Nur für Kanalplan = <i>Benutzerdefiniert</i></p> <p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <p>Mit Hinzufügen können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen.</p> <p>Mithilfe von -Symbol können Sie Einträge löschen.</p>
Beacon Period	<p>Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an.</p> <p>Dieser Wert wird in Beacon und Probe Response Frames übermittelt.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>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>
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>

Feld	Beschreibung
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>

10.3.3 Drahtlosnetzwerke (VSS)

Slave Access Points
Funkmodulprofile
Drahtlosnetzwerke (VSS)

VSS-Beschreibung	Netzwerkname (SSID)	Anzahl der zugeordneten Funkmodule	Sicherheit	Status	Aktion		
vss-2	default	0	Inaktiv				

Nicht zugewiesenes VSS allen Funkmodulen zuweisen
START

Neu


Abb. 58: Wireless LAN Controller->Slave-AP-Konfiguration->Drahtlosnetzwerke (VSS)

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

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

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

10.3.3.1 Bearbeiten oder Neu

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

Slave Access Points

Funkmodulprofile

Drahtlosnetzwerke (VSS)

Service Set Parameter

Netzwerkname (SSID)	<input type="text"/>	<input checked="" type="checkbox"/> Sichtbar
Intra-cell Repeating	<input checked="" type="checkbox"/> Aktiviert	
ARP Processing	<input type="checkbox"/> Aktiviert	
WMM	<input checked="" type="checkbox"/> Aktiviert	
Sicherheitseinstellungen		
Sicherheitsmodus	Inaktiv ▾	
Client-Lastverteilung		
Max. Anzahl Clients - Hard Limit	<input type="text" value="32"/>	
Max. Anzahl Clients - Soft Limit	<input type="text" value="28"/>	
Auswahl des Client-Bands	Deaktiviert, optimiert für Fast Roaming ▾	
MAC-Filter		
Zugriffskontrolle	<input type="checkbox"/> Aktiviert	
Dynamische Black List	<input checked="" type="checkbox"/> Aktiviert	
Fehlversuche per Zeitraum	<input type="text" value="10"/> <input type="text" value="60"/>	Sekunden
Sperrzeit für Black List	<input type="text" value="500"/>	Sekunden
VLAN		
VLAN	<input type="checkbox"/> Aktiviert	
Bandbreitenbeschränkung für jeden WLAN-Client		
Rx Shaping	Keine Begrenzung ▾	
Tx Shaping	Keine Begrenzung ▾	

OK

Abbrechen

Abb. 59: Wireless LAN Controller->Slave-AP-Konfiguration->Drahtlosnetzwerke (VSS)->Neu

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

Felder im Menü Service Set Parameter

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

Feld	Beschreibung
	Beachten Sie, dass ARP Processing nicht zusammen mit der Funktion MAC-Bridge angewendet werden kann.
WMM	<p>Wählen Sie aus, ob für das Drahtlosnetzwerk Sprach- oder Videodaten-Priorisierung mittels WMM (Wireless Multimedia) aktiviert sein soll, um stets eine optimale Übertragungsqualität bei zeitkritischen Anwendungen zu erreichen. Es wird Datenpriorisierung nach DSCP (Differentiated Services Code Point) oder IEEE802.1d unterstützt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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, z. B. <i>hallo</i> für <i>WEP 40</i>, <i>wep104</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA und 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 und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p>

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

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
Max. Anzahl Clients - Hard Limit	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf 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>

Feld	Beschreibung
	Der Standardwert ist <i>32</i> .
Max. Anzahl Clients - Soft Limit	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Um eine vollständige Auslastung eines Radiomoduls zu vermeiden, können Sie hier eine "weiche" Begrenzung der Anzahl verbundener Clients vornehmen. Wird diese Anzahl erreicht, werden neue Verbindungsanfragen zunächst abgelehnt. Findet der Client kein anderes Drahtlosnetzwerk und wiederholt daher seine Anfrage, wird die Verbindung akzeptiert. Erst bei Erreichen des Max. Anzahl Clients - Hard Limit werden Anfragen strikt abgelehnt.</p> <p>Der Wert der Max. Anzahl Clients - Soft Limit muss gleich oder kleiner sein als der Max. Anzahl Clients - Hard Limit.</p> <p>Der Standardwert ist <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	Legen Sie Einträge mit Hinzufügen an und geben Sie die MAC-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.
Dynamische Black List	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

Feld	Beschreibung
	<p>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 <i>2</i> bis <i>4094</i>.</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</i> (Standardwert) • <i>1 Mbit/s, 1 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>1 Mbit/s, 1 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>

10.4 Monitoring

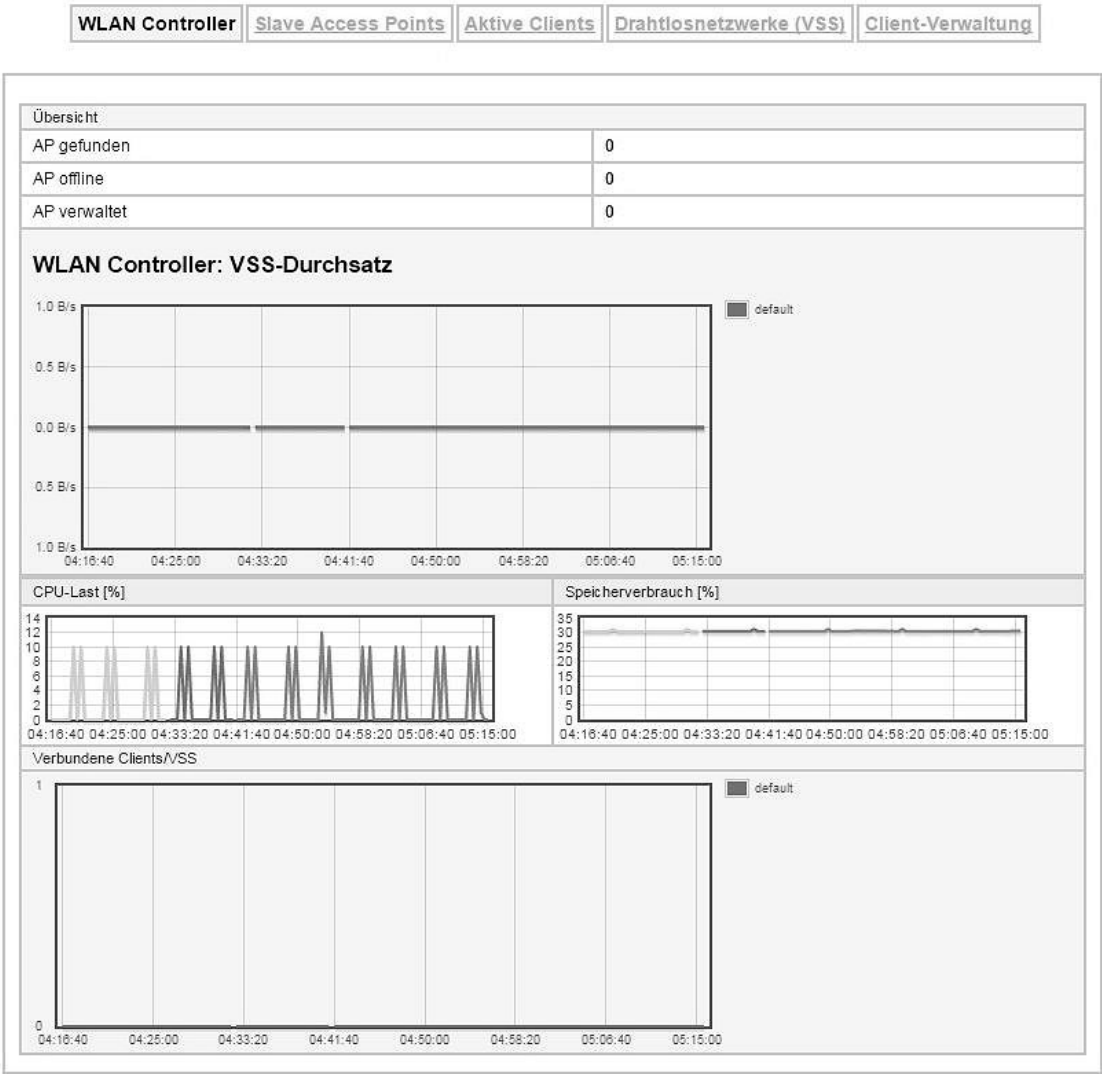
Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.



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.

10.4.1 WLAN Controller



10.4.2 Slave Access Points

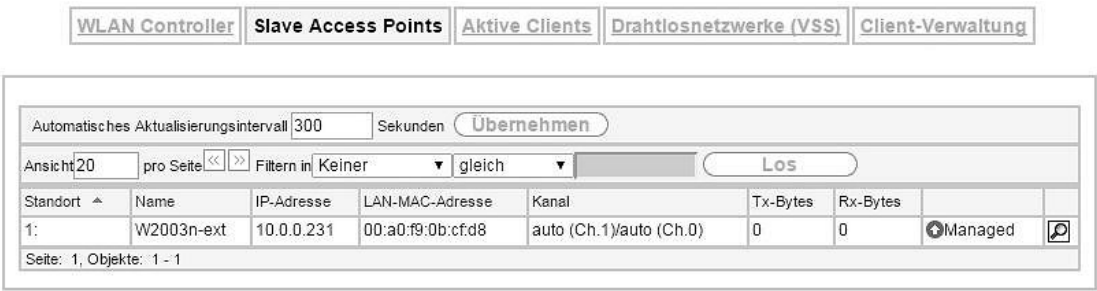


Abb. 61: Wireless LAN Controller->Monitoring->Slave Access Points

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**.

10.4.2.1 Übersicht

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

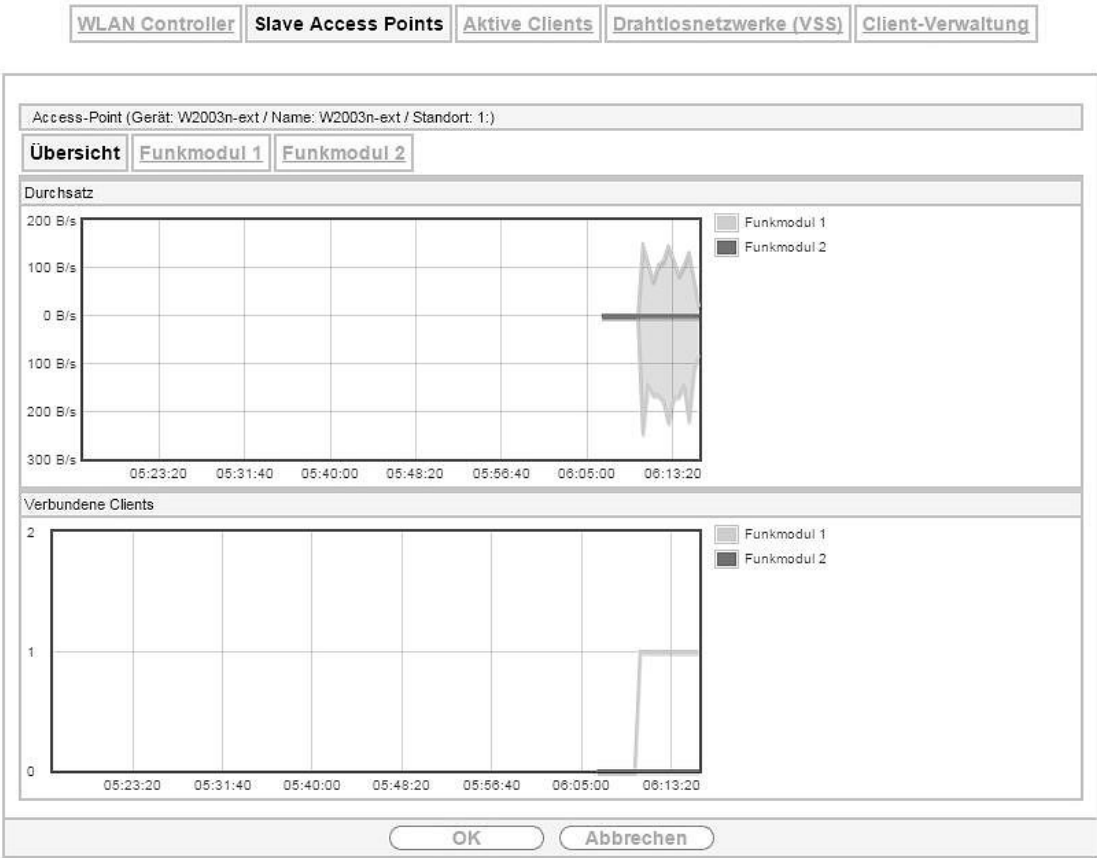


Abb. 62: Wireless LAN Controller->Monitoring->Slave Access Points->Übersicht

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 zeitabhän-

Status	Bedeutung
	gig an.

10.4.2.2 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.

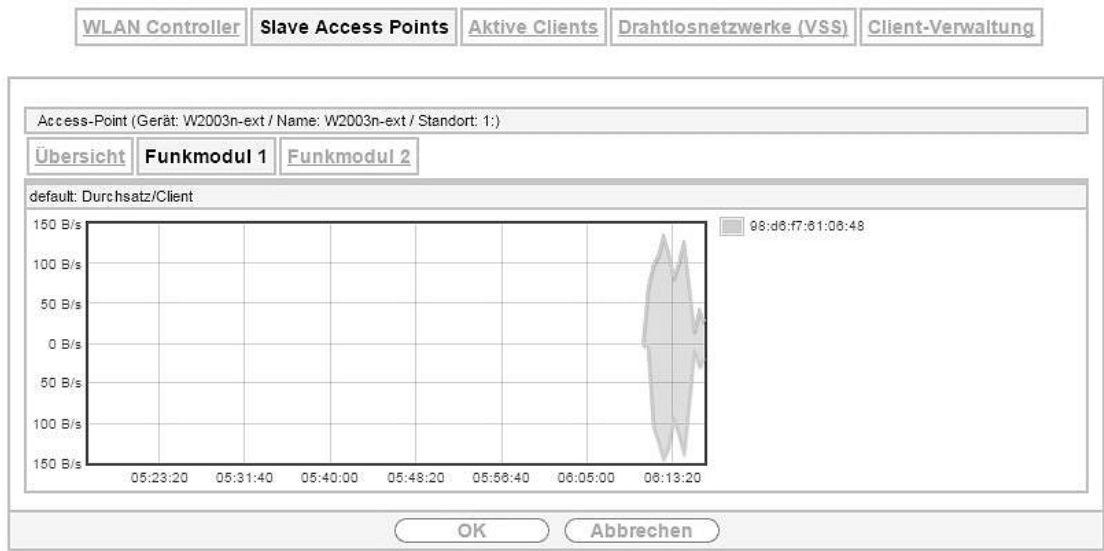


Abb. 63: Wireless LAN Controller->Monitoring->Slave Access Points->Funkmodul

Werte in der Liste Funkmodul

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

10.4.3 Aktive Clients

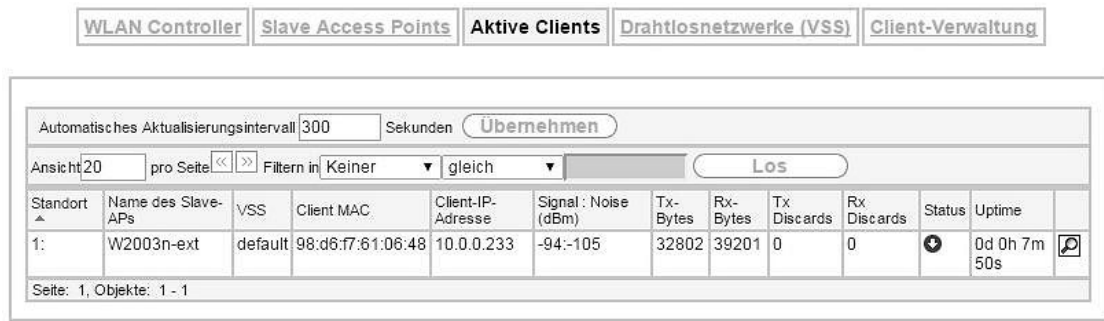


Abb. 64: Wireless LAN Controller->Monitoring->Aktive Clients


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

Für jeden Client sehen Sie einen Eintrag mit folgendem Parametersatz: **Standort, Name 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.
Angemeldet	Der Client meldet sich gerade beim WLAN an.

Status	Bedeutung
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.



10.4.5 Client-Verwaltung

WLAN Controller

Slave Access Points

Aktive Clients

Drahtlosnetzwerke (VSS)

Client-Verwaltung

Ansicht20

pro Seite<<>>

Filtern inKeiner

gleich

Los

Standort ^	Name des Slave-APs	VSS	MAC-Adresse (VSS)	Aktive Clients	2,4/5-GHz-Übergang	Abgewiesene Clients soft/hard	
1:	W2003n-ext	default	00:a0:f9:0b:cf:e1	0	0	0/0	
1:	W2003n-ext	default	00:a0:f9:0b:cf:e0	1	0	0/0	

Seite: 1, Objekte: 1 - 2

Übernehmen

Abb. 67: Wireless LAN Controller->Monitoring+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.

10.5 Umgebungs-Monitoring

Dieses Menü dient zur Überwachung entfernter Access Points und Clients.

10.5.1 Benachbarte APs

Benachbarte APs

Rogue APs

Rogue Clients

Ansicht	20	pro Seite	<<	>>	Filtern in	Keiner	>	gleich	>	Los
SSID	MAC-Adresse	Signal dBm	Kanal	Sicherheit	Zuletzt gesehen	Stärkstes Signal empfangen von	Summe der Erkennungen			
Bintec-Dev-Data	02:a0:f9:0b:cf:e8	-91	1	WPA and WPA 2 PSK	12.03.2000, 05:42:59	1:-W2003n-ext	1			
Bintec-Dev-Voice	00:a0:f9:0b:cf:e8	-91	1	WPA and WPA 2 PSK	12.03.2000, 05:42:59	1:-W2003n-ext	1			
Seite: 1, Objekte: 1 - 2										
Aktionen										
Benachbarte APs neu scannen				START						

Abb. 68: Wireless LAN Controller+Umgebungs-Monitoring->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 Sicherheitseinstel-

lungen 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.

10.5.2 Rogue APs

Benachbarte APs **Rogue APs** Rogue Clients

Ansicht 20
pro Seite << >>
Filtern in: Keiner ▼ gleich ▼
Los

SSID ▲	MAC-Adresse	Signal dBm	Kanal	Zuletzt gesehen	Gefunden durch AP	Angenommen
Seite: 1						
Aktionen						
Benachbarte APs neu scannen		START				

OK

Abb. 69: Wireless LAN Controller+Umgebungs-Monitoring->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.

10.5.3 Rogue Clients

Benachbarte APs Rogue APs **Rogue Clients**

Ansicht 20
pro Seite << >>
Filtern in: Keiner ▼ gleich ▼
Los

MAC-Adresse des Rogue Clients ▲	Netzwerkname (SSID)	Angegriffener Access Point	Signal dBm	Art des Angriffs	Zuerst gesehen	Zuletzt gesehen	Statische Black List Alle auswählen/ Alle deaktivieren	Löschen Alle auswählen/ Alle deaktivieren
Seite: 1								


Neu Übernehmen

Abb. 70: Wireless LAN Controller+Umgebungs-Monitoring->Rogue Clients

Im Menü **Wireless LAN Controller+Umgebungs-Monitoring->Rogue Clients** werden die Clients an-

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

10.5.3.1 Neu

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

Benachbarte APs Rogue APs **Rogue Clients**

Neuer Eintrag in die Blacklist

MAC-Adresse des Rogue Clients	
Netzwerkname (SSID)	Eine auswählen ▼

OK Abbrechen

Abb. 71: **Wireless LAN Controller+Umgebungs-Monitoring->Rogue Clients->Neu**

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.

10.6 Wartung

Dieses Menü dient zur Wartung Ihrer managed Access Points.

10.6.1 Firmware-Wartung

Firmware-Wartung

Managed Access Points

Ansicht 20
pro Seite << >>
Filtern in Keine
gleich
Los

Firmware aktualisieren Alle auswählen/ Alle deaktivieren	Standort	Gerät	IP-Adresse	LAN-MAC-Adresse	Firmware-Version	Status
<input type="checkbox"/>	1:	W2003n-ext	10.0.0.231	00:a0:f9:0b:cf:d8	V.9.1 Rev. 10 (Patch 2) IPSec from 2014/08/29 00:00:00	

Seite: 1, Objekte: 1 - 1

Aktion

Systemsoftware aktualisieren

Quelle

HTTP-Server

URL

OK
Abbrechen

Abb. 72: Wireless LAN Controller->Wartung->Firmware-Wartung

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

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

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

Mögliche Werte für Status

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

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

Felder im Menü Firmware-Wartung

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

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

Kapitel 11 Netzwerk

11.1 Routen

Standard-Route (Default Route)


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

11.1.1 Konfiguration von IPv4-Routen

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

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse** = 192.168.2.0, **Netzmaske** = 255.255.255.0, **Gateway** = 192.168.2.1, **Schnittstelle** = LAN_EN1-0, **Routentyp** = *Netzwerkroute via Schnittstelle* angezeigt,

11.1.1.1 Bearbeiten oder Neu

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

Konfiguration von IPv4-Routen	IPv6-Routenkonfiguration	IPv4-Routing-Tabelle	IPv6-Routingtabelle	Optionen
<div> <div>Basisparameter</div> <div> Routentyp <div>Netzwerkroute via Schnittstelle ▼</div> </div> <div> Schnittstelle <div>Keine ▼</div> </div> <div> Routenklasse <div> <input checked="" type="radio"/> Standard <input type="radio"/> Erweitert </div> </div> <div>Routenparameter</div> <div> Ziel-IP-Adresse/Netzmaske <div> <input type="text"/> / <input type="text"/> </div> </div> <div> Lokale IP-Adresse <div><input type="text" value="0.0.0.0"/></div> </div> <div> Metrik <div><input type="text" value="1"/></div> </div> </div> <div> <div>OK</div> <div>Abbrechen</div> </div>				

Abb. 73: **Netzwerk->Routen->Konfiguration von IPv4-Routen->Neu** mit **Routenklasse** = Standard.

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

Konfiguration von IPv4-Routen

IPv6-Routenkonfiguration

IPv4-Routing-Tabelle

IPv6-Routingtabelle

Optionen

Basisparameter

Routentyp

Netzwerkroute via Schnittstelle

Schnittstelle

Keine

Routenklasse

Standard

Erweitert

Routenparameter

Ziel-IP-Adresse/Netzmaske

Lokale IP-Adresse

0.0.0.0

Metrik

1

Erweiterte Routenparameter

Beschreibung

Quellschnittstelle

Beliebig

Quell-IP-Adresse/Netzmaske

0.0.0.0 / 0.0.0.0

Layer 4-Protokoll

Beliebig

Quell-Port

Beliebig

Port

-1

bis Port

-1

Zielport

Beliebig

Port

-1

bis Port

-1

DSCP-/TOS-Wert

Nicht beachten

Modus

Wählen und warten

OK


Abbrechen

Abb. 74: Netzwerk->Routen->Konfiguration von IPv4-Routen ->Neu mit Routenklasse Erweitert = Aktiviert

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.</p>

Feld	Beschreibung
	<p>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-Informationen zu einem bestimmten Netzwerk ergänzt. <div>  Hinweis <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</i>, <i>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> <p>Bei Routentyp = <i>Netzwerkroute via Schnittstelle</i></p> <p>Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein.</p>

Feld	Beschreibung
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> <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>Einzel</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 (einzeln 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>


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>Einzel</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>
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 benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. • <i>Verbindlich</i>: Die Route ist immer benutzbar. • <i>Wählen und fortfahren</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist.


Feld	Beschreibung
	<ul style="list-style-type: none">• <i>Nie einwählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist.• <i>Immer wählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

11.1.2 IPv6-Routenkonfiguration

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

11.1.2.1 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.

Konfiguration von IPv4-Routen

IPv6-Routenkonfiguration

IPv4-Routing-Tabelle

IPv6-Routingtabelle

Optionen

Routenparameter

Beschreibung

Route aktiv

☒ Aktiviert

Routentyp

Netzwerkroute via Gateway ▾

Zielschnittstelle

Eine auswählen ▾

Quelladresse/Länge

/64

Zieladresse/Länge

/64

Gateway-Adresse

OK

Abbrechen

Abb. 75: **Netzwerk->Routen->IPv6-Routenkonfiguration->Neu**

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

Felder im Menü Routenparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die IPv6-Route an.
Route aktiv	Wählen Sie, ob die Route aktiv oder inaktiv sein soll. Mit <i>Aktiviert</i> wird die Route auf den Status aktiv gesetzt. Standardmäßig ist die Funktion aktiv.
Routentyp	Wählen Sie die Art der Route aus. Mögliche Werte: <ul style="list-style-type: none">• <i>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 verfü-

Feld	Beschreibung
	<p>bar ist.</p> <ul style="list-style-type: none"> • <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>
Gateway-Adresse	Geben Sie die IPv6-Adresse für den nächsten Hop ein.

11.1.3 IPv4-Routing-Tabelle

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

Im Auslieferungszustand wird ein vordefinierter Eintrag mit den Parametern **Ziel-IP-Adresse** = `192.168.2.0`, **Netzmaske** = `255.255.255.0`, **Gateway** = `192.168.2.1`, **Schnittstelle** = `LAN_EN1-0`, **Routentyp** = *Netzwerkroute via Schnittstelle*, **Protokoll** = *Lokal* angezeigt,


Konfiguration von IPv4-Routen	IPv6-Routenkonfiguration	IPv4-Routing-Tabelle	IPv6-Routingtabelle	Optionen
---	--	-----------------------------	-------------------------------------	--------------------------

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los								
Ziel-IP-Adresse	Netzmaske	Gateway	Schnittstelle	Metrik	Routentyp	Erweiterte Route	Protokoll	
0.0.0.0	0.0.0.0	0.0.0.0	WAN_INITIAL_CONTACT	1	Standardroute über Gateway	<input type="checkbox"/>	Lokal	
10.0.0.0	255.0.0.0	10.0.0.165	BRIDGE_BR0	0	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	Lokal	
172.16.0.0	255.255.0.0	172.16.98.127	LAN_EN1-4	0	Netzwerkroute via Schnittstelle	<input type="checkbox"/>	Lokal	
Seite: 1, Objekte: 1 - 3								

Abb. 76: **Netzwerk->Routen->IPv4-Routing-Tabelle**

Felder im Menü IPv4-Routing-Tabelle

Feld	Beschreibung
Ziel-IP-Adresse	Zeigt die IP-Adresse des Ziel-Hosts bzw. Zielnetzes an.

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

11.1.4 IPv6-Routingtabelle

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

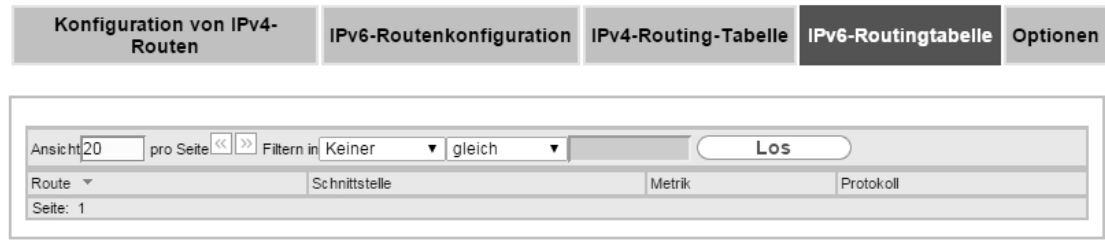


Abb. 77: **Netzwerk->Routen->IPv6-Routingtabelle**

Felder im Menü IPv6-Routingtabelle

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.

11.1.5 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.

Konfiguration von IPv4-Routen

IPv6-Routenkonfiguration

IPv4-Routing-Tabelle

IPv6-Routingtabelle

Optionen

Überprüfung der Rückroute

Modus

☐ Für alle Schnittstellen aktivieren

☒ Für bestimmte Schnittstellen aktivieren

☐ Für alle Schnittstellen deaktivieren

Ansicht20

pro Seite<<>>

Filtern inKeiner gleich

Los

Nr.	Schnittstelle	Überprüfung der Rückroute
1	en1-4	<input type="checkbox"/> Aktiviert
2	efm35-60	<input type="checkbox"/> Aktiviert
3	ethoa35-5	<input type="checkbox"/> Aktiviert
4	Initial_Contact	<input type="checkbox"/> Aktiviert
5	br0	<input type="checkbox"/> Aktiviert

Seite: 1, Objekte: 1 - 5

OK

Abbrechen

Abb. 78: Netzwerk->Routen->Optionen

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>

11.2 Allgemeine IPv6-Präfixe

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

Das Konzept der Allgemeinen Präfixe hat zwei entscheidende Vorteile:


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

Um IPv6 zu verwenden, müssen Sie konfigurieren, wie Sie Subnetze und IPv6-Adressen festlegen und verteilen lassen wollen (siehe "IPv6-Adressen konfigurieren unter [Schnittstellen](#) auf Seite 64 sowie die für IPv6 relevanten Parameter im Menü **LAN->IP-Konfiguration->Schnittstellen**).

11.2.1 Konfiguration eines Allgemeinen Präfixes

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

11.2.1.1 Bearbeiten oder Neu

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

Konfiguration eines Allgemeinen Präfixes

Basisparameter	
Aktiver Allgemeiner Präfix	<input checked="" type="checkbox"/> Aktiviert
Name	<input type="text"/>
Typ	<input checked="" type="radio"/> Dynamisch <input type="radio"/> Statisch
Von Schnittstelle	<input type="text" value="Eine auswählen"/>

Abb. 79: **Netzwerk->Allgemeine IPv6-Präfixe->Konfiguration eines Allgemeinen Präfixes->Neu**

Optionen im Menü Basisparameter

Feld	Beschreibung
Aktiver Allgemeiner Präfix	<p>Wählen Sie, ob das Präfix aktiv oder inaktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird das Präfix auf den Status aktiv gesetzt.</p> <p>Standardmäßig ist das Präfix aktiv.</p>
Name	<p>Geben Sie einen Namen für das Allgemeine Präfix ein.</p> <p>Ein sprechender Name dient dazu, das Allgemeine Präfix aus einer Präfixliste leichter auswählen zu können.</p>
Typ	<p>Wählen Sie, wie der Adressraum zugewiesen werden soll.</p> <p>Mögliche Werte:</p>

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

11.3 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 133).

Konkrete Hinweise für die Konfiguration von NAT finden Sie am Ende des Kapitels unter [NAT - Konfigurationsbeispiel](#) auf Seite 138.

11.3.1 NAT-Schnittstellen

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

NAT-Schnittstellen
NAT-Konfiguration

Schnittstelle	NAT aktiv	Loopback aktiv	Verwerfen ohne Rückmeldung	PPTP-Passthrough	Portweiterleitungen
BRIDGE_BR0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-0-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WAN_EFM35-60	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
WLAN_STA7-90	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Seite: 1, Objekte: 1 - 5

OK
Abbrechen

Abb. 80: **Netzwerk->NAT->NAT-Schnittstellen**

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

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

Optionen im Menü NAT-Schnittstellen

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

11.3.2 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.

11.3.2.1 Neu

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

NAT-Schnittstellen

NAT-Konfiguration

Basisparameter

Beschreibung

Schnittstelle

Beliebig

Art des Datenverkehrs

eingehend (Ziel-NAT)

Ursprünglichen Datenverkehr angeben

Dienst

Benutzerdefiniert

Protokoll

Beliebig

Quell-IP-Adresse/Netzmaske

Beliebig

Original Ziel-IP-Adresse/Netzmaske

Beliebig

Substitutionswerte

Neue Ziel-IP-Adresse/Netzmaske

Host0.0.0.0

OK

Abbrechen

Abb. 81: Netzwerk->NAT->NAT-Konfiguration ->Neu

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

Feld im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für die NAT-Konfiguration ein.
Schnittstelle	<p>Wählen Sie die Schnittstelle, für die NAT konfiguriert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">Beliebig (Standardwert): NAT wird für alle Schnittstellen konfiguriert.<Schnittstellename>: 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">eingehend (Ziel-NAT) (Standardwert): Der Datenverkehr, der von außen kommt.ausgehend (Quell-NAT): Der Datenverkehr, der nach außen geht.exklusiv (ohne NAT): 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">full-cone (nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiiierende Quelladresse und den initialen Quellport senden.restricted-cone (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>port-restricted-cone</i> (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • <i>symmetrisch</i> (Standardwert) Für beliebige Protokolle: In ausgehender Richtung werden eine extern gültige Quelladresse und ein extern gültiger Quell-Port administrativ festgelegt. In eingehender Richtung sind nur Antwortpakete innerhalb der bestehenden Verbindung zugelassen.

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

Felder im Menü Ursprünglichen Datenverkehr angeben

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IGMP</i> • <i>IGP</i> • <i>IGRP</i> • <i>IP</i> • <i>IPinIP</i> • <i>IPv6</i> • <i>IPX in IP</i> • <i>ISO-IP</i> • <i>Kryptolan</i> • <i>L2TP</i> • <i>OSPF</i> • <i>PUP</i> • <i>RDP</i> • <i>RSVP</i> • <i>SKIP</i> • <i>TCP</i> • <i>TLSP</i> • <i>UDP</i> • <i>VRRP</i> • <i>XNS-IDP</i>
Quell-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i> oder <i>exklusiv (ohne NAT)</i></p> <p>Geben Sie die Quell-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
Original Ziel-IP-Adresse/Netzmaske	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i></p> <p>Geben Sie die Ziel-IP-Adresse und gegebenenfalls die zugehörige Netzmaske der ursprünglichen Datenpakete ein.</p>
Original Ziel-Port/Bereich	<p>Nur für Art des Datenverkehrs = <i>eingehend (Ziel-NAT)</i>, Dienst = <i>Benutzerdefiniert</i> und Protokoll = <i>TCP, UDP, TCP/UDP</i></p> <p>Geben Sie den Ziel-Port bzw. den Ziel-Port-Bereich der 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> <p>Wenn Sie <i>Port angeben</i> wählen, können Sie einen einzelnen Port angeben, mit der Auswahl von <i>Portbereich angeben</i> können Sie einen zusammenhängenden Bereich von Ports definieren, der als Filter für den</p>

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

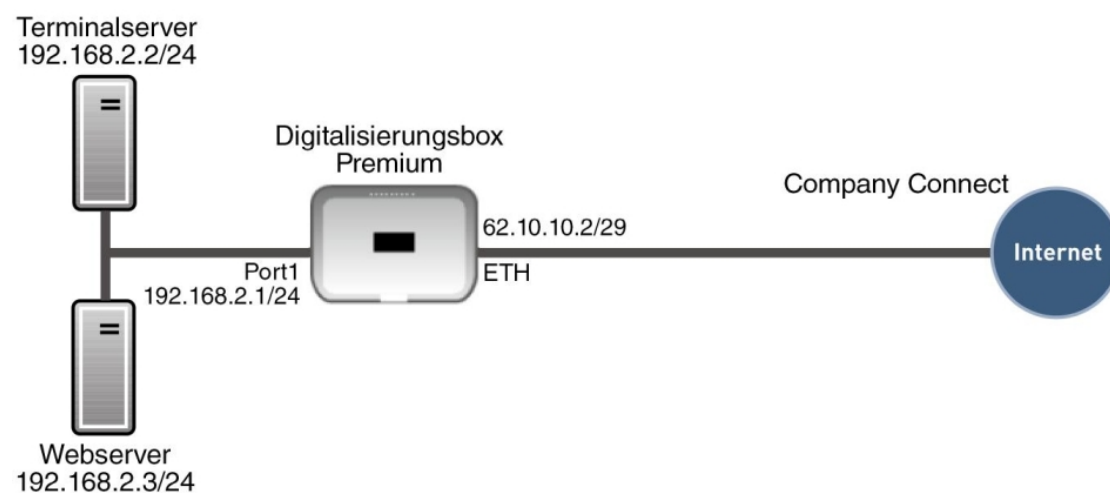
Feld	Beschreibung
	<p>auf den der ursprüngliche Quell-Port umgesetzt werden soll.</p> <p>Mit Auswahl von <i>Original</i> belassen Sie den ursprünglichen Quell-Port. Wenn Sie <i>Original</i> deaktivieren, erscheint ein Eingabefeld und Sie können einen neuen Quell-Port eingeben. Standardmäßig ist <i>Original</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>Original Port/Bereich beginnt mit</i>: Es erscheint ein Eingabefeld, in das Sie die Portnummer eingeben können, bei der der Portbereich beginnen soll, durch den der ursprüngliche Portbereich ersetzt wird. Die Anzahl der Ports bleibt dabei gleich.

11.3.3 NAT - Konfigurationsbeispiel

Voraussetzungen

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

Beispielszenario



Konfigurationsziel

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

Konfigurationsschritte im Überblick

NAT einschalten

Feld	Menü	Wert
NAT aktiv	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für <i>LAN_EN5-0</i>

Feld	Menü	Wert
Verwerfen ohne Rückmeldung	Netzwerk -> NAT -> NAT-Schnittstellen	Aktiviert für <i>LAN_EN5-0</i>

NAT-Freigaben konfigurieren

Feld	Menü	Wert
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>GUI</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>
Original Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>Host, z. B. 62.10.10.2</i>
Original Ziel-Port/Bereich	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>80</i>
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>127.0.0.1</i>
Neuer Ziel-Port	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	<i>Original deaktiviert, 80</i>

Webserver

Feld	Menü	Wert
Beschreibung	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	z. B. <i>Webserver</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>http</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	z. B. <i>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>

Feld	Menü	Wert
Original Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	96
Original Ziel-Port/Bereich	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	3389
Neue Ziel-IP-Adresse/Netzmaske	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	Host, z. B. 192.168.2.2
Neuer Ziel-Port	Netzwerk -> NAT -> NAT-Konfiguration -> Neu	Original


11.4 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.

11.4.1 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.

11.4.1.1 Neu

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

Lastverteilungsgruppen
Special Session Handling

Basisparameter				
Gruppenbeschreibung	<input style="width: 90%;" type="text"/>			
Verteilungsrichtlinie	Sitzungs-Round-Robin ▼			
Verteilungsmodus	<input checked="" type="radio"/> Immer <input type="radio"/> Nur aktive Schnittstellen verwenden			
Schnittstellenauswahl für Verteilung				
Schnittstelle	Verteilungsverhältnis	Routenselektor	IP-Adresse zur Nachverfolgung	
<input type="button" value="Hinzufügen"/>				
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>				

Abb. 82: **Netzwerk->Lastverteilung->Lastverteilungsgruppen->Neu**

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

Felder im Menü Basisparameter

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

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

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

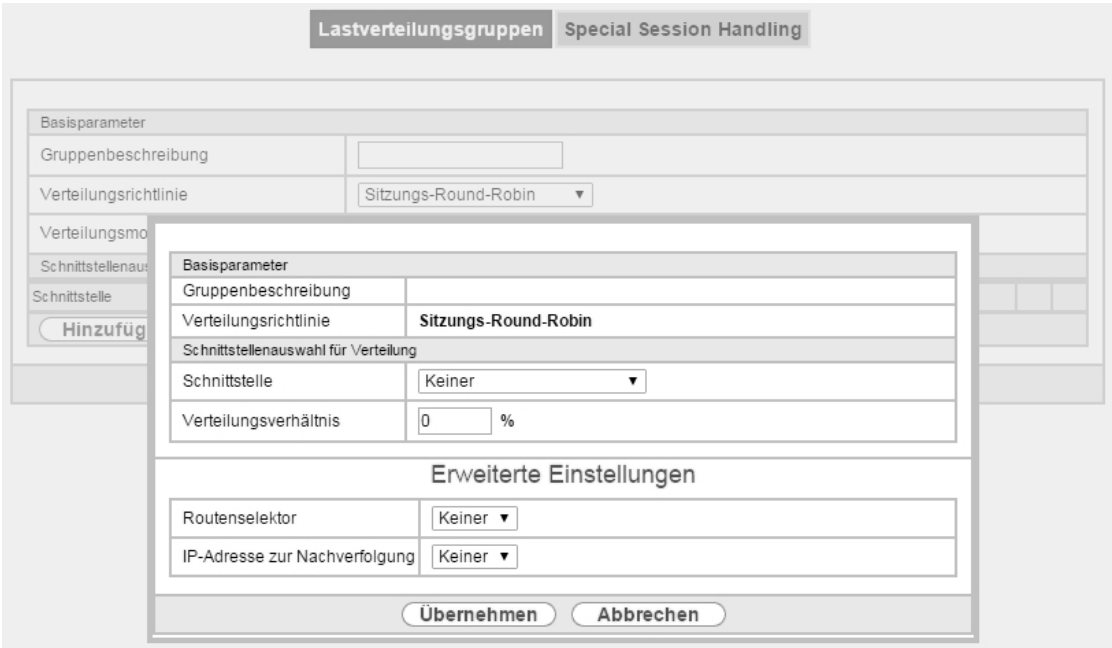


Abb. 83: Netzwerk->Lastverteilung->Lastverteilungsgruppen->Hinzufügen

Felder im Menü Basisparameter

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

Felder im Menü Schnittstellenauswahl für Verteilung

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Routenselektor	<p>Der Parameter Routenselektor ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routininformation erweitert. Der Routenselektor ist in bestimmten Anwendungsfällen notwendig, um die vom Router verwalteten IP Sessions eindeutig je Loadbalancing -Gruppe bilanzieren zu können. Für die Anwendung des Parameters gelten folgende Regeln:</p> <ul style="list-style-type: none">Ist eine Schnittstelle nur einer Lastverteilungsgruppe zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig.Ist eine Schnittstelle mehreren Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich.

Feld	Beschreibung
	<ul style="list-style-type: none"> Innerhalb einer Lastverteilungsgruppe muss der Routenselektor aller Schnittstelleneinträge identisch konfiguriert sein. <p>Wählen Sie die Ziel-IP-Adresse der gewünschten Route aus.</p> <p>Sie können unter allen Routen und allen erweiterten Routen wählen.</p>
IP-Adresse zur Nachverfolgung	<p>Mit dem Parameter IP-Adresse zur Nachverfolgung können Sie eine bestimmte Route überwachen lassen.</p> <p>Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die 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 Auszuführende Aktion überwacht werden (Aktion = <i>Überwachen</i>) .</p>

11.4.2 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** angenommen.

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 **Zielpport** (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.

11.4.2.1 Bearbeiten oder Neu

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

Lastverteilungsgruppen

Special Session Handling

Basisparameter	
Admin-Status	<input checked="" type="checkbox"/> Aktiviert
Beschreibung	<input type="text"/>
Dienst	Benutzerdefiniert ▾
Protokoll	Beliebig ▾
Ziel-IP-Adresse/Netzmaske	Beliebig ▾
Quellschnittstelle	Beliebig ▾
Quell-IP-Adresse/Netzmaske	Beliebig ▾
Special Handling Timer	<input type="text" value="900"/> Sekunden

Erweiterte Einstellungen

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

OK

Abbrechen

Abb. 84: Netzwerk->Lastverteilung->Special Session Handling->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob Special Session Handling aktiv sein soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.
Dienst	Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem: <ul style="list-style-type: none">• <i>activity</i>• <i>apple-qt</i>• <i>auth</i>• <i>chargen</i>• <i>clients_1</i>• <i>daytime</i>• <i>dhcp</i>• <i>discard</i>

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

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

Felder im Menü Erweiterte Einstellungen

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

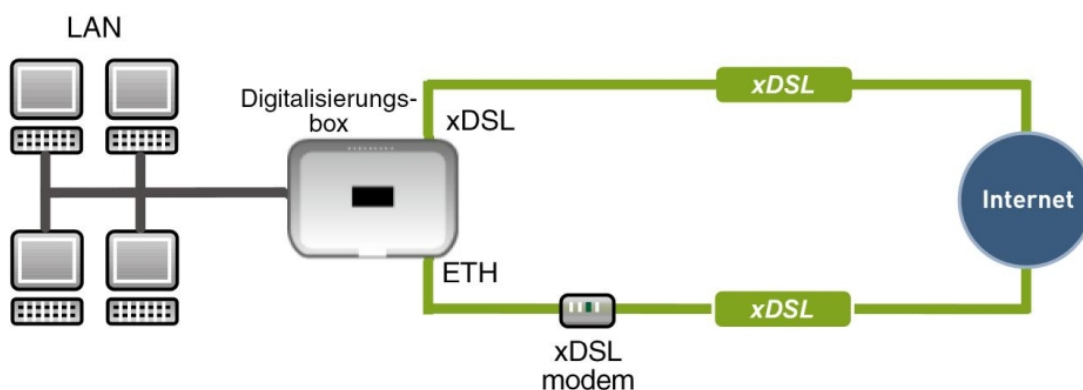
Feld	Beschreibung
	<p>Standardmäßig sind die beiden Parameter Zieladresse und Zielport aktiv.</p> <p>Belassen Sie die Voreinstellung <i>Aktiviert</i> bei einem oder bei beiden Parametern, so muss der Wert des jeweiligen Parameters bei den später gesendeten Datenpaketen derselbe sein wie beim ersten Datenpaket.</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>

11.4.3 Lastverteilung - Konfigurationsbeispiel

Voraussetzungen

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

Beispielszenario



Konfigurationsziel

- Der Datenverkehr wird auf Basis von IP-Sitzungen jeweils zur Hälfte auf die beiden DSL-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 DSL-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 verbindungsspezifisch verwendet werden. Die Konfiguration der DNS-Server wird beim Anlegen der DSL-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 -> Internet -> Internetverbindungen -> Neu	<i>Internes DSL-Modem</i>
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>DSL-1</i>
Typ	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Benutzerdefiniert über PPPoE (PPP über Ethernet)</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>fes-te_ip@provider.de</i>
Passwort	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>test12345</i>

**Hinweis**

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

Zweite Internetverbindung einrichten

Feld	Menü	Wert
Verbindungstyp	Assistenten -> Internet -> Internetverbindungen -> Neu	<i>Externes Gateway/Kabelmodem</i>
Beschreibung	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>DSL-2</i>
Physischer Ethernet-Port	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>ETH5</i>
Typ	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	<i>Benutzerdefiniert</i>
Benutzername	Assistenten -> Internet -> Internetverbindungen -> Neu -> Weiter	z. B. <i>#0001@t-online.de</i>
Passwort	Assistenten -> Internet -> 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_DSL-1</i>
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>50</i>
Schnittstelle	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>WAN_DSL-2</i>
Verteilungsverhältnis	Netzwerk -> Lastverteilung -> Lastverteilungsgruppen -> Neu -> Hinzufügen	<i>50</i>

Special Session Handling

Feld	Menü	Wert
Beschreibung	Netzwerk -> Lastverteilung -> Special Sessi-	z. B. <i>HTTPS</i>

Feld	Menü	Wert
	on Handling -> Neu	
Dienst	Netzwerk -> Lastverteilung -> Special Session Handling -> Neu	<i>http (SSL)</i>
Special Handling Timer	Netzwerk -> Lastverteilung -> Special Session Handling -> Neu	<i>900 Sekunden</i>

11.5 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

11.5.1 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**.

11.5.1.1 Neu

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

IPv4/IPv6-Filter

QoS-Klassifizierung

QoS-Schnittstellen/Richtlinien

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	any ▼
IPv4-Zieladresse/-netzmaske	Beliebig ▼
IPv6-Zieladresse/-länge	Beliebig ▼
IPv4-Quelladresse/-netzmaske	Beliebig ▼
IPv6-Quelladresse/-länge	Beliebig ▼
DSCP / Traffic Class Filter (Layer 3)	Nicht beachten ▼
COS-Filter (802.1p/Layer 2)	Nicht beachten ▼

OK

Abbrechen

Abb. 85: **Netzwerk->QoS->IPv4/IPv6-Filter->Neu**

Das Menü **Netzwerk->QoS->IPv4/IPv6-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Der Standardwert ist <i>any</i>.</p>
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Wählen Sie einen Typ aus.</p> <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> <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>

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 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 Quell-IP-Adresse/Länge ist nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Quell-Netzwerk-Adresse und die Präfixlänge ein.
Quell-Port/Bereich	<p>Nur für Protokoll = <i>TCP</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
2)	Mögliche Werte sind ganze Zahlen zwischen 0 und 7. Wertebereich 0 bis 7. Der Standardwert ist <i>Nicht beachten</i> .

11.5.2 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.

11.5.2.1 Neu

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

IPv4/IPv6-Filter

QoS-Klassifizierung

QoS-Schnittstellen/Richtlinien

Basisparameter

Klassenplan

Neu ▾

Beschreibung

Filter

Eine auswählen ▾

Richtung

Ausgehend ▾

High-Priority-Klasse

☐

Klassen-ID

1 ▾

DSCP/Traffic-Class-Filter setzen (Layer 3)

Erhalten ▾

Setze COS Wert (802.1p/Layer 2)

Erhalten ▾

Schnittstellen

Schnittstelle

Hinzufügen

OK


Abbrechen

Abb. 86: Netzwerk->QoS->QoS-Klassifizierung->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Klassenplan	Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen. Mögliche Werte: <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	Nur für Klassenplan = <i>Neu</i> Geben Sie die Bezeichnung des Klassenplans ein.
Filter	Wählen Sie ein IP-Filter aus. Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll.

Feld	Beschreibung
	<p>Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll.</p> <p>Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü Netzwerk->QoS->IPv4/IPv6-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 style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p> Hinweis</p> <p>Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.)</p> </div> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 254.</p>
DSCP/Traffic-Class-Filter setzen (Layer 3)	<p>Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (Klassen-ID) setzen bzw. ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erhalten</i> (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.

Feld	Beschreibung
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>

11.5.3 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.

11.5.3.1 Neu

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

IPv4/IPv6-Filter

QoS-Klassifizierung

QoS-Schnittstellen/Richtlinien

Basisparameter

Schnittstelle

en1-4

Priorisierungsalgorithmus

Priority Queueing

Traffic Shaping

☐ Aktiviert

Queues/Richtlinien

Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag mit der niedrigsten Priorität erstellt.

Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping
<input type="text"/> <input type="button" value="Hinzufügen"/>				

OK

Abbrechen

Abb. 87: **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu**

Das Menü **Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, für die QoS konfiguriert werden soll.
Priorisierungsalgorithmus	<p>Wählen Sie den Algorithmus aus, nach dem die Abarbeitung der Queues erfolgen soll. Sie aktivieren bzw. deaktivieren damit QoS auf der ausgewählten Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Priority Queueing</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird streng gemäß der Priorität der Queues verteilt. • <i>Weighted Round Robin</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird gemäß der Gewichtung (weight) der Queues verteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig behandelt. • <i>Weighted Fair Queueing</i>: QoS wird auf der Schnittstelle aktiviert. Die verfügbare Bandbreite wird möglichst "fair" unter den (automatisch erkannten) Datenverbindungen (Traffic-Flows) innerhalb einer Queue aufgeteilt. Ausnahme: High-Priority-Pakete werden immer vorrangig bedient. • <i>Deaktiviert</i> (Standardwert): QoS wird auf der Schnittstelle deaktiviert. Die ggf. vorhandene Konfiguration wird nicht gelöscht und kann bei Bedarf wieder aktiviert werden.
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> • <i>Ethernet und VLAN</i> • <i>PPP over Ethernet</i> • <i>PPPoE und VLAN</i>

Feld	Beschreibung
	<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 Aktiviert ist und die Größe des Protokoll-Headers unterhalb Layer 3 nicht undefiniert (<i>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>
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.
Queues/Richtlinien	Konfigurieren Sie die gewünschten QoS-Queues.

Feld	Beschreibung
	<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 Standard-eintrag 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-Modus)	<p>Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen.</p> <p>Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere</p>

Feld	Beschreibung
	Priorität als Queues mit inaktivem RTT-Modus haben.
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> <p>Bei deaktiviertem Überbuchen zugelassen kann die Queue niemals Bandbreite über die eingestellte Bandbreitenbegrenzung hinaus belegen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Burst-Größe	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie die maximale Anzahl an Bytes ein, die kurzfristig noch übertragen werden darf, wenn die für diese Queue erlaubte Datenrate bereits erreicht ist.</p> <p>Mögliche Werte sind 0 bis 64000.</p> <p>Der Standardwert ist 0.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Dropping-Algorithmus	<p>Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Tail Drop</i> (Standardwert): Das neu hinzugekommene Paket wird verworfen. • <i>Head Drop</i>: Das älteste Paket in der Queue wird verworfen. • <i>Random Drop</i>: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.

Feld	Beschreibung
Vermeidung von Datenstau (RED)	<p>Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen.</p> <p>Pakete, deren Datengröße zwischen Min. Queue-Größe und Max. Queue-Größe liegt, werden vorbeugend verworfen, um einen Queue-Überlauf zu verhindern (RED=Random Early Detection). Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine insgesamt kleinere Queue, sodass selbst Traffic-Bursts meist ohne größere Paketverluste übertragen werden können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Min. Queue-Größe	<p>Geben Sie den unteren Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 0.</p>
Max. Queue-Größe	<p>Geben Sie den oberen Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 16384.</p>

11.6 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 Zugangsentscheidung 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 eine **Digitalisierungsbox** miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access-Listen ein effektives Mittel.

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

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

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

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

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

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

oder

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

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

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

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

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.



Achtung

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

Greifen Sie zur Filter-Konfiguration möglichst über die serielle Konsolen-Schnittstelle (nicht für alle Geräte verfügbar) oder mit ISDN-Login auf Ihr Gateway zu.

11.6.1 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.

Zugriffsfilter
Regelketten
Schnittstellenzuweisung

Ansicht 20	pro Seite << >>	Filtern in Keiner ▼	gleich ▼		Los
Index	Beschreibung	Quelle	Ziel	TOS-Dezimalwert	
Seite: 1					
Neu					

Abb. 88: **Netzwerk->Zugriffsregeln->Zugriffsfilter**

11.6.1.1 Bearbeiten oder Neu

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

Zugriffsfilter

Regelketten

Schnittstellenzuweisung

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	any ▾
IPv4-Zieladresse/-netzmaske	Beliebig ▾
IPv6-Zieladresse/-länge	Beliebig ▾
IPv4-Quelladresse/-netzmaske	Beliebig ▾
IPv6-Quelladresse/-länge	Beliebig ▾
DSCP / Traffic Class Filter (Layer 3)	Nicht beachten ▾
COS-Filter (802.1p/Layer 2)	Nicht beachten ▾
<div>OKAbbrechen</div>	

Abb. 89: Netzwerk->Zugriffsregeln->Zugriffsfilter->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"><i>activity</i><i>apple-qt</i><i>auth</i><i>chargen</i><i>clients_1</i><i>daytime</i><i>dhcp</i><i>discard</i> <p>Der Standardwert ist <i>any</i>.</p>
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>
Typ	<p>Nur bei Protokoll = <i>ICMP</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><i>Beliebig</i><i>Echo reply</i><i>Destination unreachable</i><i>Source quench</i><i>Redirect</i><i>Echo</i><i>Time exceeded</i><i>Timestamp</i><i>Timestamp reply</i> <p>Der Standardwert ist <i>Beliebig</i>.</p> <p>Siehe RFC 792.</p>

Feld	Beschreibung
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> <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 Quell-IP-Adresse/Länge ist nicht näher spezifiziert. • <i>Host</i>: Geben Sie die Quell-IP-Adresse des Hosts ein.

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

11.6.2 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.

Zugriffsfilter

Regelketten

Schnittstellenzuweisung

Ansicht20

pro Seite<<>>

Filtern inKeiner gleich


Los

Beschreibung	Filter	Aktion		
Seite: 1				

Neu

Abb. 90: Netzwerk->Zugriffsregeln->Regelketten

11.6.2.1 Bearbeiten oder Neu

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

Zugriffsfilter

Regelketten

Schnittstellenzuweisung

Basisparameter

Regelkette

Neu

Beschreibung

Zugriffsfilter

Eines auswählen

Aktion

Zulassen, wenn Filter passt

OK

Abbrechen


Abb. 91: Netzwerk->Zugriffsregeln->Regelketten->Neu

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	<p>ter passt.</p> <ul style="list-style-type: none">• <i>Verweigern, wenn Filter nicht passt</i>: Paket abweisen, wenn das Filter nicht passt.• <i>Nicht beachten</i>: Nächste Regel anwenden.

Um die Regeln einer Regelkette in eine andere Reihenfolge zu bringen, wählen Sie im Listenmenü bei dem Eintrag, der verschoben werden soll, die Schaltfläche . Daraufhin öffnet sich ein Dialog, bei dem Sie unter **Verschieben** entscheiden können, ob der Eintrag *unter* (Standardwert) oder *über* eine andere Regel dieser Regelkette verschoben wird.

11.6.3 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.

ZugriffsfilterRegelkettenSchnittstellenzuweisung


Ansicht20 pro Seite<<>> Filtern inKeiner gleich Los

Schnittstelle	Regelkette	Verwerfen ohne Rückmeldung	Berichtsmethode
Seite: 1			

Neu

Abb. 92: Netzwerk->Zugriffsregeln->Schnittstellenzuweisung

11.6.3.1 Bearbeiten oder Neu

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

ZugriffsfilterRegelkettenSchnittstellenzuweisung

Basisparameter

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

OKAbbrechen

Abb. 93: Netzwerk->Zugriffsregeln->Schnittstellenzuweisung->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, der eine konfigurierte Regelkette zugeordnet werden soll.
Regelkette	Wählen Sie eine Regelkette aus.
Verwerfen ohne Rückmeldung	Legen Sie fest, ob beim Abweisen eines IP-Paketes der Absender informiert werden soll.

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

Kapitel 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 unter-

schiedlichen 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.



Abb. 94: **Multicast->Allgemein->Allgemein**

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

Felder im Menü Grundeinstellungen

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

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.

IGMP

Optionen

IGMP-Einstellungen

Schnittstelle	<div>Keiner</div>
Abfrage Intervall	<div>125</div> Sekunden
Maximale Antwortzeit	<div>10,0</div> Sekunden
Robustheit	<div>2</div>
Antwortintervall (Letztes Mitglied)	<div>1,0</div> Sekunden
Maximale Anzahl der IGMP-Statusmeldungen	<div>0</div> Meldungen pro Sekunde
Modus	<div><input type="radio"/> Host <input checked="" type="radio"/> Routing</div>

Erweiterte Einstellungen

IGMP Proxy

☐ Aktiviert

OK

Abbrechen

Abb. 95: Multicast->IGMP->IGMP->Neu

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

Felder im Menü IGMP-Einstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der IGMP aktiviert werden soll, d.h. Queries werden versendet und Antworten akzeptiert.
Abfrage Intervall	Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen. Möglich Werte sind 0 bis 600. Der Standardwert ist 125.
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 0,0 bis 25,0. Der Standardwert ist 10,0.

Feld	Beschreibung
Robustheit	<p>Wählen Sie den Multiplikator zur Steuerung interner Timer-Werte aus. Mit einem höheren Wert kann z. B. in einem verlustreichen Netzwerk ein Paketverlust kompensiert werden. Durch einen zu hohen Wert kann sich aber auch die Zeit zwischen dem Abmelden und dem Stopp des eingehenden Datenverkehrs erhöhen (Leave Latency).</p> <p>Möglich Werte sind 2 bis 8.</p> <p>Der Standardwert ist 2.</p>
Antwortintervall (Letztes Mitglied)	<p>Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet.</p> <p>Wenn Sie den Wert verkleinern, wird schneller erkannt, ob das letzte Mitglied eine Gruppe verlassen hat und somit keine Pakete mehr für diese Gruppe an diese Schnittstelle weitergeleitet werden müssen.</p> <p>Möglich Werte sind 0,0 bis 25,0.</p> <p>Der Standardwert ist 1,0.</p>
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.

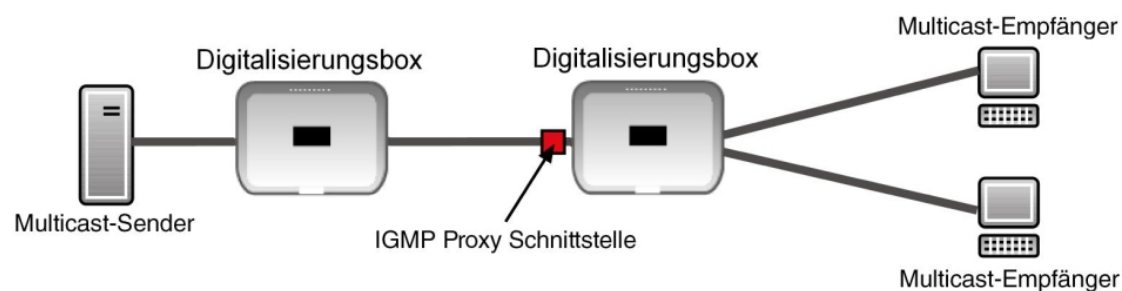


Abb. 96: IGMP Proxy

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>
Proxy-Schnittstelle	<p>Nur für IGMP Proxy = aktiviert</p> <p>Wählen Sie die Schnittstelle Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen.</p>

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.

IGMP

Optionen

Grundeinstellungen

IGMP-Status	<input type="radio"/> Aktiv <input type="radio"/> Inaktiv <input checked="" type="radio"/> Auto	
Modus	<input checked="" type="radio"/> Kompatibilitätsmodus <input type="radio"/> Nur Version 3	
Maximale Gruppen	<input type="text" value="64"/>	
Maximale Quellen	<input type="text" value="64"/>	
Maximale Anzahl der IGMP-Statusmeldungen	<input type="text" value="0"/>	Meldungen pro Sekunde

OK

Abbrechen

Abb. 97: Multicast->IGMP->Optionen

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

Felder im Menü Grundeinstellungen

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

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.

Weiterleiten

Basisparameter

Alle Multicast-Gruppen	<input type="checkbox"/> Aktiviert
Multicast-Gruppen-Adresse	<input type="text"/>
Quellschnittstelle	<div>Keiner</div>
Zielschnittstelle	<div>Keiner</div>

OK

Abbrechen

Abb. 98: Multicast->Weiterleiten->Weiterleiten->Neu

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

Felder im Menü Basisparameter

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

Kapitel 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.

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

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

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



Hinweis





Beachten Sie die Vorgaben Ihres Providers!

Einwahl-Verbindungen über ISDN dienen dazu, zu Netzwerken oder Hosts außerhalb Ihres LANs eine Verbindung herzustellen.

Alle eingetragenen Verbindungen werden in der entsprechenden Liste angezeigt, welche die **Beschreibung**, den **Benutzernamen**, die **Authentifizierung** und den aktuellen **Status** enthält.

Das Feld **Status** kann folgende Werte annehmen:

Mögliche Werte für Status

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

Standard-Route (Default Route)

Bei einer Standard-Route werden automatisch alle Daten auf eine Verbindung geleitet, wenn keine andere passende Route verfügbar ist. Ein Zugang zum Internet sollte immer als Standard-Route zum Internet-Service-Provider (ISP) eingerichtet sein. Weitergehende Informationen zum möglichen Routentyp finden Sie unter **Netzwerk->Routen**.

NAT aktivieren

Mit Network Address Translation (NAT) verbergen Sie Ihr gesamtes Netzwerk nach außen hinter nur einer IP-Adresse. Für die Verbindung zum Internet Service Provider (ISP) sollten Sie dies auf jeden Fall tun.

Bei aktiviertem NAT sind zunächst nur ausgehende Sessions zugelassen. Um bestimmte Verbindungen von außen zu Hosts innerhalb des LANs zu erlauben, müssen diese explizit definiert und zugelassen werden.

Timeout bei Inaktivität festlegen

Der Timeout bei Inaktivität wird festgelegt, um die Verbindung bei Nichtbenutzen, d.h. wenn keine Nutzdaten mehr gesendet werden, automatisch zu trennen und somit ggf. Gebühren zu sparen.

Blockieren nach Verbindungsfehler

Mit dieser Funktion richten Sie eine Wartezeit für ausgehende Verbindungsversuche ein, nachdem ein Verbindungsversuch durch Ihr Gerät fehlgeschlagen ist.

Authentifizierung

Wenn bei ISDN-Verbindungen ein Ruf eingeht, wird über den ISDN-D-Kanal die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann Ihr Gerät den Anrufer identifizieren (CLID), wenn dieser auf Ihrem Gerät eingetragen ist. Nach der Identifizierung mit CLID kann Ihr Gerät zusätzlich eine PPP-Authentisierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird.

Für alle PPP-Verbindungen benötigt Ihr Gerät Vergleichsdaten, die Sie eintragen müssen. Legen Sie fest, welche Authentisierungsverhandlung ausgeführt werden soll und tragen Sie ein gemeinsames Passwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf Ihrem Gerät eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Callback

Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann der Callback-Mechanismus für jede Verbindung über eine ISDN- oder über eine AUX-Schnittstelle verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf zustande, nachdem der Anrufer eindeutig identifiziert wurde. Ihr Gerät kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch von einem Verbindungspartner einen Rückruf anfordern. Die Identifizierung kann aufgrund der Calling Party Number oder aufgrund der PAP/CHAP/MS-CHAP-Authentifizierung erfolgen. Im ersten Fall erfolgt die Identifikation ohne Rufannahme, da die Calling Party Number über den ISDN-D- Kanal übermittelt wird, im zweiten Fall mit Rufannahme.

Kanalbündelung

Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Kanalbündelung kann nur bei ISDN-Verbindungen für Bandbreitenerhöhung bzw. als Backup angewendet werden. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch

Dynamische Kanalbündelung bedeutet, dass Ihr Gerät bei Bedarf, also bei großen Datenraten, weitere ISDN-B-Kanäle für Verbindungen zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen B-Kanäle wieder geschlossen.

Falls auf der Gegenstelle Geräte anderer Fabrikate verwendet werden, stellen Sie sicher, dass diese dynamische Kanalbündelung für Bandbreitenerhöhung bzw. als Backup unterstützen.

Statisch

Bei statischer Kanalbündelung legen Sie im Voraus fest, wie viele B-Kanäle Ihr Gerät für Verbindungen nutzen soll, unabhängig von der übertragenen Datenrate.

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.

PPPoE
PPTP
PPPoA
IP Pools

Basisparameter	
Beschreibung	<input style="width: 90%;" type="text"/>
PPPoE-Modus	<input checked="" type="radio"/> Standard <input type="radio"/> Mehrfachverbindung
PPPoE-Ethernet-Schnittstelle	Eine auswählen ▼
Benutzername	<input style="width: 90%;" type="text"/>
Passwort	<input style="width: 90%;" type="password"/>
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	<input style="width: 50px;" type="text" value="300"/> Sekunden
IPv4-Einstellungen	
Sicherheitsrichtlinie	<input checked="" type="radio"/> Nicht Vertrauenswürdig <input type="radio"/> Vertrauenswürdig
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
IPv6-Einstellungen	
IPv6	<input type="checkbox"/> Aktiviert

Erweiterte Einstellungen	
Blockieren nach Verbindungsfehler für	<input style="width: 50px;" type="text" value="60"/> Sekunden
Maximale Anzahl der erneuten Einwählversuche	<input style="width: 50px;" type="text" value="5"/>
Authentifizierung	PAP/CHAP ▼
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
Erweiterte IPv4-Einstellungen	
MTU	<input checked="" type="checkbox"/> Automatisch

OK
Abbrechen

Abb. 99: **WAN->Internet + Einwählen->PPPoE->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE (<i>Standard</i>) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll (<i>Mehrfachverbindung</i>). Wählen Sie <i>Mehr-</i>

Feld	Beschreibung
	<p><i>fachverbindung</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 benutzen wollen, müssen Sie den Ethernet-Switch Ihres Geräts im Split-Port-Modus betreiben.</p>
PPPoE-Ethernet-Schnittstelle	<p>Nur für PPPoE-Modus = <i>Standard</i></p> <p>Wählen Sie die Ethernet-Schnittstelle aus, die für eine Standard-PPPoE-Verbindung vorgegeben wird.</p> <p>Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist.</p> <p>Bei Verwendung des internen DSL-Modems, wählen Sie hier die in WAN->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle aus.</p> <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> <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</p>

Feld	Beschreibung
	<p>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 <i>Firewall</i> auf Seite 227 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. • <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.

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

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob die gewählte PPPoE- Schnittstelle das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 227 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 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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind <i>0</i> bis <i>100</i>.</p> <p>Der Standardwert ist <i>5</i>.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Erweiterte IPv4-Einstellungen

Feld	Beschreibung
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die Verbindung verwendet werden darf.</p> <p>Mit dem Standardwert <i>Automatisch</i> wird der Wert beim Verbindungsaufbau durch das Link Control Protocol vorgegeben.</p>

Feld	Beschreibung
	Wenn Sie <i>Automatisch</i> deaktivieren, können Sie einen Wert eingeben. Mögliche Werte sind 1 bis 8192. Der Standardwert ist 0.

13.1.2 PPTP

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

In diesem Menü konfigurieren Sie eine Internet-Verbindung, die zum Verbindungsaufbau das Point-to-Point Tunneling Protocol (PPTP) verwendet. Dies ist z. B. in Österreich notwendig.

13.1.2.1 Neu

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

PPPoE

PPTP

PPPoA

IP Pools

Basisparameter

Beschreibung

PPTP-Ethernet-Schnittstelle

Eine auswählen ▾

Benutzername

Passwort

Immer aktiv

☐ Aktiviert

Timeout bei Inaktivität

300

Sekunden

IPv4-Einstellungen

Sicherheitsrichtlinie

☒ Nicht Vertrauenswürdig ☐ Vertrauenswürdig

IP-Adressmodus

☐ Statisch ☒ IP-Adresse abrufen

Standardroute

☒ Aktiviert

NAT-Eintrag erstellen

☒ Aktiviert

Erweiterte Einstellungen

Blockieren nach Verbindungsfehler für

60

Sekunden

Maximale Anzahl der erneuten Einwählversuche

5

Authentifizierung

PAP ▾

DNS-Aushandlung

☒ Aktiviert

TCP-ACK-Pakete priorisieren

☐ Aktiviert

PPTP-Adressmodus

Statisch

Lokale PPTP-IP-Adresse

10.0.0.140

Entfernte PPTP-IP-Adresse

10.0.0.138

LCP-Erreichbarkeitsprüfung

☒ Aktiviert

OK

Abbrechen

Abb. 100: **WAN->Internet + Einwählen->PPTP->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um die Internetverbindung eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen

Feld	Beschreibung
	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 Physisikalische Schnittstellen->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle z. B. <i>ethoa50-0</i>, aus.</p>
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte sind 0 bis 3600 (Sekunden). 0 deaktiviert den Timeout.</p> <p>Der Standardwert ist 300.</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>

Felder im Menü 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 227 konfigurieren.</p>
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine temporär gültige IP-Adresse vom Provider. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.

Feld	Beschreibung
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Weisen Sie der PPTP-Schnittstelle eine IP-Adresse aus Ihrem LAN zu, die als interne Quelladresse Ihres Geräts verwendet werden soll.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen PPTP-Partner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<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. • <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.

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

13.1.3 PPPoA

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

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

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

13.1.3.1 Neu

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

PPPoE

PPTP

PPPoA

IP Pools

Basisparameter	
Beschreibung	<input type="text"/>
ATM PVC	Eine auswählen ▾
Benutzername	<input type="text"/>
Passwort	<input type="password"/>
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	<input type="text" value="300"/> Sekunden
IPv4-Einstellungen	
Sicherheitsrichtlinie	<input checked="" type="radio"/> Nicht Vertrauenswürdig <input type="radio"/> Vertrauenswürdig
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
IPv6-Einstellungen	
IPv6	<input type="checkbox"/> Aktiviert

Erweiterte Einstellungen

Blockieren nach Verbindungsfehler für	<input type="text" value="60"/> Sekunden
Maximale Anzahl der erneuten Einwählversuche	<input type="text" value="5"/>
Authentifizierung	PAP ▾
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert

OK

Abbrechen

Abb. 101: WAN->Internet + Einwählen->PPPoA->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
ATM PVC	Wählen Sie ein im Menü ATM->Profile angelegtes ATM-Profil, dargestellt durch die vom Provider vorgegebenen globalen ID VPI und VCI.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort für die PPPoA-Verbindung ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.

Feld	Beschreibung
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen soll.</p> <p>Mögliche Werte sind <i>0</i> bis <i>3600</i> (Sekunden). <i>0</i> deaktiviert den Shorthold.</p> <p>Der Standardwert ist <i>300</i>.</p> <p>Bsp. <i>10</i> für FTP-Übertragungen, <i>20</i> für LAN-zu-LAN-Übertragungen, <i>90</i> für Internetverbindungen.</p>

Felder im Menü IPv4-Einstellungen

Feld	Beschreibung
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 227 konfigurieren.</p>
IP-Adressmodus	<p>Wählen Sie aus, ob Ihr Gerät eine statische IP-Adresse hat oder diese dynamisch erhält.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IP-Adresse abrufen</i> (Standardwert): Ihr Gerät erhält dynamisch eine IP-Adresse. • <i>Statisch</i>: Sie geben eine statische IP-Adresse ein.
Standardroute	<p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p>

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

Felder im Menü IPv6-Einstellungen

Feld	Beschreibung
IPv6	<p>Wählen Sie aus, ob das gewählte ATM-Profil das Internet Protocol Version 6 (IPv6) für die Datenübertragung verwenden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung das gewählte ATM-Profil betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i> (Standardwert): Es werden nur diejenigen IP-Pakete durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 außerhalb Ihres LAN verwenden wollen.</p> <ul style="list-style-type: none"> • <i>Vertrauenswürdig</i>: Es werden alle IP-Pakete durchgelassen, außer denen, die explizit verboten sind. <p>Wir empfehlen Ihnen, diese Einstellung zu verwenden, wenn Sie IPv6 in Ihrem LAN verwenden wollen.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 227 konfigurieren.</p>
IPv6-Modus	<p>Nur für IPv6 = <i>Aktiviert</i></p> <p>Das gewählte ATM-Profil 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 das ATM-Profil empfangen werden sollen. Mithilfe der Router Advertisements wird die Default Router List sowie 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.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Der Standardwert ist <i>60</i> .
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte sind <i>0</i> bis <i>100</i> . Der Standardwert ist <i>5</i> .
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist. Mögliche Werte: <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Diese ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.


13.1.4 IP Pools

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

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

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

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.

PPPoE

PPTP

PPPoA

IP Pools

Basisparameter

IP-Poolname

IP-Adressbereich

DNS-Server

Primär

Sekundär

OK

Abbrechen

Abb. 102: WAN->Internet + Einwählen->IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll. Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

13.2 ATM

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

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

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

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

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

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

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

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

13.2.1 Profile

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

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

Standardmäßig ist ein ATM-Profil mit der Beschreibung *AUTO-CREATED* vorkonfiguriert, dessen Werte (VPI 1 und VCI 32) z. B. für eine ATM-Verbindung der Telekom geeignet sind.



Hinweis

Die ATM-Encapsulierungen sind in den RFCs 1483 und 2684 beschrieben. Sie finden die RFCs auf den entsprechenden Seiten der IETF (www.ietf.org/rfc.html).

13.2.1.1 Neu

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

Profile

Dienstkategorien

OAM-Regelung

ATM-Profilparameter

Provider

-- Benutzerdefiniert --

Beschreibung

Typ

Ethernet über ATM

Virtual Path Identifier (VPI)

8

Virtual Channel Identifier (VCI)

32

Encapsulierung

LLC Bridged no FCS

Einstellungen für Ethernet über ATM

Standard-Ethernet für PPPoE-Schnittstellen

☐ Aktiviert

Adressmodus

☒ Statisch ☐ DHCP

IP-Adresse/Netzmaske

IP-Adresse

Netzmaske

Hinzufügen

MAC-Adresse

☒ Voreingestellte verwenden

OK

Abbrechen

Abb. 103: WAN->ATM->Profile->Neu

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

Felder im Menü ATM-Profilparameter

Feld	Beschreibung
Provider	Wählen Sie eines der vorkonfigurierten ATM-Profile für Ihren Provider aus der Liste aus oder definieren Sie mit -- Benutzerdefiniert -- ein Profil.
Beschreibung	Nur für Provider = -- Benutzerdefiniert -- Geben Sie eine beliebige Beschreibung für die Verbindung ein.
ATM-Schnittstelle	Nur, wenn mehrere ATM-Schnittstellen verfügbar sind, z. B. wenn bei Geräten mit SHDSL mehrere Schnittstellen separat konfiguriert sind. Wählen Sie die ATM-Schnittstelle, die Sie für die Verbindung verwenden wollen.
Typ	Nur für Provider = -- Benutzerdefiniert -- Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte: <ul style="list-style-type: none">Ethernet über ATM (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet.Geroutete Protokolle über ATM: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) werden geroutete Protokolle über ATM (RPoA) verwendet.PPP über ATM: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.
Virtual Path Identifier (VPI)	Nur für Provider = -- Benutzerdefiniert -- Geben Sie den VPI-Wert der ATM-Verbindung ein. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades. Verwenden Sie die Vorgaben Ihres Providers.

Feld	Beschreibung
	<p>Mögliche Werte sind <i>0</i> bis <i>255</i>.</p> <p>Der Standardwert ist <i>8</i>.</p>
Virtual Channel Identifier (VCI)	<p>Nur für Provider = <i>-- Benutzerdefiniert --</i></p> <p>Geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten. Verwenden Sie die Vorgaben Ihres Providers.</p> <p>Mögliche Werte sind <i>32</i> bis <i>65535</i>.</p> <p>Der Standardwert ist <i>32</i>.</p>
Enkapsulierung	<p>Nur für Provider = <i>-- Benutzerdefiniert --</i></p> <p>Wählen Sie die zu verwendende Enkapsulierung aus. Verwenden Sie die Vorgaben Ihres Providers.</p> <p>Mögliche Werte (nach RFC 2684):</p> <ul style="list-style-type: none"> • <i>LLC Bridged no FCS</i> (Standardwert für Ethernet über ATM): Wird nur für Typ = <i>Ethernet über ATM</i> angezeigt. <p>Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> • <i>LLC Bridged FCS</i>: Wird nur für Typ = <i>Ethernet über ATM</i> angezeigt. <p>Bridged Ethernet mit LLC/SNAP-Enkapsulierung mit Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> • <i>Nicht ISO</i> (Standardwert für Geroutete Protokolle über ATM): Wird nur für Typ = <i>Geroutete Protokolle über ATM</i> angezeigt. <p>Enkapsulierung mit LLC/SNAP-Header, geeignet für IP-Routing.</p> <ul style="list-style-type: none"> • <i>LLC</i>: Wird nur für Typ = <i>PPP über ATM</i> angezeigt. <p>Enkapsulierung mit LLC-Header.</p> <ul style="list-style-type: none"> • <i>VC-Multiplexing</i> (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Enkapsulierung (Null Einkapselung) mit Frame Check Sequence (Prüfsummen).

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

Feld	Beschreibung
Standard-Ethernet für PP-PoE-Schnittstellen	<p>Nur für Typ = <i>Ethernet über ATM</i></p> <p>Wählen Sie aus, ob diese Ethernet-over-ATM-Schnittstelle für alle PP-PoE-Verbindungen verwendet werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Adressmodus	<p>Nur für Typ = <i>Ethernet über ATM</i></p> <p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse / Netzmaske zugewiesen. • <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse/Netzmaske	<p>Nur für Adressmodus = <i>Statisch</i></p> <p>Geben Sie die IP-Adressen (IP-Adresse) und die entsprechenden Netzmasken (Netzmaske) der ATM-Schnittstellen ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.</p>
MAC-Adresse	<p>Geben Sie der routerinternen Schnittstelle der ATM-Verbindung eine MAC-Adresse, z. B. <i>00:a0:f9:06:bf:03</i>. Ein Eintrag wird nur in speziellen Fällen benötigt.</p> <p>Für Internetverbindungen ist es ausreichend, die Option Voreingestellte verwenden (Standardeinstellung) auszuwählen. Es wird eine Adresse verwendet, die von der MAC-Adresse des <i>en1-0</i> abgeleitet ist.</p>
DHCP-MAC-Adresse	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Geben Sie die MAC-Adresse der routerinternen Schnittstelle der ATM-Verbindung ein, z. B. <i>00:e1:f9:06:bf:03</i>.</p> <p>Sollte Ihnen Ihr Provider eine MAC-Adresse für DHCP zugewiesen haben, so tragen Sie diese hier ein.</p> <p>Sie haben auch die Möglichkeit, die Option Voreingestellte verwenden (Standardeinstellung) auszuwählen. Es wird eine Adresse verwendet, die von der MAC-Adresse des <i>en1-0</i> abgeleitet ist.</p>
DHCP-Hostname	<p>Nur für Adressmodus = <i>DHCP</i></p> <p>Geben Sie ggf. den beim Provider registrierten Host-Namen an, der von Ihrem Gerät für DHCP-Anfragen verwendet werden soll.</p> <p>Die maximale Länge des Eintrags beträgt 45 Zeichen.</p>

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

Feld	Beschreibung
IP-Adresse/Netzmaske	Geben Sie die IP-Adressen (IP-Adresse) und die entsprechenden Netzmasken (Netzmaske) der ATM-Schnittstelle ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

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

Feld	Beschreibung
Client-Typ	<p>Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auf Anforderung</i> (Standardwert): Die PPPoA wird nur bei Bedarf

Feld	Beschreibung
	aufgebaut, z. B. für den Internetzugang. Zusätzliche Informationen zu PPP über ATM finden Sie unter PPPoA auf Seite 182.

13.2.2 Dienstkategorien

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

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

Achtung

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

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

13.2.2.1 Neu

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

Profile
Dienstkategorien
QAM-Regelung

Basisparameter	
Virtual Channel Connection (VCC)	VPI8, VCI32 ▼
ATM-Dienstkategorie	Eine auswählen ▼
Peak Cell Rate (PCR)	0 Bit/s
Sustained Cell Rate (SCR)	0 Bit/s
Maximale Burst-Größe (MBS)	0 Bit/s

OK
Abbrechen

Abb. 104: **WAN->ATM->Dienstkategorien->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Virtual Channel Connection (VCC)	Wählen Sie die bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus, für welche die Dienstkategorie festgelegt werden soll.
ATM-Dienstkategorie	<p>Wählen Sie aus, auf welche Art der Datenverkehr der ATM-Verbindung geregelt werden soll.</p> <p>Durch die Auswahl der ATM-Dienstkategorie wird implizit eine Priorität zugeordnet: von CBR (höchste Priorität) über VBR.1 / VBR.3 bis VBR (niedrigste Priorität).</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> <i>Unspecified Bit Rate (UBR)</i> (Standardwert): Der Verbindung

Feld	Beschreibung
	<p>wird keine bestimmte Datenrate garantiert. Die Peak Cell Rate (PCR) legt die Grenze fest, bei deren Überschreiten Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen.</p> <ul style="list-style-type: none"> • <i>Constant Bit Rate (CBR)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen, die von der Peak Cell Rate (PCR) bestimmt wird. Diese Kategorie eignet sich für kritische Anwendungen (Real-Time), die eine garantierte Datenrate voraussetzen. • <i>Variable Bit Rate V.1 (VBR.1)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen - Sustained Cell Rate (SCR). Diese darf insgesamt um das in Maximale Burst-Größe (MBS) konfigurierte Volumen überschritten werden. Jeglicher weiterer ATM-Traffic wird verworfen. Die Peak Cell Rate (PCR) bildet dabei die maximal mögliche Datenrate. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen. • <i>Variable Bit Rate V.3 (VBR.3)</i>: Der Verbindung wird eine garantierte Datenrate zugewiesen - Sustained Cell Rate (SCR). Diese darf insgesamt um das in Maximale Burst-Größe (MBS) konfigurierte Volumen überschritten werden. Weiterer ATM-Traffic wird markiert und je nach Auslastung des Zielnetzes mit niedriger Priorität behandelt, d. h. wird bei Bedarf verworfen. Die Peak Cell Rate (PCR) bildet dabei die maximal mögliche Datenrate. Diese Kategorie eignet sich für kritische Anwendungen mit stoßweisem Datenaufkommen.
Peak Cell Rate (PCR)	<p>Geben Sie einen Wert für die maximale Datenrate in Bits pro Sekunde ein.</p> <p>Mögliche Werte: 0 bis 10000000.</p> <p>Der Standardwert ist 0.</p>
Sustained Cell Rate (SCR)	<p>Nur für ATM-Dienstkategorie = <i>Variable Bit Rate V.1 (VBR.1)</i> oder <i>Variable Bit Rate V.3 (VBR.3)</i></p> <p>Geben Sie einen Wert für die mindestens zur Verfügung stehende, garantierte Datenrate in Bits pro Sekunde ein.</p> <p>Mögliche Werte: 0 bis 10000000.</p> <p>Der Standardwert ist 0.</p>
Maximale Burst-Größe (MBS)	<p>Nur für ATM-Dienstkategorie = <i>Variable Bit Rate V.1 (VBR.1)</i> oder <i>Variable Bit Rate V.3 (VBR.3)</i></p> <p>Geben Sie hier einen Wert für die maximale Anzahl in Bits pro Sekunde ein, um welche die PCR kurzzeitig überschritten werden darf.</p> <p>Mögliche Werte: 0 bis 100000.</p> <p>Der Standardwert ist 0.</p>

13.2.3 OAM-Regelung

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



Hinweis

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

Zur Überwachung der ATM-Verbindung stehen zwei Mechanismen zur Verfügung: Loopback-Tests und OAM Continuity Check (OAM CC). Sie können unabhängig voneinander konfiguriert werden.



Achtung

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

Im Menü **WAN->ATM->OAM-Regelung** wird eine Liste aller überwachten OAM-Fluss-Levels angezeigt.

13.2.3.1 Neu

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

Profile

Dienstkategorien

OAM-Regelung

OAM-Flusskonfiguration

OAM-Fluss-Level

F5

Virtual Channel Connection (VCC)

VPI8, VCI32

Loopback

Loopback Ende-zu-Ende

☐ Aktiviert

Loopback-Segment

☐ Aktiviert

CC-Aktivierung

Continuity Check (CC) Ende-zu-Ende

Passiv

Richtung

Beide

Continuity Check (CC) Segment

Passiv

Richtung

Beide

OK

Abbrechen

Abb. 105: **WAN->ATM->OAM-Regelung->Neu**

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

Felder im Menü OAM-Flusskonfiguration

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

Feld	Beschreibung
(VPC)	Wählen Sie die zu überwachende bereits konfigurierte Virtual Path Connection (angezeigt durch den VPI) aus.

Felder im Menü Loopback

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

Felder im Menü CC-Aktivierung

Feld	Beschreibung
Continuity Check (CC) Ende-zu-Ende	<p>Wählen Sie aus, ob Sie den OAM-CC-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • <i>Keine Aushandlung</i>: Je nach Einstellung im Feld Richtung werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine CC-Aushandlung statt. • <i>Passiv</i>: Die Funktion ist nicht aktiv. <p>Wählen Sie außerdem aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • <i>Senke</i>: CC-Daten werden empfangen. • <i>Quelle</i>: CC-Daten werden generiert.
Continuity Check (CC) Segment	<p>Wählen Sie aus, ob Sie den OAM-CC-Test für die Segment-Verbindung (Segment=Verbindung des lokalen Endpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • <i>Keine Aushandlung</i>: Je nach Einstellung im Feld Richtung werden OAM CC Requests entweder gesendet und/oder beantwortet, es findet keine CC-Aushandlung statt. • <i>Keiner</i>: Die Funktion ist nicht aktiv. <p>Wählen Sie weiterhin aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • <i>Senke</i>: CC-Daten werden empfangen. • <i>Quelle</i>: CC-Daten werden generiert.

13.3 Real Time Jitter Control

Bei Telefongesprächen über das Internet haben Sprachdaten-Pakete normalerweise höchste Priorität. Trotzdem können bei geringer Bandbreite der Upload Verbindung während eines Telefongesprächs merkbare Verzögerungen bei der Sprachübertragung auftreten, wenn gleichzeitig andere Datenpakete geroutet werden.

Die Funktion Real Time Jitter Control löst dieses Problem. Um die "Leitung" für die Sprachdaten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

13.3.1 Regulierte Schnittstellen

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

13.3.1.1 Neu

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

Regulierte Schnittstellen

Grundeinstellungen

Schnittstelle

Keine ▾

Kontrollmodus

Nur kontrollierte RTP-Streams ▾

Maximale Upload-Geschwindigkeit

0

kbit/s

OK

Abbrechen

Abb. 106: **WAN->Real Time Jitter Control->Regulierte Schnittstellen->Neu**

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Schnittstelle	Legen Sie fest, für welche Schnittstellen die Sprachübertragung optimiert werden soll.
Kontrollmodus	Wählen Sie den Modus für die Optimierung aus. Mögliche Werte: <ul style="list-style-type: none">Nur kontrollierte RTP-Streams (Standardwert): Anhand der Daten, die über das Media Gateway geroutet werden, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung.Alle RTP-Streams: Alle RTP-Streams werden optimiert.Inaktiv: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt.Immer: 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 Preshared 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 48) 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

Digitalisierungsbox unterstützt 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 konfigurierter IPSec-Peers nach Priorität sortiert angezeigt.

Abb. 107: VPN->IPSec->IPSec-Peers

Peer Überwachung

Das Überwachungsmenü eines Peers wird durch Auswahl der -Schaltfläche beim entsprechenden Peer in der Peerliste aufgerufen. Siehe [Werte in der Liste IPSec-Tunnel](#) auf Seite 329.

14.1.1.1 Neu

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


IPSec-Peers		Phase-1-Profil	Phase-2-Profil	XAUTH-Profil	IP Pools	Optionen										
Peer-Parameter																
Administrativer Status	<input checked="" type="radio"/> Aktiv <input type="radio"/> Inaktiv															
Beschreibung	Peer-1															
Peer-Adresse	IP-Version IPv4 bevorzugt ▼ <input type="text"/>															
Peer-ID	Fully Qualified Domain Name (FQDN) ▼ <input type="text"/> Peer-1.															
IKE (Internet Key Exchange)	IKEv1 ▼															
Preshared Key	<input type="text"/>															
IP-Version des Tunnelnetzwerks	IPv4 ▼															
IPv4-Schnittstellenrouten																
Sicherheitsrichtlinie	<input type="radio"/> Nicht Vertrauenswürdig <input checked="" type="radio"/> Vertrauenswürdig															
IPv4-Adressvergabe	Statisch ▼															
Standardroute	<input type="checkbox"/> Aktiviert															
Lokale IP-Adresse	<input type="text"/>															
Routeneinträge	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td>1 ▼</td> <td></td> </tr> </tbody> </table> <div>Hinzufügen</div>						Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	1 ▼			
Entfernte IP-Adresse	Netzmaske	Metrik														
<input type="text"/>	<input type="text"/>	1 ▼														
Zusätzlicher Filter des IPv4-Datenverkehrs																
Zusätzlicher Filter des IPv4-Datenverkehrs	<table border="1"> <thead> <tr> <th>Beschreibung</th> <th>Protokoll</th> <th>Quell-IP/Maske:Port</th> <th>Ziel-IP/Maske:Port</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <div>Hinzufügen</div>						Beschreibung	Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port		<input type="text"/>				
Beschreibung	Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port													
<input type="text"/>																
Erweiterte Einstellungen																
Erweiterte IPSec-Optionen																
Phase-1-Profil	Keines (Standardprofil verwenden) ▼															
Phase-2-Profil	Keines (Standardprofil verwenden) ▼															
XAUTH-Profil	Eines auswählen ▼															
Anzahl erlaubter Verbindungen	<input checked="" type="radio"/> Ein Benutzer <input type="radio"/> Mehrere Benutzer															
Startmodus	<input checked="" type="radio"/> Auf Anforderung <input type="radio"/> Immer aktiv															
Erweiterte IP-Optionen																
Öffentliche Schnittstelle	Vom Routing ausgewählt ▼															
Öffentliche IPv4-Quelladresse	<input type="checkbox"/> Aktiviert															
Überprüfung der IPv4-Rückroute	<input type="checkbox"/> Aktiviert															
IPv4 Proxy ARP	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv															
IPv4 IPSec Callback																
Modus	Inaktiv ▼															
<div>OK</div> <div>Abbrechen</div>																

Abb. 108: VPN->IPSec->IPSec-Peers->Neu

Das Menü VPN->IPSec->IPSec-Peers->Neu besteht aus folgenden Feldern:

Felder im Menü Peer-Parameter

Feld	Beschreibung
Administrativer Status	<p>Wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Peer-Konfiguration versetzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Aktiv</i> (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. <i>Inaktiv</i>: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.

Feld	Beschreibung
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> <div>  Hinweis <p>Diese Auswahl ist nur relevant, wenn ein Host-Name als Peer-Adresse eingegeben wird.</p> </div> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <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> <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 konfigu-

Feld	Beschreibung
	<p>riert. Der Preshared Key ist das gemeinsame Passwort.</p> <ul style="list-style-type: none"> • <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 erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektnamen des Zertifikats verwendet.</p> <p>Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe Zertifikate auf Seite 48), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.</p>
Preshared Key	<p>Geben Sie das mit dem Peer vereinbarte Passwort ein.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer <i>0x</i> am Anfang des Eintrags.</p>
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> <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

Feld	Beschreibung
	<p>durchgelassen, die einer Verbindung zugeordnet werden können, die aus einer vertrauenswürdigen Zone aufgebaut wurde.</p> <p>Ausnahmen für die gewählte Einstellung können Sie im Menü <i>Firewall</i> auf Seite 227 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>: Nur für IKEv1 auswählbar. Wählen Sie diese Option, wenn Ihr Gateway als IPSec-Client vom Server eine IP-Adresse erhalten soll. • <i>Server im IKE-Konfigurationsmodus</i>: Wählen Sie diese Option, wenn Ihr Gateway als Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten IP-Zuordnungspool entnommen.
Konfigurationsmodus	<p>Nur bei IPv4-Adressvergabe = <i>Server im IKE-Konfigurationsmodus</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Pull</i> (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage. • <i>Push</i>: Das Gateway schlägt dem Client eine IP-Adresse vor und der Client muss diese akzeptieren oder zurückweisen. <p>Dieser Wert muss für beide Seiten des Tunnels identisch sein.</p>
IP-Zuordnungspool	<p>Nur bei IPv4-Adressvergabe = <i>Server im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie einen im Menü VPN->IPSec->IP Pools konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool konfiguriert wurde, erscheint in diesem Feld die Meldung <i>Noch nicht definiert</i>.</p>
Standardroute	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Wählen Sie aus, ob die Route zu diesem IPSec-Peer als Standardroute festgelegt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Server im IKE-Konfigurationsmodus</i></p> <p>Geben Sie die WAN IP-Adresse Ihrer IPSec-Verbindung an. Es kann die gleiche IP-Adresse sein, die als LAN IP-Adresse an Ihrem Router konfiguriert ist.</p>
Metrik	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Client im IKE-Konfigurationsmodus</i> und Standardroute = <i>Aktiviert</i></p> <p>Wählen Sie die Priorität der Route aus.</p> <p>Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.</p>

Feld	Beschreibung
	Wertebereich von 0 bis 15. der Standardwert ist 1.
Routeneinträge	<p>Nur für IPv4-Adressvergabe = <i>Statisch</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <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) = <i>IKEv1</i></p> <p>Legen Sie mithilfe von Hinzufügen einen neuen Filter an.</p>

Felder im Menü IPv6-Schnittstellenrouten

Feld	Beschreibung
Sicherheitsrichtlinie	<p>Wählen Sie, mit welcher Sicherheitseinstellung die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht Vertrauenswürdig</i>: Es werden nur 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> (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 227 konfigurieren.</p>
Lokales IPv6-Netzwerk	<p>Wählen Sie ein Netzwerk aus. Sie können unter den Link-Präfixen wählen, die unter LAN->IP-Konfiguration->Schnittstellen->Neu angelegt sind.</p> <p>Geben Sie die Lokale IPv6-Adresse mit der entsprechenden Präfixlänge ein. Dieser Präfix muss mit :: enden. Standardmäßig ist eine Präfixlänge von /64 vorgegeben.</p>
Entferntes IPv6-Netzwerk	<p>Fügen Sie mit Hinzufügen einen neuen Präfix hinzu. Geben Sie die Adresse der Tunnelgegenstelle ein. Standardmäßig ist eine Länge von 64 und eine Priorität von 1 vorgegeben. Je niedriger der Wert der Priorität ist, desto höhere Priorität besitzt die Route.</p>

Zusätzlicher Filter des Datenverkehrs

Digitalisierungsbox unterstützt 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.

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

IPSec-Peers

Phase-1-Profile

Phase-2-Profile

XAUTH-Profile

IP Pools

Optionen

Peer-Parameter

Administrativer Status

☒ Aktiv
☐ Inaktiv

Beschreibung

Peer-1

Peer-Adresse

Basisparameter

Beschreibung

Protokoll

Beliebig

Quell-IP-Adresse/Netzmaske

Netzwerk

Ziel-IP-Adresse/Netzmaske

Netzwerk

Übernehmen

Abbrechen

Peer-ID

IKE (Internet Key Exchange)

Preshared Key

IP-Version des Peers

IPv4-Schnittstellenmodus

IPv4-Adressvergabe

Statisch

Standardroute

☐ Aktiviert

Lokale IP-Adresse

0.0.0.0

Routeneinträge

Entfernte IP-Adresse

0.0.0.0

Netzmaske

0.0.0.0

Metrik

1

Hinzufügen

Zusätzlicher Filter des IPv4-Datenverkehrs

Beschreibung

Protokoll

Quell-IP/Maske:Port

Ziel-IP/Maske:Port

Hinzufügen

Erweiterte Einstellungen

OK

Abbrechen

Abb. 109: VPN->IPSec->IPSec-Peers->Neu->Hinzufügen

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Protokoll	Wählen Sie ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
Quell-IP-Adresse/Netzmaske	<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> <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	<p>Nur für Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie den Quell-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.</p>
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und die zugehörige Netzmaske der Datenpakete ein.
Ziel-Port	<p>Nur für Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie den Ziel-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.</p>

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

Felder im Menü Erweiterte IPSec-Optionen

Feld	Beschreibung
Phase-1-Profile	<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 verwendet wird, werden zuerst die Transaktionen für XAuth und dann diejenigen für den IKE-Konfigurationsmodus durchgeführt.</p>
Anzahl erlaubter Verbindungen	<p>Wählen Sie aus, wieviele Benutzer sich mit diesem Peer-Profil verbinden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Ein Benutzer</i> (Standardwert): Es kann sich nur ein Peer mit den in diesem Profil definierten Daten verbinden. • <i>Mehrere Benutzer</i>: Es können sich mehrere Peers mit den in diesem Profil definierten Daten verbinden. Bei jeder Verbindungsanfrage mit den in diesem Profil definierten Daten, wird der Peer-Eintrag dupliziert. <p>Die Konfiguration des dynamischen Peers darf keine Peer ID und keine Peer-IP-Adresse enthalten. Die Clients, die sich mit dem Gateway verbinden, müssen jedoch über eine Peer ID verfügen, da diese verwendet wird, um die durch dynamische Peers erstellten IPSec-Tunnel voneinander zu trennen.</p> <p>Der resultierende Peer auf dem Gateway würde nun auf alle eingehenden Tunnel-Requests zutreffen. Daher ist es notwendig, ihn an das Ende der IPSec-Peer-Liste zu stellen. Andernfalls wären alle in der Liste folgenden Peers inaktiv.</p>

Feld	Beschreibung
Startmodus	<p>Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auf Anforderung</i> (Standardwert): Der Peer wird durch einen Trigger in den aktiven Zustand versetzt. • <i>Immer aktiv</i>: Der Peer ist immer aktiv.

Felder im Menü Erweiterte IP-Optionen

Feld	Beschreibung
Öffentliche Schnittstelle	<p>Legen Sie diejenige öffentliche (oder WAN-) Schnittstelle fest, über die dieser Peer sich mit seinem VPN-Partner verbinden soll. Wenn Sie <i>Vom Routing ausgewählt</i> auswählen, wird die Entscheidung, über welche Schnittstelle der Datenverkehr geleitet wird, gemäß der aktuellen Routingtabelle getroffen. Wenn Sie eine Schnittstelle auswählen, wird unter Beachtung der Einstellung unter Öffentlicher Schnittstellenmodus diese Schnittstelle verwendet.</p>
Öffentlicher Schnittstellenmodus	<p>Legen Sie fest, wie strikt die Einstellung unter Öffentliche Schnittstelle gehandhabt wird. Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erzwingen</i>: Unabhängig von den Prioritäten der aktuellen Routingtabelle wird nur die ausgewählte Schnittstelle verwendet. • <i>Bevorzugt</i>: Die Prioritäten der aktuellen Routingtabelle werden verwendet. Nur wenn mehrere gleichwertige Routen zur Verfügung stehen, wird die Route über die gewählte Schnittstelle verwendet.
Öffentliche IPv4-Quelladresse	<p>Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die Öffentliche IPv4-Quelladresse aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
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 neueste Version des bintec elmeg IPSec Clients.</p>
IPv4 Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer <i>aktiv</i> (aktiv) oder <i>Ruhend</i> (ruhend) ist. Bei <i>Ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum IPSec Peer besteht.

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen **Digitalisierungsbox**-Geräte den DynDNS-Dienst. Dieser Dienst ermöglicht die Identifikation eines Peers anhand eines durch DNS auflösbaren Host-Namens. Die Konfiguration der IP-Adresse des Peers ist nicht notwendig.

Der DynDNS-Dienst signalisiert aber nicht, ob ein Peer wirklich online ist, und kann einen Peer nicht veranlassen, eine Internetverbindung aufzubauen, um einen IPSec-Tunnel über das Internet zu ermöglichen. Diese Möglichkeit wird mit IPSec-Callback geschaffen: Mithilfe eines direkten ISDN-Rufs bei einem Peer kann diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf von Ihrem Gerät nicht angenommen werden muss. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muss zunächst auf der passiven Seite im Menü **Physikalische Schnittstellen->ISDN-Ports->MSN-Konfiguration->Neu** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld **Dienst** der Wert *IPSec* zur Verfügung. Dieser Eintrag sorgt dafür, dass auf dieser Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Bei aktivem Callback wird, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlasst, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer (**MSN** im Menü **Physikalische Schnittstellen->ISDN-Ports->MSN-Konfiguration->Neu** für **Dienst** *IPSec*) eingeht. Auf diese Weise wird sichergestellt, dass beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt, wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.



Hinweis

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec-Daemon zunächst die Schnittstelle aktiviert, über die der Tunnel realisiert werden soll. Sofern auf dem lokalen Gerät IPSec mit DynDNS konfiguriert ist, wird die eigene IP-Adresse propagiert und erst dann der ISDN-Ruf an das entfernte Gerät abgesetzt. Auf diese Art ist sichergestellt, dass das entfernte Gerät das lokale auch tatsächlich erreichen kann, wenn es den Tunnelaufbau initiiert.

Übermittlung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Geräts über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs. Einschränkungen, die bei der IPSec-Konfiguration mit dynamischen IP-Adressen auftreten, können so umgangen werden.



Hinweis

Um die Funktion IP-Adressübermittlung über ISDN nutzen zu können, müssen Sie eine kostenfreie Zusatzlizenz erwerben.

Die Lizenzdaten der Zusatzlizenzen erhalten Sie über die Online-Lizenzierungs-Seiten im Support-Bereich auf www.bintec-elmeg.com. Bitte folgen Sie den Anweisungen der Online-Lizenzierung.

Vor Systemsoftware Release 7.1.4 unterstützte der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Auslösers auf indirektem Wege (z. B. über DynDNS) ermittelt werden konnte. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse über ISDN umgangen. Darüber hinaus ermöglicht es diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus (Haupt Modus) für den Tunnelaufbau zu verwenden.

Funktionsweise: Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht. Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in *Felder im Menü IPv4 IPSec Callback* auf Seite 211 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der automatischen Auswahl durch das Gerät sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.



Hinweis

Damit Ihr Gerät die Informationen des gerufenen Peers über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Geräten analog vorgenommen werden.

Folgende Rollenverteilungen sind möglich:

- Eine Seite übernimmt die aktive, die andere die passive Rolle.
- Beide Seiten können beide Rollen (Beide) übernehmen.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

- (1) Peer A (der Auslöser des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.
- (2) Ihr Gerät erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden MIB-Eintrag.
- (3) Ihr Gerät setzt den initialen ISDN-Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.
- (4) Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten Calling Party Number (der ISDN-Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.
- (5) Der IPSec-Daemon auf Ihrem Gerät von Peer B kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil des Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.
- (6) Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.



Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Die folgenden Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü IPv4 IPSec Callback

Feld	Beschreibung
Modus	<p>Wählen Sie den Callback-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): IPSec-Callback ist deaktiviert. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • <i>Passiv</i>: Das lokale Gerät reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. • <i>Aktiv</i>: Das lokale Gerät setzt einen ISDN-Ruf an das entfernte Gerät ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gerät nicht. • <i>Beide</i>: Ihr Gerät kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gerät absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlasst (durch einen ausgehenden ISDN-Ruf).
Ankommende Rufnummer	<p>Nur für Modus = <i>Passiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.</p>
Ausgehende Rufnummer	<p>Nur für Modus = <i>Aktiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät 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

Feld	Beschreibung
	<p>automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen.</p> <ul style="list-style-type: none"> • <i>Spezifischen D-Kanalmodus verwenden</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. • <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übertragen. (Dies verursacht Kosten.) • <i>Nur B-Kanalmodus verwenden</i>: Ihr Gerät überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.
Modus des D-Kanals	<p>Nur für Übertragungsmodus = <i>Spezifischen D-Kanalmodus verwenden</i> oder <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i></p> <p>Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen.</p> <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 konfigurierter IPSec-Phase-1-Profile angezeigt.

IPSec-Peers

Phase-1-Profile

Phase-2-Profile

XAUTH-Profile

IP Pools

Optionen

IKEv1 (Internet Key Exchange, Version 1)

Ansicht 20

pro Seite << >>

Filtern in Keiner

gleich

Los

Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer		
<input checked="" type="radio"/>	Multi-Proposal	[AES/SHA1][AES/MD5][3DES/MD5]	Preshared Keys	Aggressiv	2 (1024 Bit)	0KB / 4h		

Seite: 1, Objekte: 1 - 1

Neues IKEv1-Profil erstellen

Neu

IKEv2 (Internet Key Exchange, Version 2)

Ansicht 20

pro Seite << >>

Filtern in Keiner

gleich

Los

Standard	Beschreibung	Proposals	Lebensdauer		
<input type="radio"/>	Multiproposal	[AES/SHA1][AES/MD5][3DES/SHA1][3DES/MD5]	4h		

Seite: 1, Objekte: 1 - 2

Neues IKEv2-Profil erstellen

Neu

OK

Abbrechen

Abb. 110: **VPN->IPSec->Phase-1-Profile**

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

IPSec-Peers	Phase-1-Profile	Phase-2-Profile	XAUTH-Profile	IP Pools	Optionen
-------------	------------------------	-----------------	---------------	----------	----------

Phase-1-Parameter (IKE)													
Beschreibung	IKE-1												
Proposals	<table border="1"> <tr> <th>Verschlüsselung</th> <th>Authentifizierung</th> <th>Aktiviert</th> </tr> <tr> <td>AES ▼</td> <td>MD5 ▼</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES ▼</td> <td>MD5 ▼</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES ▼</td> <td>MD5 ▼</td> <td><input type="checkbox"/></td> </tr> </table>	Verschlüsselung	Authentifizierung	Aktiviert	AES ▼	MD5 ▼	<input type="checkbox"/>	AES ▼	MD5 ▼	<input type="checkbox"/>	AES ▼	MD5 ▼	<input type="checkbox"/>
Verschlüsselung	Authentifizierung	Aktiviert											
AES ▼	MD5 ▼	<input type="checkbox"/>											
AES ▼	MD5 ▼	<input type="checkbox"/>											
AES ▼	MD5 ▼	<input type="checkbox"/>											
DH-Gruppe	<input type="radio"/> 1 (768 Bit) <input checked="" type="radio"/> 2 (1024 Bit) <input type="radio"/> 5 (1536 Bit)												
Lebensdauer	14400 Sekunden 0 kBytes												
Authentifizierungsmethode	Preshared Keys ▼												
Modus	<input type="radio"/> Main Modus (ID Protect) <input checked="" type="radio"/> Aggressiv <input type="checkbox"/> Strikt												
Lokaler ID-Typ	Fully Qualified Domain Name (FQDN) ▼												
Lokaler ID-Wert	octopus_f55												

Erweiterte Einstellungen	
Erreichbarkeitsprüfung	Automatische Erkennung ▼
Blockzeit	30 Sekunden
NAT-Traversal	Aktiviert ▼

Abb. 111: VPN->IPSec->Phase-1-Profile->Neu

Das Menü VPN->IPSec->Phase-1-Profile->Neu besteht aus folgenden Feldern:

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

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, welche die Art der Regel eindeutig identifiziert.
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Nachrichten-Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Nachrichten-Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld. Mindestens ein Proposal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <i>3DES</i> (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. • <i>AES</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die

Feld	Beschreibung
	<p>AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter <i>AES</i> gewählt, wird eine Schlüssellänge von 128 Bit verwendet.</p> <ul style="list-style-type: none"> • <i>AES-128</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 128 Bits angewendet. • <i>AES-192</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 192 Bits angewendet. • <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> (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • <i>SHA1</i>: SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. • <i>RipeMD 160</i>: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt. • <i>Tiger192</i>: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus. <p>Beachten Sie, dass die Beschreibung der Verschlüsselung und Authentifizierung oder der Hash-Algorithmen auf dem Kenntnisstand und der Meinung des Autors zum Zeitpunkt der Erstellung dieses Handbuchs basiert. Die Qualität der Algorithmen im besonderen unterliegt relativen Gesichtspunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.</p>
DH-Gruppe	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Die Diffie-Hellmann-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von Digitalisierungsbox unterstützt wird, steht für "modular exponentiation".</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>2 (1024 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>5 (1536 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	<p>Legen Sie die Lebensdauer für Phase-1-Schlüssel fest.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • Eingabe in Sekunden: Geben Sie die Lebensdauer für Phase-1-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist <i>14400</i>, das bedeutet, dass die Schlüssel erneuert werden, wenn vier Stunden abgelaufen sind. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-1- Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Der Standardwert ist <i>0</i>; das bedeutet, dass die Anzahl der gesendeten kBytes keine Rolle spielt.
Authentifizierungsmethode	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Pre Shared Keys wählen. Diese werden bei der Peerkonfiguration im Menü VPN->IPSec->IPSec-Peers konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • <i>DSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert. • <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert. • <i>RSA-Verschlüsselung</i>: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
Lokales Zertifikat	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Nur für Authentifizierungsmethode = <i>DSA-Signatur</i>, <i>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>

Feld	Beschreibung
	<p>Wählen Sie den Typ der lokalen ID aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i>
Lokaler ID-Wert	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für Authentifizierungsmethode = <i>DSA-Signatur</i>, <i>RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i> wird die Option Subjektnamen aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektnamen aus Zertifikat verwenden aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektnamen des Zertifikats verwendet.</p> <p>Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe Zertifikate auf Seite 48), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.</p>

Erreichbarkeitsprüfung

In der Kommunikation zweier IPSec-Peers kann es dazu kommen, dass einer der beiden z. B. aufgrund von Routing-Problemen oder aufgrund eines Neustarts nicht erreichbar ist. Dies ist aber erst dann feststellbar, wenn das Ende der Lebensdauer der Sicherheitsverbindung erreicht ist. Bis zu diesem Zeitpunkt gehen die Datenpakete verloren. Um dies zu verhindern, gibt es verschiedene Mechanismen einer Erreichbarkeitsprüfung. Im Feld **Erreichbarkeitsprüfung** wählen Sie aus, ob ein Mechanismus angewendet werden soll, um die Erreichbarkeit eines Peers zu überprüfen.

Hierbei stehen zwei Mechanismen zur Verfügung: Heartbeats und Dead Peer Detection.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Erreichbarkeitsprüfung	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Methode aus, mit der die Funktionalität der IPSec-Verbindung überprüft werden soll.</p> <p>Neben dem Standardverfahren Dead Peer Detection (DPD) ist auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. 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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden &Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • <i>Dead Peer Detection</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Erreichbarkeit des Peers nur überprüft, wenn tatsächlich Daten an ihn gesendet werden sollen. • <i>Dead Peer Detection (Idle)</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vorgenommen. <p>Nur für Phase-1-Parameter (IKEv2)</p> <p>Aktivieren oder deaktivieren Sie die Erreichbarkeitsprüfung.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Blockzeit	<p>Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche.</p> <p>Zur Verfügung stehen Werte von <i>-1</i> bis <i>86400</i> (Sekunden), der Wert <i>-1</i> bedeutet die Übernahme des Wertes im Standardprofil, der Wert <i>0</i>, dass der Peer in keinem Fall blockiert wird.</p> <p>Der Standardwert ist <i>30</i>.</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-Profiles</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert): NAT-Traversal ist aktiv. • <i>Deaktiviert</i>: NAT-Traversal ist deaktiviert. • <i>Erzwingen</i>: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. <p>Nur für <i>IKEv2-Profiles</i></p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CA-Zertifikate	Nur für Phase-1-Parameter (IKE)

Feld	Beschreibung
	<p>Nur für Authentifizierungsmethode = <i>DSA-Signatur</i>, <i>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.

The screenshot shows the 'Phase-2-Profile' configuration window. At the top, there are tabs for 'IPSec-Peers', 'Phase-1-Profile', 'Phase-2-Profile' (selected), 'XAUTH-Profile', 'IP Pools', and 'Optionen'. Below the tabs is a search bar with 'Ansicht 20', 'pro Seite << >>', 'Filtern in Keiner', 'gleich', and a 'Los' button. A table lists profiles with columns: 'Standard', 'Beschreibung', 'Proposals', 'PFS-Gruppe', and 'Lebensdauer'. The first row shows 'Standard' as the selected profile. At the bottom, there are buttons for 'Neu', 'OK', and 'Abbrechen'.

Abb. 112: **VPN->IPSec->Phase-2-Profile**

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.

The screenshot shows the 'Phase-2-Profile' configuration window with the 'Neu' (New) button selected. The window displays the 'Phase-2-Parameter (IPSEC)' section. The 'Beschreibung' field is set to 'IPSec-1'. The 'Proposals' section has a table with columns: 'Verschlüsselung', 'Authentifizierung', and 'Aktiviert'. The first row shows 'AES' for encryption, 'MD5' for authentication, and the 'Aktiviert' checkbox is checked. The 'PFS-Gruppe verwenden' section has a checked 'Aktiviert' checkbox and radio buttons for '1 (768 Bit)', '2 (1024 Bit)' (selected), and '5 (1536 Bit)'. The 'Lebensdauer' section has a '7200' value for 'Lebensdauer' and a '80' value for 'kBytes Schlüssel erneut erstellen nach'. Below this is the 'Erweiterte Einstellungen' section with three rows: 'IP-Komprimierung' (unchecked), 'Erreichbarkeitsprüfung' (set to 'Automatische Erkennung'), and 'PMTU propagieren' (checked). At the bottom, there are buttons for 'OK' and 'Abbrechen'.

Abb. 113: **VPN->IPSec->Phase-2-Profile->Neu**

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

Felder im Menü Phase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	<p>Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <i>3DES</i> (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • <i>-- ALLE --</i>: Alle Optionen können verwendet werden. • <i>AES</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter <i>AES</i> gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • <i>AES-128</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • <i>AES-192</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • <i>AES-256</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i> (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • <i>-- ALLE --</i>: Alle Optionen können verwendet werden. • <i>SHA1</i>: SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. <p>Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in</p>

Feld	Beschreibung
	Phase 2 nicht zur Verfügung stehen.
PFS-Gruppe verwenden	<p>Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (<i>Aktiviert</i>), sind die Optionen die gleichen, wie bei der Konfiguration von DH-Gruppe im Menü VPN->IPSec->Phase-1-Profile . PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind.</p> <p>Das Feld hat folgende Optionen:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>2 (1024 Bit)</i> (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>5 (1536 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	<p>Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen.</p> <p>Die neuen SAs werden bereits kurz vor dem Ablauf der aktuellen SAs ausgehandelt. Der Standardwert beträgt gemäß RFC 2407 acht Stunden, das bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <ul style="list-style-type: none"> • Eingabe in Sekunden: Geben Sie die Lebensdauer für Phase-2-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. 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	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

Feld	Beschreibung
	<p>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 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 eine Digitalisierungsbox ist. Wenn ja, wird <i>Heartbeats (Senden &Erwarten)</i> (bei Gegenstelle mit Digitalisierungsbox) oder <i>Inaktiv</i> (bei Gegenstelle ohne Digitalisierungsbox) gesetzt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden &Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen.
PMTU propagieren	<p>Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

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

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

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

14.1.4.1 Neu

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

Abb. 114: VPN->IPSec->XAUTH-Profile->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für dieses XAuth-Profil ein.
Rolle	Wählen Sie die Rolle des Gateways bei der XAuth-Authentifizierung aus. Mögliche Werte: <ul style="list-style-type: none"> <i>Server</i> (Standardwert): Das Gateway fordert einen Berechtigungsnachweis an. <i>Client</i>: Das Gateway weist seine Berechtigung nach.
Modus	Nur für Rolle = Server Wählen Sie aus, wie die Authentifizierung durchgeführt wird. Mögliche Werte: <ul style="list-style-type: none"> <i>RADIUS</i> (Standardwert): Die Authentifizierung wird über einen RADIUS-Server durchgeführt. Dieser wird im Menü Systemverwaltung->Remote Authentifizierung->RADIUS konfiguriert und im Feld RADIUS-Server Gruppen-ID ausgewählt. <i>Lokal</i>: Die Authentifizierung wird über eine lokal angelegte Liste durchgeführt.
Name	Nur für Rolle = Client Geben Sie den Authentifizierungsnamen des Clients ein.
Passwort	Nur für Rolle = Client Geben Sie das Authentifizierungspasswort ein.
RADIUS-Server Gruppen-ID	Nur für Rolle = Server Wählen Sie die gewünschte in Systemverwaltung->Remote Authentifi-


Feld	Beschreibung
	zierung->RADIUS konfigurierte RADIUS-Gruppe aus.
Benutzer	Nur für Rolle = <i>Server</i> und Modus = <i>Lokal</i> 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.

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-Adressvergabe** *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.

IPSec-PeersPhase-1-ProfilePhase-2-ProfileXAUTH-Profile**IP Pools**Optionen

Basisparameter

IP-Poolname

IP-Adressbereich

-

DNS-Server

Primär

Sekundär

OK

Abbrechen

Abb. 115: VPN->IPSec->IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll. Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

14.1.6 Optionen

IPSec-Peers	Phase-1-Profile	Phase-2-Profile	XAUTH-Profile	IP Pools	Optionen
-------------	-----------------	-----------------	---------------	----------	----------

Globale Optionen	
IPSec aktivieren	<input type="checkbox"/> Aktiviert
Vollständige IPSec-Konfiguration löschen	
IPSec-Debug-Level	Debug ▼

Erweiterte Einstellungen	
IPSec über TCP	<input type="checkbox"/> NCP Path Finder Technologie
Initial Contact Message senden	<input checked="" type="checkbox"/> Aktiviert
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<input type="checkbox"/> Aktiviert
Zero Cookies verwenden	<input type="checkbox"/> Aktiviert
Dynamische RADIUS-Authentifizierung	<input type="checkbox"/> Aktiviert
PKI-Verarbeitungsoptionen	
Zertifikatsanforderungs-Payloads nicht beachten	<input type="checkbox"/> Aktiviert
Zertifikatsanforderungs-Payloads senden	<input checked="" type="checkbox"/> Aktiviert
Zertifikatsketten senden	<input checked="" type="checkbox"/> Aktiviert
CRLs senden	<input type="checkbox"/> Aktiviert
Key Hash Payloads senden	<input checked="" type="checkbox"/> Aktiviert

Abb. 116: VPN->IPSec->Optionen

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

Felder im Menü Globale Optionen

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Benachrichtigung</i> • <i>Information</i> • <i>Debug</i> (Standardwert, niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level "Debug" sämtliche erzeugten Meldungen aufgezeichnet werden.</p>

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen **Digitalisierungsbox**-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	<p>Wählen Sie aus, ob IPSec über TCP verwendet werden soll.</p> <p>IPSec über TCP basiert auf der NCP-Path-Finder-Technologie. Diese Technologie sorgt dafür, dass der Datenverkehr (IKE, ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session eingebettet wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Initial Contact Message senden	<p>Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von <i>Aktiv</i> zu <i>Inaktiv</i>, <i>Ruhend</i> oder <i>Blockiert</i> geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zero Cookies verwenden	<p>Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen.</p> <p>Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall <i>Aktiviert</i>.</p>
Größe der Zero Cookies	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten und auf 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>

Feld	Beschreibung
	<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 Zertifikatanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungs-Payloads senden	<p>Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatanforderungen gesendet werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Zertifikatsketten senden	<p>Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.</p>
CRLs senden	<p>Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Key Hash Payloads senden	<p>Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen.</p> <p>Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung. Aktivieren Sie diese Funktion mit <i>Aktiviert</i>, um dieses Verhalten zu unterdrücken.</p>

Kapitel 15 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügt die **Digitalisierungsbox** 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 **Digitalisierungsbox** 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 einzelnen Sicherheitsinstanzen und ihrer Funktionsweise.

NAT

Eine der Grundfunktionen von NAT ist die Umsetzung lokaler IP-Adressen Ihres LANs in die globalen IP-Adressen, die Ihnen von Ihrem ISP zugewiesen werden, und umgekehrt. Dabei werden zunächst alle von außen initiierten Verbindungen abgeblockt, d. h. jedes Paket, welches Ihr Gerät nicht einer bereits bestehenden Verbindung zuordnen kann, wird abgewiesen. Auf diese Art kann eine Verbindung lediglich von innen nach außen aufgebaut werden. Ohne explizite Genehmigungen wehrt NAT jeden Zugriff aus dem WAN auf das LAN ab.

IP Access Listen

Hier werden Pakete ausschließlich aufgrund der oben aufgeführten Kriterien zugelassen oder abgewiesen, d. h. der Zustand der Verbindung wird nicht berücksichtigt (außer bei **Dienste** = *TCP*).

SIF

Die SIF sondert alle Pakete aus, die nicht explizit oder implizit zugelassen werden. Dabei gibt es sowohl

ein "Verweigern", bei dem keine Fehlermeldung an den Sender des zurückgewiesenen Pakets ausgegeben wird, als auch ein "Ablehnen", bei dem der Sender über die Ablehnung des Pakets informiert wird.

Die eingehenden Pakete werden folgendermaßen bearbeitet:

- Zunächst überprüft die SIF, ob ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann. Ist dies der Fall, wird es weitergeleitet. Kann das Paket keiner bestehenden Verbindung zugeordnet werden, wird überprüft, ob eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden). Ist dies der Fall, wird das Paket ebenfalls akzeptiert.
- Wenn das Paket keiner bestehenden und auch keiner zu erwartenden Verbindung zugeordnet werden kann, werden die SIF-Filterregeln angewendet: Trifft auf das Paket eine Deny-Regel zu, wird es abgewiesen, ohne dass eine Fehlermeldung an den Sender des Pakets geschickt wird; trifft eine Reject-Regel zu, wird das Paket abgewiesen und eine ICMPHost-Unreachable-Meldung an den Sender des Paktes ausgegeben. Nur wenn auf das Paket eine Accept-Regel zutrifft, wird es weitergeleitet.
- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen (= Standardverhalten).

Konkrete Hinweise für die Konfiguration einer Stateful Inspection Firewall (SIF) finden Sie am Ende des Kapitels unter [SIF - Konfigurationsbeispiel](#) auf Seite 241.

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 Schnittstelle** 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.


IPv4-FilterregelnIPv6-FilterregelnOptionen


Ansicht20 pro Seite<<>>Filtern inKeiner gleichLos


Abfolge	Quelle	Ziel	Dienst	Aktion	Priorität	Richtlinie aktiv
Seite: 1						
Standardfilterregeln						
Abfolge	Quelle	Ziel	Dienst	Aktion	Priorität	Richtlinie aktiv
n+1	Vertrauenswürdige Schnittstelle	 Beliebig	beliebig	Zugriff	Keiner	<input checked="" type="checkbox"/> Aktiviert
n+2	Nicht vertrauenswürdige Schnittstellen	Beliebig	beliebig	Verweigern	Keiner	<input checked="" type="checkbox"/> Aktiviert

NeuOKAbbrechen

Abb. 117: Firewall->Richtlinien->IPv4-Filterregeln

Mit der Schaltfläche  in der Zeile **Vertrauenswürdige Schnittstelle** 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 Dialog, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

15.1.1.1 Neu

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

IPv4-FilterregelnIPv6-FilterregelnOptionen

Basisparameter

Quelle	--- GROUPS ---
Ziel	--- GROUPS ---
Dienst	--- SERVICES ---
Aktion	Zugriff

OKAbbrechen

Abb. 118: Firewall->Richtlinien->IPv4-Filterregeln->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	<p>Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</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</p>

Feld	Beschreibung
	<p>aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <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 vertrauenswürdigen und nicht vertrauenswürdigen Zonen besteht. Die beiden Sicherheitsrichtlinien *Vertrauenswürdig* bzw. *Nicht Vertrauenswürdig* beschreiben diese Vorstellung. Sie definieren die beiden Filterregeln **Vertrauenswürdige Schnittstelle** 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 konfigurierter IPv6-Filterregeln angezeigt.

IPv4-Filterregeln
IPv6-Filterregeln
Optionen

Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los

Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv
Seite: 1					
Standardfilterregeln					
Abfolge	Quelle	Ziel	Dienst	Aktion	Richtlinie aktiv
n+1	Vertrauenswürdige Schnittstelle	Beliebig	beliebig	Zugriff	<input checked="" type="checkbox"/> Aktiviert
n+2	Nicht vertrauenswürdige Schnittstellen	Beliebig	beliebig	Verweigern	<input checked="" type="checkbox"/> Aktiviert

Neu
OK
Abbrechen

Abb. 119: Firewall->Richtlinien->IPv6-Filterregeln

Mit der Schaltfläche in der Zeile **Vertrauenswürdige Schnittstelle** 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.

IPv4-Filterregeln
IPv6-Filterregeln
Optionen

Basisparameter

Quelle	--- GROUPS --- ▼
Ziel	--- GROUPS --- ▼
Dienst	--- SERVICES --- ▼
Aktion	Zugriff ▼

OK
Abbrechen

Abb. 120: Firewall->Richtlinien->IPv6-Filterregeln->Neu

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

Felder im Menü Basisparameter

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

IPv4-FilterregelnIPv6-FilterregelnOptionen

Globale Firewall-Optionen

Status der IPv4-Firewall

☒ Aktiviert

Protokollierte Aktionen

Alle

Vollständige IPv4-Filterung

☒ Aktivieren

Sitzungstimer

UDP-Inaktivität

180

Sekunden

TCP-Inaktivität

3600

Sekunden

PPTP-Inaktivität

86400

Sekunden

Andere Inaktivität

30

Sekunden

Firewall auf Werkseinstellungen zurücksetzen

Firewall auf Werkseinstellungen zurücksetzen

Zurücksetzen

OK

Abbrechen

Abb. 121: Firewall->Richtlinien->Optionen

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

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Status der IPv4-Firewall	<p>Aktivieren oder deaktivieren Sie die IPv4-Firewall-Funktion.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierte Aktionen	<p>Wählen Sie den Firewall-Syslog-Level aus.</p> <p>Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Alle</i> (Standardwert): Alle Firewall-Aktivitäten werden angezeigt.• <i>Verweigern</i>: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion".• <i>Annehmen</i>: Nur Accept-Ereignisse werden angezeigt.• <i>Keiner</i>: Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige IPv4-Filterung	<p>Bei TCP-Sessions überwacht die SIF im ersten Schritt, ob eine Session korrekt und vollständig aufgebaut wird. Im zweiten Schritt erfolgt die eigentliche Filterung. Für diesen "Normalfall" ist die Standardeinstellung Vollständige IPv4-Filterung <i>Aktivieren</i> vorgesehen.</p> <p>Wenn bei zweiseitiger Kommunikation eine Richtung des Datenverkehrs über den Router läuft, die Datenpakete der entgegengesetzten Richtung aber einen anderen Weg nehmen, wird der Datenverkehr vom Router nicht zugelassen, weil die Session aus Sicht der SIF unvollständig ist. Dies gilt auch, wenn es eine Regel gibt, die denselben Datenverkehr bei vollständiger Session durchlassen würde.</p> <p>Um den Datenverkehr bei solchen unvollständigen Sessions durchzulassen, müssen Sie Vollständige IPv4-Filterung deaktivieren.</p>

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 30 bis 86400.</p> <p>Der Standardwert ist 180.</p>
TCP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine TCP -Session als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von 30 bis 86400.</p> <p>Der Standardwert ist 3600.</p>
PPTP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine PPTP-Session als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von 30 bis 86400.</p> <p>Der Standardwert ist 86400.</p>
Andere Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine Session eines anderen Typs als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von 30 bis 86400.</p> <p>Der Standardwert ist 30.</p>

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 konfigurierter 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 Schnittstellen-Gruppen einzurichten.

IPv4-GruppenIPv6-Gruppen

Basisparameter

Beschreibung

Mitglieder

Schnittstelle

Auswahl

LAN_LOCAL

☐

LAN_EN1-4

☐

WAN_EFM35-60

☐

LAN_EN1-0-1

☐

BRIDGE_BR0

☐

WLAN_STA7-90

☐

WAN_ETHOA35-5

☐

OK

Abbrechen

Abb. 122: Firewall->Schnittstellen->IPv4-Gruppen->Neu

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

Felder im Menü **Basisparameter**

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

15.2.2 IPv6-Gruppen

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

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

15.2.2.1 Neu

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

IPv4-GruppenIPv6-Gruppen

Basisparameter

Beschreibung

Mitglieder

Schnittstelle

Auswahl

LOCAL

☐

OK

Abbrechen

Abb. 123: Firewall->Schnittstellen->IPv6-Gruppen->Neu

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

Felder im Menü **Basisparameter**

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der IPv6-Schnittstellen-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Schnittstellen die Mitglie-

Feld	Beschreibung
	der 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 konfigurierter Adressen angezeigt.

15.3.1.1 Neu

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

Adressliste Gruppen

Basisparameter	
Beschreibung	<input type="text"/>
IPv4	<input checked="" type="checkbox"/> Aktiviert
Adresstyp	<input checked="" type="radio"/> Adresse/Subnetz <input type="radio"/> Adressbereich
Adresse/Subnetz	<input type="text"/> / <input type="text" value="255.255.255.0"/>
IPv6	<input type="checkbox"/> Aktiviert

OK Abbrechen

Abb. 124: Firewall->Adressen->Adressliste->Neu

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein.
IPv6	<p>Erlaubt die Konfiguration von IPv6-Adresslisten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Adresse/Präfix	<p>Nur für IPv6 = <i>Aktiviert</i></p> <p>Geben Sie die IPv6-Adresse und das zugehörige Präfix ein.</p>

15.3.2 Gruppen

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

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

15.3.2.1 Neu

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

AdresslisteGruppen

Basisparameter

Beschreibung

IP-Version

☒ IPv4

☐ IPv6

Auswahl

AdressenAuswahl

ANY

OK

Abbrechen

Abb. 125: Firewall->Adressen->Gruppen->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Adressgruppe ein.
IP-Version	<p>Wählen Sie die verwendete IP-Version aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">IPv4IPv6 <p>Standardmäßig ist <i>IPv4</i> ausgewählt.</p>
Auswahl	Wählen Sie aus den zur Verfügung stehenden Adressen die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

15.4 Dienste

15.4.1 Diensteliste

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

15.4.1.1 Neu

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

DienstelisteGruppen

Basisparameter

Beschreibung

Protokoll

Beliebig

OK

Abbrechen

Abb. 126: Firewall->Dienste->Diensteliste->Neu

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Echo Reply</i> • <i>Destination Unreachable</i> • <i>Source Quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time Exceeded</i> • <i>Parameter Problem</i> • <i>Timestamp</i> • <i>Timestamp Reply</i> • <i>Information Request</i> • <i>Information Reply</i> • <i>Address Mask Request</i> • <i>Address Mask Reply</i>
Code	<p>Nur für Typ = <i>Destination Unreachable</i> stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig (Standardwert)</i> • <i>Net Unreachable</i> • <i>Host Unreachable</i> • <i>Protocol Unreachable</i> • <i>Port Unreachable</i> • <i>Fragmentation Needed</i> • <i>Communication with Destination Network is 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 konfigurierter 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.

Diensteliste

Gruppen

Basisparameter

Beschreibung

Mitglieder

Dienst	Auswahl
activity	<input type="checkbox"/>
ah	<input type="checkbox"/>
any	<input type="checkbox"/>
apple-qt	<input type="checkbox"/>
auth	<input type="checkbox"/>
chargen	<input type="checkbox"/>
clients_1	<input type="checkbox"/>
clients_2	<input type="checkbox"/>
daytime	<input type="checkbox"/>
dhcp	<input type="checkbox"/>
discard	<input type="checkbox"/>
dns	<input type="checkbox"/>
echo	<input type="checkbox"/>
esp	<input type="checkbox"/>
exec	<input type="checkbox"/>
finger	<input type="checkbox"/>
ftp	<input type="checkbox"/>
gopher	<input type="checkbox"/>
http	<input type="checkbox"/>
t-online (XCEPT)	<input type="checkbox"/>
talk	<input type="checkbox"/>
telnet	<input type="checkbox"/>
terminal server	<input type="checkbox"/>
ttcp	<input type="checkbox"/>
time	<input type="checkbox"/>
timed	<input type="checkbox"/>
trace	<input type="checkbox"/>
unix print	<input type="checkbox"/>
unpriv	<input type="checkbox"/>
ups	<input type="checkbox"/>
uucp-path	<input type="checkbox"/>
who	<input type="checkbox"/>
whois	<input type="checkbox"/>
wins	<input type="checkbox"/>
x400	<input type="checkbox"/>

OK

Abbrechen

Abb. 127: Firewall->Dienste->Gruppen->Neu

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

Felder im Menü **Basisparameter**

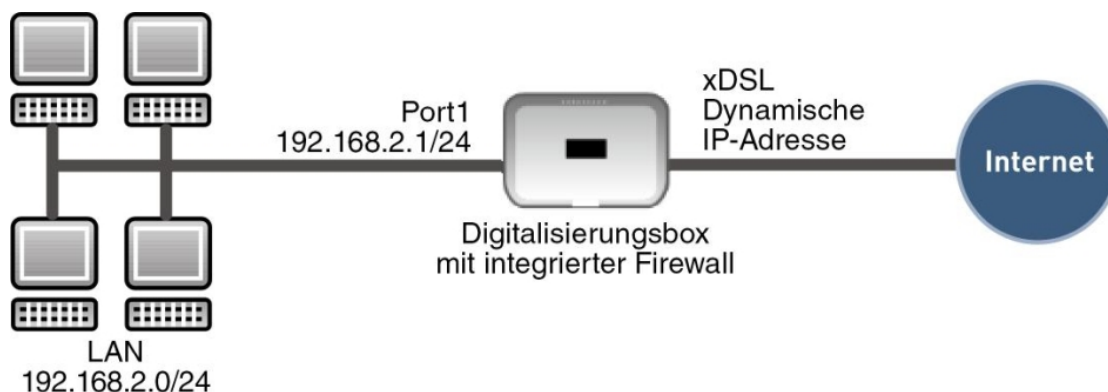
Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung der Service-Gruppe ein.
Mitglieder	Wählen Sie aus den zur Verfügung stehenden Service-Aliases die Mitglieder der Gruppe aus. Aktivieren Sie dazu das Feld in der Spalte Auswahl .

15.5.1 SIF - Konfigurationsbeispiel

Voraussetzungen

- Verbindung zum Internet
- Ihr LAN muss mit dem Port 1, 2, 3 oder 4 Ihrer Digitalisierungsbox verbunden sein

Beispielszenario



Konfigurationsziel

- Den Mitarbeitern eines Unternehmens sollen nur bestimmte Dienste im Internet zur Verfügung stehen (HTTP, HTTPS, FTP, DNS).
- Die Digitalisierungsbox soll als DNS-Proxy arbeiten, das heißt, die Clients verwenden die Digitalisierungsbox als DNS-Server.
- Nur der Systemadministrator und der Geschäftsführer sollen eine HTTP- und eine Telnetverbindung zur Digitalisierungsbox 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 der Digitalisierungsbox 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	<i>z. B. Administrator</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	<i>z. B. 192.168.2.2 mit 255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	<i>z. B. Geschäftsführer</i>
Adresstyp	Firewall -> Adressen ->	<i>Adresse/Subnetz</i>

Feld	Menü	Wert
	Adressliste -> Neu	
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.2.3</i> mit <i>255.255.255.255</i>
Beschreibung	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>Digitalisierungsbox</i>
Adresstyp	Firewall -> Adressen -> Adressliste -> Neu	<i>Adresse/Subnetz</i>
Adresse/Subnetz	Firewall -> Adressen -> Adressliste -> Neu	z. B. <i>192.168.2.254</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>192.168.2.0</i> mit <i>255.255.255.0</i>

Adressgruppen

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

Dienstgruppen

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

Filterregel 1: Digitalisierungsbox verwalten (Systemadministrator)

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

Filterregel 2: Digitalisierungsbox als DNS-Proxy verwenden

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	<i>LOCAL</i>

Feld	Menü	Wert
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	ANY
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	dns
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Zugriff
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Netzwerk_Intern
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Digitalisierungsbox
Dienst	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	dns
Aktion	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Zugriff

Filterregel 3: Zugriff von außen auf die Digitalisierungsbox verweigern

Feld	Menü	Wert
Quelle	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	ANY
Ziel	Firewall -> Richtlinien -> IPv4-Filterregeln -> Neu	Digitalisierungsbox
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 VoIP

Voice over IP (VoIP) nutzt das IP-Protokoll für Sprach- und Bildübertragung.

Der wesentliche Unterschied zur herkömmlichen Telefonie besteht darin, dass die Sprachinformationen nicht über eine geschaltete Verbindung in einem Telefonnetz übertragen werden, sondern durch das Internet-Protokoll in Datenpakete aufgeteilt, die auf nicht festgelegten Wegen in einem Netzwerk zum Ziel gelangen. Diese Technologie macht sich so für die Sprachübertragung die Infrastruktur eines bestehenden Netzwerks zu Nutze und teilt sich dieses mit anderen Kommunikationsdiensten.

Das Session Initiation Protocol (SIP) dient dabei zum Aufbau, zum Abbau und zur Steuerung einer Kommunikationssitzung.

16.1 Application Level Gateway

Um IP-Telefonen die Verbindung über SIP mit einem VoIP Provider zu ermöglichen, verfügt Ihr Gerät über ein Application Level Gateway (ALG), d.h. einen entsprechenden Proxy, der die notwendigen NAT- und Firewall-Freigaben vornimmt.



Hinweis

Das Application Level Gateway muss immer dann genutzt werden, wenn auf der Schnittstelle, welche die Verbindung zum Internet herstellt, NAT aktiviert ist.

16.1.1 SIP-Proxys

Sie sehen hier eine Liste der bereits konfigurierten Application Level Gateway Einträge. Diese Einträge aktivieren das ALG. Jeder Eintrag definiert einen bestimmten TCP oder UDP Zielport, der vom ALG überwacht werden soll. Standardmäßig sind im Auslieferungszustand zwei Einträge für die SIP Ports TCP 5060 und UDP 5060 entsprechend der IANA Definition angelegt.

16.1.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Application Level Gateway Einträge zu erstellen.

SIP-Proxys SIP-Endpunkte

Basisparameter	
Beschreibung	<input type="text"/>
Administrativer Status	<input checked="" type="checkbox"/> Aktiviert
Protokoll	UDP <input type="text"/> Zielport <input type="text"/>
Timeout der Sitzung	<input type="text"/> Sekunden
Low Latency Transmission	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 128: **VoIP->Application Level Gateway->SIP-Proxys->** **->Neu**

Das Menü **VoIP->Application Level Gateway->SIP-Proxys->** **->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Application Level Gateways ein.

Feld	Beschreibung
Administrativer Status	<p>Wählen Sie aus, ob der SIP Proxy aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches verwendet werden soll.</p> <p>Mögliche Werte: <i>UDP</i> (Standardwert) oder <i>TCP</i>.</p> <p>Geben Sie als Zielpport den Port ein, der vom Proxy überwacht werden soll.</p> <p>Pro Destination Port, zu dem sich VoIP Clients aus dem LAN verbinden können, müssen Sie einen Proxy anlegen.</p> <p>Die Ports können Provider-spezifisch sein.</p>
Timeout der Sitzung	<p>Geben Sie die Zeit in Sekunden ein, welche eine Session bestehen bleiben soll, wenn keine Datenpakete gesendet oder empfangen werden.</p> <p>Dieser Wert muss größer sein als die SIP Expire Time des angeschlossenen SIP Clients (SIP Telefone, Terminaladapter usw.)</p> <p>Der Standardwert ist <i>1800</i>.</p>
Low Latency Transmission	<p>Wählen Sie aus, ob ein Mechanismus zur Minimierung der Laufzeit, die VoIP-Datenpakete für den "Weg" zwischen zwei Gesprächspartnern benötigen, verwendet werden soll. Das garantiert eine gute Sprachqualität bei hoher Leitungsauslastung.</p> <p>Beachten Sie, dass Low Latency Transmission nur für Rufe eingeschaltet werden muss, die nicht über die in VoIP ->Media Gateway konfigurierten Verbindungen hergestellt werden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

16.1.2 SIP-Endpunkte

Hier wird eine Liste aller SIP-Sessions angezeigt, welche vom ALG verwaltet werden.


Dazu gehören statische Einträge, um interne SIP-Server/-Proxies (z. B. interne Asterisk-Server) vom WAN aus (Internet) durch NAPT hindurch erreichbar zu machen. Weiterhin können interne SIP-Clients ohne Registrierung durch einen statischen Eintrag erreichbar gemacht werden. Außerdem werden dynamisch alle aktiven SIP-Sitzungen erkannt, die von internen SIP-Terminals aus initiiert wurden, und hier aufgelistet. Diese werden nur für Monitoring und Administration angezeigt und können nicht bearbeitet werden.



Hinweis

Alle automatisch generierten Einträge, die länger als 24 Stunden nicht verwendet wurden, werden automatisch aus der Tabelle gelöscht.

16.1.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um statische Einträge für SIP-Terminals innerhalb des LAN hinzuzufügen, welche von Terminals aus dem WAN über die NAPT-Barriere erreichbar sein sollen. Wählen Sie das Symbol , um vorhandene statische Einträge zu bearbeiten.



Hinweis

Dynamisch erstellte Einträge aktiver Sitzungen können nicht bearbeitet werden. Diese Einträge können nur entfernt werden, mit der Folge, dass die entsprechende SIP-Verbindung sofort beendet wird.

SIP-Proxy
SIP-Endpunkte

Basisparameter	
Endpunkttyp	<input checked="" type="radio"/> Client <input type="radio"/> Server
Protokoll	<div style="border: 1px solid black; padding: 2px;">UDP ▼</div>
Interne IP-Adresse	<div style="border: 1px solid black; height: 15px; width: 100%;"></div>
Entfernter Port	<div style="border: 1px solid black; padding: 2px;">0</div>
Externer Port	<div style="border: 1px solid black; padding: 2px;">0</div>

OK
Abbrechen

Abb. 129: **VoIP->Application Level Gateway->SIP-Endpunkte->** **->Neu**

Das Menü **VoIP->Application Level Gateway->SIP-Endpunkte->** **->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Endpunkttyp	<p>Wählen Sie die Rolle des SIP-Endpunktes im LAN aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Client</i> (Standardwert): Der interne SIP-Endpunkt ist ein SIP-Client (z. B. Telefone). <i>Server</i>: Der interne SIP-Endpunkt ist ein SIP-Server, an dem sich SIP-Endpunkt von extern anmelden können.
Protokoll	<p>Wählen Sie das Protokoll aus, welches für die Datenübertragung verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>UDP</i> (Standardwert) <i>TCP</i> <p>Wenn ein Protokoll automatisch erkannt wurde, sollte es nicht geändert werden.</p>
Interne IP-Adresse	Geben Sie die IP-Adresse des internen SIP-Endpunktes im LAN an.
Entfernter Port	<p>Nur für Endpunkttyp = <i>Client</i></p> <p>Geben Sie den Port des entfernten SIP-Terminals (im WAN) an.</p>
Interner Port	<p>Nur für Endpunkttyp = <i>Server</i></p> <p>Geben Sie den Port des internen SIP-Endpunktes im LAN an.</p>
Externer Port	<p>Geben Sie den Port auf der WAN-Seite des Gateways an, der für den Zugang durch die NAPT-Barriere zu einem SIP-Endpunkt im LAN genutzt wird.</p> <p>Bei Clients wird der externe Port automatisch erkannt und sollte nicht ge-</p>

Feld	Beschreibung
	ändert werden.


16.2 Einstellungen

16.2.1 Teilnehmer

Hier können Sie die Rufnummern der Endgeräte (=Teilnehmer) konfigurieren, die an das Media Gate-way angebunden sind, d.h. die Rufnummern der SIP-Endgeräte sowie der angeschalteten ISDN-Endgeräte abhängig von den verfügbaren Schnittstellen.

Im Menü **VoIP->Einstellungen->Teilnehmer** wird eine Liste aller vorhandenen Teilnehmer angezeigt.

16.2.1.1 Bearbeiten oder Neu

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

TeilnehmerSIP-KontenStandorteISDN-TrunksOptionen

Basisparameter

Beschreibung	
Teilnehmer / Benutzername	
Schnittstellentyp	<input checked="" type="radio"/> SIP <input type="radio"/> ISDN <input type="radio"/> Analog
Registrierung	<input checked="" type="checkbox"/> Aktiviert
Standort	Nicht definiert (Registrierung nur in privaten Netzwerken) ▼
Gültigkeit	60 Sekunden
Authentifizierungs-ID	
Passwort	
Protokoll	UDP ▼
Port	5060

Erweiterte Einstellungen

Codec-Einstellungen

Codec-Reihenfolge	<input checked="" type="radio"/> Standard <input type="radio"/> Qualität <input type="radio"/> Niedrigste <input type="radio"/> Höchste															
Sortierreihenfolge	<table><tr><td><input checked="" type="checkbox"/> G.711 uLaw</td><td><input checked="" type="checkbox"/> G.711 aLaw</td><td><input checked="" type="checkbox"/> G.729</td><td><input type="checkbox"/> G.726-40</td><td><input type="checkbox"/> T.38 Fax</td></tr><tr><td><input type="checkbox"/> G.726-32</td><td><input type="checkbox"/> G.726-24</td><td><input type="checkbox"/> G.726-16</td><td><input type="checkbox"/> RFC 2833</td><td><input type="checkbox"/> SRTP</td></tr><tr><td><input type="checkbox"/> Daten (RFC 4040)</td><td><input type="checkbox"/> SIP-Info</td><td></td><td></td><td></td></tr></table>	<input checked="" type="checkbox"/> G.711 uLaw	<input checked="" type="checkbox"/> G.711 aLaw	<input checked="" type="checkbox"/> G.729	<input type="checkbox"/> G.726-40	<input type="checkbox"/> T.38 Fax	<input type="checkbox"/> G.726-32	<input type="checkbox"/> G.726-24	<input type="checkbox"/> G.726-16	<input type="checkbox"/> RFC 2833	<input type="checkbox"/> SRTP	<input type="checkbox"/> Daten (RFC 4040)	<input type="checkbox"/> SIP-Info			
<input checked="" type="checkbox"/> G.711 uLaw	<input checked="" type="checkbox"/> G.711 aLaw	<input checked="" type="checkbox"/> G.729	<input type="checkbox"/> G.726-40	<input type="checkbox"/> T.38 Fax												
<input type="checkbox"/> G.726-32	<input type="checkbox"/> G.726-24	<input type="checkbox"/> G.726-16	<input type="checkbox"/> RFC 2833	<input type="checkbox"/> SRTP												
<input type="checkbox"/> Daten (RFC 4040)	<input type="checkbox"/> SIP-Info															

Sprachqualitätseinstellungen

Echounterdrückung	<input checked="" type="checkbox"/> Aktiviert
Comfort Noise Generation (CNG)	<input checked="" type="checkbox"/> Aktiviert
Paketgröße	20 ms

OK

Abbrechen

Abb. 130: **VoIP->Einstellungen->Teilnehmer->  ->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Teilnehmers ein.
Teilnehmer / Benutzername	ISDN-Endgeräte: Geben Sie die Rufnummer des Teilnehmers.

Feld	Beschreibung
me	<p>SIP-Endgeräte: Geben Sie den Benutzernamen ein.</p> <p>Maximal können 40 Zeichen eingegeben werden.</p>
Schnittstellentyp	<p>Wählen Sie den Schnittstellentyp aus, welcher verwendet werden soll.</p> <p>Die Auswahl ist von den verfügbaren Schnittstellen abhängig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SIP</i>: Ein SIP-Endgerät wird für den Ruf verwendet. • <i>ISDN</i>: Ein ISDN-Endgerät wird für den Ruf verwendet. • <i>Analog</i>: Ein analoges Endgerät wird für den Ruf verwendet.
Analoge Schnittstelle auswählen	<p>Nur für Schnittstellentyp = <i>Analog</i></p> <p>Wählen Sie eine analoge Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • fxs4-0 (Standardwert) • fxs4-1 • fxs4-2 • fxs4-3
ISDN-Schnittstelle auswählen	<p>Nur für Schnittstellentyp = <i>ISDN</i></p> <p>Wählen Sie eine ISDN-Schnittstelle aus. Welche ISDN-Schnittstellen Sie auswählen können, hängt vom verwendeten Gerät ab.</p>
Registrierung	<p>Nur für Schnittstellentyp = <i>SIP</i></p> <p>Wählen Sie, ob der Registrierungsmechanismus per SIP REGISTER Meldung benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Abgesehen von diesem Standard-Vorgehen können die relevanten Daten auch an eine bestimmte IP-Adresse geschickt werden, die den Verbindungspartnern bereits bekannt ist. Dann entfallen Registrierung und Authentisierung, in diesem Fall muss die Funktion Registrierung deaktiviert sein. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP.</p>
Gültigkeit	<p>Nur wenn Registrierung aktiviert ist.</p> <p>Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird.</p> <p>Bei Clients wird der externe Port automatisch erkannt und sollte nicht geändert werden.</p> <p>Zur Verfügung stehen Werte von 0 bis 3600.</p> <p>Der Standardwert ist 60.</p>
SIP-Endpunkt-IP-Adresse	<p>Nur wenn Registrierung deaktiviert ist.</p>

Feld	Beschreibung
	Für Konfigurationen, bei denen keine Registrierung vorgesehen ist (z. B. Anbindung an einen Microsoft Exchange Communication Server), kann die Verbindung als statischer Host eingerichtet werden. Hierzu ist es nötig, die statische IP-Adresse des Endgeräts anzugeben.
Authentifizierungs-ID	<p>Nur für Schnittstellentyp = <i>SIP</i></p> <p>Tragen Sie einen Namen ein, der zur Authentifizierung verwendet wird.</p> <p>Maximal können 20 Zeichen eingegeben werden.</p> <p>Den hier vergebenen Namen müssen Sie auch auf dem SIP-Telefon eingeben.</p> <p>Wenn Sie keinen Namen eingeben, wird der Name im Feld Teilnehmer / Benutzername verwendet.</p>
Passwort	<p>Nur für Schnittstellentyp = <i>SIP</i></p> <p>Geben Sie hier ein Passwort ein.</p> <p>Maximal können 20 Zeichen eingegeben werden.</p> <p>Das hier vergebene Passwort müssen Sie auch auf dem SIP-Telefon eingeben.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches für die Datenübertragung verwendet werden soll.</p> <p>Mögliche Werte: <i>UDP</i> (Standardwert), <i>TCP</i> oder <i>TLS</i>.</p> <p>Wenn ein Protokoll automatisch erkannt wurde, sollte es nicht geändert werden.</p>
Port	<p>Geben Sie die Nummer des UDP, TCP bzw. TLS Ports, der für die Verbindung zum Server bzw. Proxy benutzt werden soll.</p> <p>Mögliche Werte sind <i>0</i> bis <i>65535</i>.</p> <p>Der Standardwert ist <i>5060</i>.</p>

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

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Reihenfolge	<p>Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Standard</i> (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich. <i>Qualität</i>: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. <i>Niedrigste</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. <i>Höchste</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.
Sortierreihenfolge	Wählen Sie die Codecs aus, die für die Verbindung vorgeschlagen wer-

Feld	Beschreibung
	<p>den sollen. Abhängig von der Einstellung im Feld Codec-Reihenfolge werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>G. 711 uLaw</i>: ISDN Codec nach US Kennlinie • <i>G. 711 aLaw</i>: ISDN Codec nach EU Kennlinie • <i>G. 729</i>: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • <i>G. 726-40</i>: Komprimiert von 63 auf 40 KBit/s • <i>G. 726-32</i>: Komprimiert von 55 auf 32 KBit/s • <i>G. 726-24</i>: Komprimiert von 47 auf 24 KBit/s • <i>G. 726-16</i>: Komprimiert von 39 auf 16 KBit/s • <i>T. 38 Fax</i>: Ermöglicht den Versand von Faxmitteilungen über Daten-netzwerke. • <i>SRTP</i>: SRTP ist eine verschlüsselte Variante des Real-Time Transport Protokolls (RTP). • <i>Daten (RFC 4040)</i>: Ermöglicht den Transport eines 64-kbit/s-Datenstroms in RTP-Paketen. • <i>SIP-Info</i>: Ermöglicht DTMF-Signalisierung über SIP <p>Standardmäßig sind <i>G. 711 uLaw</i>, <i>G. 711 aLaw</i> und <i>G. 729</i> aktiviert.</p> <p>Die tatsächlich verwendeten Codecs sind die Schnittmenge der hier festgelegten und der vom Provider signalisierten Codecs. Von diesen Co-decs fallen bei ausgehenden Rufen noch diejenigen weg, welche mehr als die verfügbare Bandbreite benötigen würden.</p>

Felder im Menü Sprachqualitätseinstellungen

Feld	Beschreibung
Echounterdrückung	<p>Wählen Sie aus, ob Echounterdrückung verwendet werden soll.</p> <p>Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Comfort Noise Generation (CNG)	<p>Wählen Sie aus, ob Comfort Noise Generation (CNG) verwendet werden soll.</p> <p>Bei digitaler Sprachübertragung sorgt dieses Verfahren durch das Erzeugen eines leichten Hintergrundrauschens dafür, dass während Gesprächspausen beim Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Paketgröße	<p>Geben Sie an, wieviel Millisekunden Sprache ein RTP-Datenpaket enthält.</p> <p>Zur Verfügung stehen Werte von <i>5</i> bis <i>500</i>.</p> <p>Der Standardwert ist <i>20</i>.</p>

16.2.2 SIP-Konten

Wenn Sie Ihr Gerät an andere SIP-Server (z. B. Server von Internet SIP Service Providern) anbinden wollen, können Sie hier die notwendigen Einträge konfigurieren. In diesem Fall fungiert das Media Gateway als SIP-Client.

Außerdem können Sie hier die Einträge für SIP-Trunking-Szenarios konfigurieren. In diesem Fall fungiert das Media Gateway als SIP-Server für andere SIP-Server. Ein Beispiel hierfür ist die Anbindung einer SIP-PBX (z. B. Asterisk) an das Media Gateway.

Das bedeutet, dass sowohl alle SIP-Provider-Accounts hier konfiguriert werden als auch mit dem Media Gateway verbundene durchwahlfähige Telefonanlagen (Direct Dial-in).




Hinweis

Verwenden Sie dieses Menü auf keinen Fall zur Konfiguration von SIP-Nebenstellen, d.h. für SIP-Clients oder PSTN-Clients wie z. B. SIP-Telefone, Terminal Adapter oder ISDN-Telefone!

SIP-Nebenstellen können Sie im Menü **VoIP->Teilnehmer** konfigurieren.

Im Menü **VoIP->Einstellungen->SIP-Konten** wird eine Liste aller vorhandenen SIP-Konten (SIP Client Modus und SIP Server Modus) angezeigt.

16.2.2.1 Bearbeiten oder Neu

Wählen Sie die Schaltfläche **Neu**, um neue SIP-Konten hinzuzufügen. Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. In diesem Menü werden sowohl SIP-Konten im SIP Client Modus als auch im SIP Server Modus konfiguriert.

Teilnehmer
SIP-Konten
Standorte
ISDN-Trunks
Optionen

Basisparameter	
Beschreibung	<input type="text"/>
Administrativer Status	<input checked="" type="checkbox"/> Aktiviert
Trunk-Modus	<input checked="" type="radio"/> Aus <input type="radio"/> Client <input type="radio"/> Server <input type="radio"/> gw-trunk
Registrar	<input type="text"/>
Ausgehender Proxy	<input type="text"/>
Realm	<input type="text"/>
Protokoll	UDP ▼ Port: 5060
Benutzername	<input type="text"/>
Authentifizierungs-ID	<input type="text"/>
Passwort	<input type="password"/>
Registrierung	<input checked="" type="checkbox"/> Aktiviert
Gültigkeit	600 <input type="text"/> Sekunden
Angerufene Adresse	Auto ▼

Erweiterte Einstellungen

Codec-Einstellungen																
Codec-Reihenfolge	<input checked="" type="radio"/> Standard <input type="radio"/> Qualität <input type="radio"/> Geringe Bandbreite <input type="radio"/> Hohe Bandbreite															
Sortierreihenfolge	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> G.711 uLaw</td> <td><input checked="" type="checkbox"/> G.711 aLaw</td> <td><input checked="" type="checkbox"/> G.729</td> <td><input type="checkbox"/> G.726-40</td> <td><input type="checkbox"/> T.38 Fax</td> </tr> <tr> <td><input type="checkbox"/> G.726-32</td> <td><input type="checkbox"/> G.726-24</td> <td><input type="checkbox"/> G.726-16</td> <td><input type="checkbox"/> RFC 2833</td> <td><input type="checkbox"/> SRTP</td> </tr> <tr> <td><input type="checkbox"/> Daten (RFC 4040)</td> <td><input type="checkbox"/> SIP-Info</td> <td></td> <td></td> <td></td> </tr> </table>	<input checked="" type="checkbox"/> G.711 uLaw	<input checked="" type="checkbox"/> G.711 aLaw	<input checked="" type="checkbox"/> G.729	<input type="checkbox"/> G.726-40	<input type="checkbox"/> T.38 Fax	<input type="checkbox"/> G.726-32	<input type="checkbox"/> G.726-24	<input type="checkbox"/> G.726-16	<input type="checkbox"/> RFC 2833	<input type="checkbox"/> SRTP	<input type="checkbox"/> Daten (RFC 4040)	<input type="checkbox"/> SIP-Info			
<input checked="" type="checkbox"/> G.711 uLaw	<input checked="" type="checkbox"/> G.711 aLaw	<input checked="" type="checkbox"/> G.729	<input type="checkbox"/> G.726-40	<input type="checkbox"/> T.38 Fax												
<input type="checkbox"/> G.726-32	<input type="checkbox"/> G.726-24	<input type="checkbox"/> G.726-16	<input type="checkbox"/> RFC 2833	<input type="checkbox"/> SRTP												
<input type="checkbox"/> Daten (RFC 4040)	<input type="checkbox"/> SIP-Info															

Sprachqualitätseinstellungen	
Echounterdrückung	<input checked="" type="checkbox"/> Aktiviert
Comfort Noise Generation (CNG)	<input checked="" type="checkbox"/> Aktiviert
Paketgröße	20 <input type="text"/> ms

OK
Abbrechen

Abb. 131: VoIP->Einstellungen->SIP-Konten-> ->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des SIP-Kontos ein.
Administrativer Status	<p>Wählen Sie aus, ob das SIP-Konto aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Trunk-Modus	<p>Wählen Sie aus, ob und in welchem Trunk-Modus das SIP-Konto betrieben werden soll.</p> <p>Durch den Trunk-Modus (DDI, Direct Dial In) wird ermöglicht, dass ein eingehender Ruf genau einem Endgerät zugeordnet werden kann (Durchwahl). Bei einem ausgehenden Ruf kann der Anrufer dem Angerufenen angezeigt werden.</p> <p>Welche Einstellung verwendet werden kann, hängt vom Provider ab.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Aus</i> (Standardwert): Der Trunk-Modus wird nicht verwendet. Das SIP-Konto hat nur eine Nummer.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Client</i>: Das Media Gateway wird als DDI-Client betrieben. Es erhält eine Durchwahl. • <i>Server</i>: Das Media Gateway wird als DDI-Server betrieben, so daß sich DDI-Clients verbinden können. • <i>gw-trunk</i>: Das Media Gateway wird als DDI-Client betrieben, aber als Trunk verwendet. Diese Einstellung dient zum Anschluss einer softwarebasierten IP-Telefonanlage von Swyx.
Registrar	<p>Nur für Trunk-Modus = <i>Aus</i>, <i>Client</i> und <i>gw-trunk</i>. Tragen Sie die IP-Adresse oder den Domännennamen (FQDN) des SIP Registrars ein. Maximale Zeichenzahl ist 40.</p> <p>Einträge mit Leerzeichen sind nicht erlaubt.</p>
SIP-Endpunkt-IP-Adresse	<p>Nur für Trunk-Modus = <i>Server</i> und Registrierung deaktiviert</p> <p>Tragen Sie die IP-Adresse oder den Domännennamen (FQDN) des SIP Proxy Servers ein.</p>
Ausgehender Proxy	<p>Nur für Trunk-Modus = <i>Aus</i>, <i>Client</i> oder <i>gw-trunk</i></p> <p>Geben Sie den Namen oder die IP-Adresse des SIP Outbound Proxy Servers ein.</p> <p>Maximal können 32 Zeichen eingegeben werden.</p> <p>Hier müssen Sie nur dann einen Eintrag vornehmen, wenn bei allen SIP Sessions die Kommunikation nicht direkt sondern über einen weiteren Proxy erfolgen soll.</p> <p>Im SIP Client Modus: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dies explizit vom Provider vorgegeben wird.</p>
Realm	<p>Tragen Sie einen weiteren Domännennamen oder eine weitere IP-Adresse des SIP Proxy Servers ein.</p> <p>Wenn Sie keine Angaben machen, wird der Eintrag im Feld Registrar verwendet.</p> <p>Im SIP Client Modus: Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dieser explizit vom Provider vorgegeben wird.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches zum Datentransport verwendet werden soll.</p> <p>Mögliche Werte: <i>UDP</i> (Standardwert) oder <i>TCP</i></p> <p>Geben Sie den Port ein, über den die Daten transportiert werden sollen.</p> <p>Der Standardwert ist <i>5060</i>.</p> <p>Im SIP Client Modus: Die Ports können Provider-spezifisch sein.</p>
Benutzername	<p>Im SIP Client Modus: Tragen Sie hier den Benutzernamen für die Authentifizierung ein, wenn Ihnen Ihr VoIP-Provider einen solchen zugewiesen hat.</p> <p>Im SIP Server Modus: Sie müssen den Benutzernamen festlegen.</p> <p>Maximal können 40 Zeichen eingegeben werden.</p>
Authentifizierungs-ID	<p>Tragen Sie einen Namen ein, der zur Authentifizierung beim Outbound Proxy verwendet wird.</p>

Feld	Beschreibung
	<p>Wenn Sie keinen Namen eingeben, wird der Name im Feld Benutzerna-me verwendet.</p> <p>Im SIP Client Modus: Tragen Sie nur dann einen Namen ein, wenn dieser explizit vom Provider vorgegeben wird.</p>
Passwort	<p>Im SIP Client Modus: Der VoIP-Provider weist Ihnen eine PIN bzw. Passwort für die Authentifizierung zu. Diesen Wert müssen Sie hier eingeben.</p> <p>Im SIP Server Modus: Legen Sie eine PIN bzw. ein Passwort fest.</p> <p>Maximal können 40 Zeichen eingegeben werden.</p>
Registrierung	<p>Wählen Sie aus, ob der Registrierungsmechanismus per SIP REGISTER Meldung benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Abgesehen von diesem Standard-Vorgehen können die relevanten Daten auch an eine bestimmte IP-Adresse geschickt werden, die den Verbindungspartnern bereits bekannt ist. Dann entfallen Registrierung und Authentisierung, in diesem Fall muss die Funktion Registrierung deaktiviert sein. Ein Beispiel für diese Vorgehensweise ist Microsoft Exchange SIP.</p>
Gültigkeit	<p>Nur wenn Registrierung aktiviert ist.</p> <p>Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird.</p> <p>Zur Verfügung stehen Werte von 0 bis 38400.</p> <p>Der Standardwert ist 600.</p> <p>Ein Server kann in seiner Antwort auf eine REGISTER Anfrage eine andere Gültigkeit festlegen, welche die hier festgelegte überschreibt.</p>
Angerufene Adresse	<p>Legt fest, aus welchem Parameter der angerufenen Adresse die Rufnummer extrahiert wird.</p> <p>Die angerufene Adresse hat folgendes Format: Adresse = "Anzeige" <Benutzer>, z. B. "+49911987543" <sip:+49911987543@tel.telekom.de></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Extrahiert die Rufnummer aus dem ersten Teil der Adresse. Wenn dies fehlschlägt, wird die Rufnummer aus dem zweiten Teil der Adresse extrahiert. • <i>Benutzer</i>: Extrahiert die Rufnummer aus dem zweiten Teil der Adresse, z. B. aus <sip:+49911987543@tel.telekom.de>. • <i>Anzeige</i>: Extrahiert die Rufnummer aus dem ersten Teil der Adresse, z. B. aus "+49911987543".

Felder im Menü Trunk-Einstellungen

Feld	Beschreibung
SIP-Header-Feld(er) für	Nur für Trunk-Modus = <i>Client</i> , <i>Server</i> oder <i>gw-trunk</i>

Feld	Beschreibung
Anruferadresse	<p>Wählen Sie für ausgehende Rufe die Position der Absender-ID (z.B. Rufnummer) im SIP-Header aus. (Bei eingehenden Rufen wird automatisch die Rufnummer aus dem SIP Header ermittelt.)</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i> (Standardwert): Die Absender-ID wird nicht übertragen. • <i>Anzeige und Benutzername</i>: Die Absender-ID wird im SIP Header im Feld "Display" und im Feld "User" übertragen. • <i>Nur Anzeige</i>: Die Absender-ID wird im SIP Header im Feld "Display" übertragen. • <i>Nur Benutzer</i>: Die Absender-ID wird im SIP Header im Feld "User" übertragen. • <i>P-Preferred</i>: Der SIP Header wird durch das sogenannte "p-preferred-identity" Feld erweitert, um dort die Absender-ID zu übertragen. • <i>P-Asserted</i>: Der SIP Header wird durch das sogenannte "p-asserted-identity" Feld erweitert, um dort die Absender-ID zu übertragen.
Rufnummer	<p>Nur für Trunk-Modus = <i>Server</i></p> <p>Sie können eine Nummer setzen, die bei ausgehenden Rufen der Absenderrufnummer als Prefix vorangestellt wird und bei eingehenden Rufen von den führenden Stellen der Zielrufnummer abgeschnitten wird. Das entspricht der Rumpfnr einer TK-Anlage.</p>

Felder im Menü Codec-Einstellungen

Feld	Beschreibung
Codec-Reihenfolge	<p>Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Der Codec, welcher im Menü an erster Stelle steht, wird verwendet, wenn möglich. • <i>Qualität</i>: Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • <i>Geringe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • <i>Hohe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchste Bandbreite benötigt, wird verwendet, wenn möglich.
Sortierreihenfolge	<p>Wählen sie die Codecs aus, die für die Verbindung vorgeschlagen werden sollen. Abhängig von der Einstellung im Feld Codec-Reihenfolge werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>G. 711 uLaw</i>: ISDN Codec nach US Kennlinie • <i>G. 711 aLaw</i>: ISDN Codec nach EU Kennlinie • <i>G. 729</i>: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • <i>G. 726-40</i>: Komprimiert von 63 auf 40 KBit/s

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>G. 726-32</i>: Komprimiert von 55 auf 32 KBit/s • <i>G. 726-24</i>: Komprimiert von 47 auf 24 KBit/s • <i>G. 726-16</i>: Komprimiert von 39 auf 16 KBit/s • <i>T. 38 Fax</i>: Ermöglicht den Versand von Faxmitteilungen über Daten-netzwerke. • <i>RFC 2833</i>: Ermöglicht DTMF-Signalisierung im Sprachkanal • <i>SRTP</i>: SRTP ist eine verschlüsselte Variante des Real-Time Transport Protokolls (RTP). • <i>Daten (RFC 4040)</i>: Ermöglicht den Transport eines 64-kbit/s-Datenstroms in RTP-Paketen. • <i>SIP-Info</i>: Ermöglicht DTMF-Signalisierung über SIP <p>Standardmäßig sind <i>G. 711 uLaw</i>, <i>G. 711 aLaw</i> und <i>G. 729</i> aktiviert.</p> <p>Die tatsächlich verwendeten Codecs sind die Schnittmenge der hier festgelegten und der vom Provider signalisierten Codecs. Von diesen Co-decs fallen bei ausgehenden Rufen noch diejenigen weg, welche mehr als die verfügbare Bandbreite benötigen würden.</p>

Felder im Menü Sprachqualitätseinstellungen

Feld	Beschreibung
Echounterdrückung	<p>Wählen Sie aus, ob Echounterdrückung verwendet werden soll.</p> <p>Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Comfort Noise Generation (CNG)	<p>Wählen Sie aus, ob Comfort Noise Generation (CNG) verwendet werden soll.</p> <p>Bei digitaler Sprachübertragung sorgt dieses Verfahren durch das Erzeugen eines leichten Hintergrundrauschens dafür, dass während Gesprächspausen beim Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Paketgröße	<p>Geben Sie an, wieviel Millisekunden Sprache ein RTP-Datenpaket enthält.</p> <p>Zur Verfügung stehen Werte von <i>5</i> bis <i>500</i>.</p> <p>Der Standardwert ist <i>20</i>.</p>

16.2.3 Standorte

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

Zur Verwendung des Bandbreitenmanagements können einzelne Standorte eingerichtet werden. Ein Standort wird anhand seiner festen IP-Adresse bzw. DynDNS-Adresse oder mittels der Schnittstelle, an der das Gerät angeschlossen ist, identifiziert. Für jeden Standort kann die verfügbare VoIP-Bandbreite (Up- und Downstream) eingestellt werden.

Nur für Kompaktsysteme: Ein vordefinierter Eintrag mit den Parametern **Beschreibung** = *LAN*, **Beinhalten Standort (Parent)** = *Keiner*, **Typ** = *Schnittstellen*, **Schnittstellen** = *LAN_EN1-0* wird angezeigt.

Teilnehmer SIP-Konten **Standorte** ISDN-Trunks Optionen

Registrierungsverhalten für VoIP-Teilnehmer ohne definierten Standort

Standardverhalten

☐ Keine Registrierung
☒ Registrierung nur in privaten Netzwerken
☐ Uneingeschränkte Registrierung

Ansicht 20 pro Seite << >> Filtern in Keine gleich Los

Beschreibung	URLs/IP-Adressen /Schnittstellen	Max. Upstream-Bandbreite	Max. Downstream-Bandbreite		
LAN	BRIDGE_BR0	-	-		

Seite: 1, Objekte: 1 - 1

OK Neu

Abb. 132: VoIP->Einstellungen->Standorte

Felder im Menü Registrierungsverhalten für VoIP-Teilnehmer ohne definierten Standort

Feld	Beschreibung
Standardverhalten	<p>Legen Sie fest, wie das System bei der Registrierung von VoIP-Teilnehmern verfahren soll, für die kein Standort definiert wurde.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Registrierung nur in privaten Netzwerken</i> (Standardwert): Der VoIP-Teilnehmer wird nur registriert, wenn er sich innerhalb des privaten Netzwerks befindet. <i>Nicht erlaubt</i>: Der VoIP-Teilnehmer wird nie registriert. <i>Uneingeschränkte Registrierung</i>: Der VoIP-Teilnehmer wird immer registriert.

16.2.3.1 Bearbeiten oder Neu

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

Teilnehmer SIP-Konten **Standorte** ISDN-Trunks Optionen

Grundeinstellungen

Beschreibung

Beinhalten Standort (Parent) Keiner ▼

Typ ☒ Adressen ☐ Schnittstellen

Adressen

IP-Adresse/DNS-Name Netzmaske
Hinzufügen

Bandbreitenbegrenzung Upstream ☐ Aktiviert

Bandbreitenbegrenzung Downstream ☐ Aktiviert

Erweiterte Einstellungen

DSCP-Einstellungen für RTP-Daten DSCP-Binärwert ▼

OK Abbrechen

Abb. 133: VoIP->Einstellungen->Standorte->Neu

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
Beschreibung	Geben Sie die Beschreibung des Eintrags ein.
Beinhalteter Standort (Parent)	Sie können die SIP-Standorte beliebig kaskadieren. Definieren Sie hier, welcher schon definierte SIP-Standort für den hier zu konfigurierenden SIP-Standort den übergeordneten Knoten bildet.
Typ	<p>Wählen Sie aus, ob der Standort mittels IP-Adressen/DNS-Namen oder Schnittstellen definiert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Adressen</i> (Standardwert): Der SIP-Standort wird über IP-Adressen bzw. DNS-Namen definiert. • <i>Schnittstellen</i>: Der SIP-Standort wird über die verfügbaren Schnittstellen definiert.
Adressen	<p>Nur für Typ = <i>Adressen</i></p> <p>Geben Sie die IP-Adressen der Geräte an den SIP-Standorten ein.</p> <p>Klicken Sie auf Hinzufügen um neue Adressen zu konfigurieren.</p> <p>Geben Sie unter IP-Adresse/DNS-Name die gewünschte IP-Adresse bzw. den DNS-Namen ein.</p> <p>Geben Sie ebenfalls die erforderliche Netzmaske ein.</p>
Schnittstellen	<p>Nur für Typ = <i>Schnittstellen</i></p> <p>Geben Sie die Schnittstellen an, an denen die Geräte eines SIP-Standorts angeschlossen sind.</p> <p>Klicken Sie auf Hinzufügen, um neue Schnittstelle auszuwählen.</p> <p>Wählen Sie unter Schnittstelle die gewünschte Schnittstelle aus.</p>
Bandbreitenbegrenzung Upstream	<p>Legen Sie fest, ob die Upstream-Bandbreite begrenzt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Bandbreite reduziert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upstream-Bandbreite	Geben Sie die maximale Datenrate in Senderichtung in kBits pro Sekunde ein.
Bandbreitenbegrenzung Downstream	<p>Legen Sie fest, ob die Downstream-Bandbreite begrenzt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Bandbreite reduziert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Downstream-Bandbreite	Geben Sie die maximale Datenrate in Empfangsrichtung in kBits pro Sekunde ein.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
DSCP-Einstellungen für RTP-Daten	<p>Wählen Sie die Art des Dienstes für RTP-Daten aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p>

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

16.2.4 ISDN-Trunks

Für die Konfiguration im Menü **ISDN-Trunks** muss Ihr Gerät über mindestens zwei ISDN-Anschlüsse im Punkt-zu-Punkt-Modus (BRI oder PRI) verfügen, die als TE (Sammelanschluss) oder NT konfiguriert sind.




Hinweis

Beachten Sie, dass bei BRI-Anschlüssen der Anschlussmodus (NT Mode oder TE Mode) per Jumper im Gerät umgeschaltet werden muss.

In diesem Menü werden ISDN-Sammelanschlüsse (Bundles) festgelegt.

16.2.4.1 Bearbeiten oder Neu

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

Teilnehmer
SIP-Konten
Standorte
ISDN-Trunks
Optionen

Basisparameter

Beschreibung	<input type="text"/>
ISDN-Modus	Trunk ▼
	<input type="checkbox"/> bri-1

OK
Abbrechen

Abb. 134: VoIP->Einstellungen->ISDN-Trunks

Das Menü **VoIP->Einstellungen->ISDN-Trunks** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Sammelanschlusses ein. Maximale Zeichenzahl ist 40.

Feld	Beschreibung
ISDN-Modus	<p>Wählen Sie den Modus aus, in welchem der Sammelanschluss betrieben wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Extern</i> (Standardwert): Punkt-zu-Punkt TE-Anschluss (Telekom Sammelanschluss) • <i>Trunk</i>: Punkt-zu-Punkt NT-Anschluss (für den Anschluss einer TK-Anlage).
Mitglieder	<p>Wählen Sie die gewünschten ISDN-Schnittstellen aus, die zu diesem Sammelanschluss gehören sollen.</p> <p>Sie können diejenigen ISDN-Schnittstellen auswählen, die im Punkt-zu-Punkt-Modus konfiguriert sind.</p>

16.2.5 Optionen

Im Menü **VoIP->Einstellungen->Optionen** können Sie globale Einstellungen für das Media Gateway vornehmen.

Teilnehmer SIP-Konten Standorte ISDN-Trunks **Optionen**

Basisparameter	
Status des Media Gateways	<input checked="" type="checkbox"/> Aktiviert
Session Border Controller Modus	Auto ▼
Anruflkontrolle für lokale Nummern	<input checked="" type="checkbox"/> Aktiviert
Media Stream Termination	<input checked="" type="checkbox"/> Aktiviert
Standard-Abwurfnebenstelle	<input type="text"/>
Wahlpause	5 <input type="text"/> Sekunden

Erweiterte Einstellungen

Kurzwahl	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">Abkürzung</div> <div style="border: 1px solid #ccc; padding: 2px; flex-grow: 1;">Ersetzen durch</div> <div style="border: 1px solid #ccc; padding: 2px; width: 30px; margin-left: 5px;"></div> </div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Hinzufügen"/> </div>
----------	--

Abb. 135: **VoIP->Einstellungen->Optionen**

Das Menü **VoIP->Einstellungen->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Status des Media Gateways	<p>Wählen Sie aus, ob die Funktion Media Gateway aktiviert sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Session Border Controller Modus	<p>Wählen Sie aus, wie sich das Media Gateway in Verbindung mit einem Session Border Controller verhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Die Anruflkontrolle wird für alle Nebenstellen, die mit einem existierenden SIP-Konto exakt übereinstimmen, vom Session Border Controller durchgeführt, d.h. alle SIP-Meldungen, die für das entsprechende SIP-Konto konfiguriert sind, werden an den Session

Feld	Beschreibung
	<p>Border Controller weitergeleitet. Für alle anderen Nebenstellen wird die Anrufkontrolle vom Media Gateway entsprechend der unter Anrufkontrolle konfigurierten Einträge durchgeführt. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup).</p> <ul style="list-style-type: none"> • <i>Aus</i>: Die Anrufkontrolle wird ausschließlich vom Media Gateway entsprechend der unter Anrufkontrolle konfigurierten Einträge und der lokalen Nebenstellen durchgeführt. Für Rufe, die über einen bestimmten Provider (SIP-Konto) geroutet werden sollen, müssen Sie einen entsprechenden Anrufkontrolle-Eintrag konfigurieren. Interne Rufe (von interner Nebenstelle zu interner Nebenstelle), die nur lokal geroutet werden müssen, benötigen keinen zusätzlichen Anrufkontrolle-Eintrag. • <i><SIP Trunk></i>: Wählen Sie ein unter VoIP->Media Gateway->SIP-Konten konfiguriertes SIP Trunk Konto aus. Die Anrufkontrolle wird in diesem Fall für alle Nebenstellen vom Session Border Controller ausgeführt, alle SIP-Meldungen werden an den Session Border Controller weitergeleitet. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup). <p>Hinweis: Einträge in Anrufkontrolle haben Vorrang vor der Session Border Controller Konfiguration!</p>
Anrufkontrolle für lokale Nummern	<p>Legen Sie fest, ob Routing-Einträge vor Durchwahlnummern favorisiert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Media Stream Termination	<p>Wählen Sie aus, wie RTP-Sessions vom System kontrolliert werden sollen.</p> <p>Wenn die Funktion aktiv ist, werden die RTP-Sessions auf dem Media Gateway terminiert, d.h. alle RTP Streams werden vom Media Gateway kontrolliert und über das Media Gateway geroutet. Die beteiligten Endgeräte (z. B. SIP-Telefone) sind nicht direkt miteinander verbunden. Beachten Sie, dass das Media Gateway bei VoIP-zu-VoIP-Verbindungen unterschiedliche Codecs der beteiligten VoIP-Endgeräte nicht übersetzt. Daher müssen die Codecs von Media Gateway und VoIP-Endgeräten übereinstimmen.</p> <p>Wenn die Funktion nicht aktiv ist, werden die RTP-Sessions nicht auf dem Media Gateway terminiert, d.h. alle RTP Streams werden ohne Terminierung vom Media Gateway geroutet. Die RTP-Datenpakete können in komplexen Netzen somit auch über andere Gateways geroutet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Standard-Abwurfnebenstelle	<p>Sie können eine Nebenstelle angeben, zu der eingehende Telefonate geleitet werden, die keiner Extension oder angeschlossenen TK-Anlage zugeordnet werden können.</p>
Wahlpause	<p>Geben Sie die maximale Verzögerungszeit ein bis das System die eingegebene Telefonnummer als vollständig wertet und der SIP-Wahlvorgang (Senden der SIP INVITE Message) startet. Diese Zeitspanne wird mit jedem Tastendruck zurückgesetzt.</p> <p>Mögliche Werte sind 0 bis 15.</p>

Feld	Beschreibung
	Der Standardwert ist 5.
	Wenn Sie die Rufnummer mit # abschließen, wird sofort gewählt.

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Kurzwahl	<p>Definieren Sie kurze Ziffernfolgen, die anstatt der kompletten Nummer gewählt werden können.</p> <p>Klicken Sie auf Hinzufügen um neue Kurzwahlen zu konfigurieren.</p> <p>Geben Sie unter Abkürzung die gewünschte Kurzwahl für den Benutzer ein, z. B. <i>123</i>.</p> <p>Geben Sie unter Ersetzen durch die Rufnummer ein, welche anstelle der Kurzwahl gewählt werden soll, z. B. <i>09119673</i>.</p> <p>Wenn in obigem Beispiel ein Benutzer <i>*123</i> eintippt, wählt das Gerät <i>09119673</i>.</p> <p>Möchte der Benutzer die Nebenstelle <i>111</i> erreichen, so tippt er <i>*123111</i> ein. Das Gerät wählt <i>09119673111</i>.</p> <p>Ein Punkt am Ende der Nummer zeigt eine komplette Nummer an. Diese wird nach dem Einsetzen sofort gewählt.</p>

Wenn Sie eine Kurzwahl aus dieser Liste nutzen wollen, müssen Sie * und dann die Kurzwahl wählen.

16.3 Media Gateway

Ein Media Gateway dient als Übersetzungsinstanz zwischen verschiedenen Telekommunikationsnetzen wie z. B. zwischen dem herkömmlichen Telefonnetz und den Next Generation Networks (IP-Netzwerken).

Mit der **Digitalisierungsbox** Media Gateway kann ein Unternehmen, das mit einer durchwahlfähigen Telefonanlage an einem leitungsvermittelten Telefonnetz ausgestattet ist, mit einem SIP Trunking Service Provider im Internet verbunden werden und somit IP-Telefonie nutzen.

Die **Digitalisierungsbox** Media Gateway unterstützt die Anbindung mehrerer SIP Provider Accounts. Sie können mit diesem Gateway Nebenstellen einrichten, einen Rufnummernplan anlegen und Telefonanlagen-Funktionen konfigurieren sowie die Sprachdaten-Übertragung bei geringer Bandbreite der Upload-Verbindung optimieren.



Hinweis


Ihr Gerät muss mit einem DSP-Modul ausgestattet sein, um die Media Gateway Funktionen nutzen zu können. Informationen zum Einbau des DSP-Moduls finden Sie in der Einbauanleitung, die dem Modul beiliegt.

16.3.1 Anrufrückmeldung

Hier können Sie die Bedingungen für das Weiterleiten von Anrufen (Routing) festlegen. Sie legen hier eine Liste mit Regeln oder Regelketten fest, die dazu dienen, die signalisierte Zielrufnummer zu manipulieren.

Im Menü **VoIP->Media Gateway->Anrufrückmeldung** wird eine Liste aller vorhandenen Einträge angezeigt.

16.3.1.1 Bearbeiten oder Neu

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

AnrufkontrolleCLID-UmwandlungRufnummerntransformation

Basisparameter

Beschreibung

Administrativer Status

☒ Aktivieren

Typ

Erlauben ▾





Anrufende Leitung

Beliebig ▾

Anrufende Adresse

Angerufene Adresse

Routing-Regeln

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion		
1	-					

Hinzufügen

Routing-Regel

Priorität

1

Administrativer Status

☒ Aktivieren

Leitung

bri-1 ▾

Transformation der gerufenen Adresse

Übernehmen

OK

Abbrechen

Abb. 136: VoIP->Media Gateway->Anrufkontrolle->  ->Neu

Das Menü **VoIP->Media Gateway->Anrufkontrolle->  ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Eintrags ein.
Administrativer Status	Wählen Sie aus, ob derEintrag aktiv sein soll. Mit <i>Aktivieren</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Typ	Wählen Sie aus, wie der Ruf weitergeleitet werden soll. Mögliche Werte: <ul style="list-style-type: none">• <i>Erlauben</i>: Für Rufe, die vom Media Gateway an eine Telefonanlage oder einen ISDN-TE-Anschluss oder einen SIP DDI Client weitergeleitet werden sollen. Dazu können verwendet werden: PRI-Schnittstellen im NT-Modus, BRI-Schnittstellen im NT-Modus, SIP-Konten im Trunk-Modus (Server Modus) .• <i>Verweigern</i>: Für Rufe, die nicht weitergeleitet (gesperrt) werden sollen.
Anrufende Leitung	Sie können die Anwendung des Eintrags auf die Leitung begrenzen, auf welcher der Ruf ankommt. Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP-Konten ab.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>fxs</i><Schnittstellen-Index>: Begrenzt den Eintrag auf die gewählte analoge Schnittstelle. • <i>bri</i><Schnittstellen-Index>: Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • <i><SIP-Konto></i>: Begrenzt den Eintrag auf das gewählte SIP-Konto. • <i>Beliebig</i>: Keine Begrenzung des Eintrags.
Anrufende Adresse	Sie können die Anwendung des Eintrags auf einen bestimmten Anrufer begrenzen. Dazu müssen Sie die Rufnummer exakt angeben (keine Wildcards).
Angerufene Adresse	<p>Geben Sie die angerufene Adresse ein, auf die die Regel angewendet werden soll.</p> <p>Dazu geben Sie eine Adresse numerisch (z. B. eine Rufnummer) oder alphanumerisch (z. B. für einen Trunk) ein, die mit der gewählten Adresse verglichen wird.</p> <p>Dabei können Sie folgende Wildcards verwenden:</p> <ul style="list-style-type: none"> • * bedeutet, dass am Ende einer Zeichenfolge beliebige weitere Zeichen folgen können. • ? dient als Platzhalter für ein beliebiges Zeichen. <p>Wenn die konfigurierte Adresse mit der signalisierten Adresse übereinstimmt, wird der Eintrag angewandt.</p>

Im Bereich **Routing-Regeln** definieren Sie Regeln, die bestimmen, wie die Rufnummer manipuliert wird, bevor sie für den Wahlvorgang verwendet wird.

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

Felder im Menü **Routing-Regeln** (Nur für Typ = Erlauben)

Feld	Beschreibung
Priorität	<p>Geben Sie eine ganze Zahl beginnend mit 1 in aufsteigender Reihenfolge ein, um die Reihenfolge der Filterregeln festzulegen.</p> <p>Die Regeln werden in der Liste in der angegebenen Reihenfolge "abgearbeitet".</p> <p>Ist eine Leitung bzw. ein SIP-Konto nicht verfügbar, wird automatisch die nächste Regel verwendet.</p>
Administrativer Status	<p>Wählen Sie aus, ob die Regel aktiv sein soll.</p> <p>Mit <i>Aktivieren</i> wird die Regel aktiv.</p> <p>Standardmäßig ist die Regel aktiv.</p>
Leitung	Wählen Sie die Leitung für den ausgehenden Ruf aus.
Transformation der gerufenen Adresse	<p>Geben Sie ein, wie die Rufnummer manipuliert werden soll, bevor sie für den Wahlvorgang verwendet wird.</p> <p>Notation: <a:b>; d.h. a wird durch b ersetzt. Jede Regel muss durch einen Strichpunkt abgeschlossen sein. Mehrere Regeln können zu einer Regelkette zusammengefasst werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>;. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der</p>


Feld	Beschreibung
	<p>"best match" Methode sortiert.</p> <p>Numerische und alphanumerische Werte sind zulässig.</p> <p>? dient als Platzhalter für ein beliebiges Zeichen.</p>
	<p>Beispiel 16.1. Beispiel für eine Regel</p> <ul style="list-style-type: none"> • Regel: <:+49911>; • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

16.3.2 CLID-Umwandlung


Hier legen Sie die Bearbeitung der Rufnummer des Anrufers (Calling Party Number) bei eingehenden Anrufen fest. Sie können z. B. zu einer empfangenen Telefonnummer einen Prefix hinzufügen, um entsprechende ausgehende Gespräche über ein bestimmtes SIP-Konto zu routen.

Im Menü **VoIP->Media Gateway->CLID-Umwandlung** wird eine Liste aller vorhandenen Einträge angezeigt, bei denen die empfangene Rufnummer bearbeitet wird.

16.3.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Einträge für CLID-Umwandlung hinzuzufügen.

Anrufkontrolle		CLID-Umwandlung		Rufnummerntransformation	
Basisparameter					
Beschreibung	<input type="text"/>				
Rufnummer	Beliebig ▼				
Angerufene Leitung	Beliebig ▼				
Angerufene Adresse	<input type="text"/>				
Transformation der rufenden Adresse	<input type="text"/>				
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 137: **VoIP->Media Gateway->CLID-Umwandlung->  ->Neu**

Das Menü **VoIP->Media Gateway->CLID-Umwandlung->  ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Eintrags ein.
Rufnummer	<p>Wählen Sie die ISDN-Leitung oder das SIP-Konto, von welcher bzw. von welchem der Anruf kommt.</p> <p>Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP-Konten ab.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>fxs</i><Schnittstellen-Index>: Begrenzt den Eintrag auf die gewählte analoge Schnittstelle. • <i>bri</i><Schnittstellen-Index>: Begrenzt den Eintrag auf die ge-

Feld	Beschreibung
	<p>wählte BRI-Schnittstelle.</p> <ul style="list-style-type: none"> • <i><SIP-Konto></i>: Begrenzt den Eintrag auf das gewählte SIP-Konto. • <i>Beliebig</i>: Keine Begrenzung des Eintrags.
Angerufene Leitung	<p>Sie können optional die Zielleitung des Anrufs angeben.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>fxs<Schnittstellen-Index></i>: Begrenzt den Eintrag auf die gewählte analoge Schnittstelle. • <i>bri<Schnittstellen-Index></i>: Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • <i><SIP-Konto></i>: Begrenzt den Eintrag auf das gewählte SIP-Konto. • <i>Beliebig</i>: Keine Begrenzung des Eintrags. <p>Geben Sie entweder Angerufene Leitung oder Angerufene Adresse ein.</p> <p>Wird ein Wert gewählt, der nicht <i>Beliebig</i> ist, so sollte Angerufene Adresse nicht benutzt werden. Ist Angerufene Leitung = <i>Beliebig</i> gesetzt und wird Angerufene Adresse nicht benutzt, so werden alle Anrufe für Angerufene Leitung behandelt.</p>
Angerufene Adresse	<p>Sie können optional die Zieladresse des Anrufs angeben.</p> <p>Geben Sie entweder Angerufene Leitung oder Angerufene Adresse ein. Wird Angerufene Adresse benutzt, so sollte Angerufene Leitung = <i>Beliebig</i> gesetzt sein.</p>
Transformation der rufen- den Adresse	<p>Geben Sie die Transformationsregel an, die auf die Rufnummer angewendet werden soll.</p> <p>Notation: <a:b>; d.h. a wird durch b ersetzt. Jede Regel muss durch einen Strichpunkt abgeschlossen werden. Mehrere Regeln können zu einer Regelkette zusammengefaßt werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>;. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert.</p> <p>? dient als Platzhalter für eine beliebige Ziffer.</p> <hr/> <p>Beispiel 16.2. Beispiel für eine Regel</p> <ul style="list-style-type: none"> • Regel: <:+49911>; • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

16.3.3 Rufnummertransformation

Hier können Sie eine Liste zum Umsetzen von Rufnummern erstellen, d.h. in dieser Liste werden externe und interne Nummern einander zugeordnet.




Hinweis

Welche Rufnummer (Called Party Number oder Calling Party Number) umgesetzt wird, hängt von der Richtung (eingehend oder ausgehend) des jeweiligen Rufs ab. Bei eingehenden Rufen wird die Called Party Number, bei ausgehenden Rufen die Calling Party Number umgesetzt.

Sie können z. B. die interne Rufnummer 340 nach außen als 09119673900 darstellen oder einen Ruf von außen, der an die Nummer 09119673200 gehen soll, intern an die Nummer 340 weiterleiten.

Im Menü **VoIP->Media Gateway->Rufnummertransformation** wird eine Liste vorhandenen Transformationen angezeigt.

16.3.3.1 Bearbeiten oder Neu

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

AnrufkontrolleCLID-UmwandlungRufnummertransformation

Basisparameter

Beschreibung	<input type="text"/>
Richtung	Beide ▾
Zugeordnete Leitung	bri-1 ▾
Lokale Adresse	<input type="text"/>
Externe Adresse	<input type="text"/>

OKAbbrechen

Abb. 138: **VoIP->Media Gateway->Rufnummertransformation ->  ->Neu**

Das Menü **VoIP->Media Gateway->Rufnummertransformation ->  ->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen der Rufnummertransformation ein.
Richtung	<p>Wählen Sie die Rufrichtung für den Eintrag.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Beide</i> (Standardwert): Für eingehende und ausgehende Rufe (bidirektional).• <i>Eingehend</i>: Für eingehende Rufe.• <i>Ausgehend</i>: Für ausgehende Rufe.
Zugeordnete Leitung	<p>Wählen Sie die ISDN-Leitung oder das SIP-Konto, über die bzw. über das Rufe geleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>fxs<Schnittstellen-Index></i>: Begrenzt den Ruf auf die gewählte analoge Schnittstelle.• <i>bri<Schnittstellen-Index></i>: Begrenzt den Ruf auf die gewählte BRI-Schnittstelle.• <i><SIP-Konto></i>: Begrenzt den Ruf auf das gewählte SIP-Konto.
Lokale Adresse	Geben Sie die interne Rufnummer (z. B. Nummer einer Nebenstelle oder TK-Anlage) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld Externe Adresse) auf die Lokale Adresse umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld Lokale Adresse) auf die Externe Adresse umgesetzt.

Feld	Beschreibung
	<p>Numerische und alphanumerische Zeichen sind zulässig.</p> <p>? dient als Platzhalter für eine beliebige Ziffer.</p> <p>Beachten Sie, dass Lokale Adresse und Externe Adresse dieselbe Anzahl von Wildcards enthalten müssen.</p>
Externe Adresse	<p>Geben Sie die externe Rufnummer (z. B. ISDN MSN oder die Rufnummer des SIP-Kontos) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld Externe Adresse) auf die Lokale Adresse umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld Lokale Adresse) auf die Externe Adresse umgesetzt.</p> <p>Das Feld Externe Adresse ist nicht sichtbar, wenn das Feld Zugeordnete Leitung = <i><SIP-Konto></i> gesetzt ist. Als Externe Adresse wird in diesem Fall wird der Benutzername des gewählten SIP-Kontos verwendet.</p>

16.4 RTSP

In diesem Menü konfigurieren Sie die Verwendung des Real-Time Streaming Protokolls (RTSP).

RTSP ist ein Netzwerkprotokoll zur Steuerung von Multimedia-Datenströmen in IP-basierten Netzwerken. Mittels RTSP werden keine Nutzdaten übertragen. Vielmehr wird damit eine Multimedia-Session zwischen Sender und Empfänger gesteuert.

Wenn Sie RTSP nutzen möchten, müssen Firewall und NAT entsprechend konfiguriert werden. Im Menü **VoIP->RTSP** können Sie den RTSP-Proxy aktivieren, um bei Bedarf angefragte RTSP-Sessions über den definierten Port zu ermöglichen.

16.4.1 RTSP-Proxy

Im Menü **VoIP->RTSP->RTSP-Proxy** konfigurieren Sie die Verwendung des Real-Time Streaming Protokolls.

RTSP-Proxy

Basisparameter	
RTSP-Proxy	<input type="checkbox"/> Aktiviert
RTSP-Port	<input style="width: 100px;" type="text" value="554"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 139: **VoIP->RTSP->RTSP-Proxy**

Das Menü **VoIP->RTSP->RTSP-Proxy** besteht aus den folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
RTSP-Proxy	<p>Wählen Sie aus, ob Sie RTSP-Sessions zulassen möchten.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
RTSP-Port	<p>Wählen Sie den Port aus, über den RTSP-Nachrichten ein- bzw. ausgehen sollen.</p> <p>Mögliche Werte sind 0 bis 65535.</p>

Feld	Beschreibung
	Der Standardwert ist 554.

Kapitel 17 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
- Realtime-Video/Audiokonferenzen (Messenger-Dienste, Universal Plug and Play)

17.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste->DNS->Globale Einstellungen->Basisparameter** werden die IP-Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der globalen Name-Server kann Ihr Gerät auch dynamisch via PPP oder DHCP erhalten bzw. diese ggf. übermitteln.

Strategie zur Namensauflösung auf Ihrem Gerät

Eine DNS-Anfrage wird von Ihrem Gerät folgendermaßen behandelt:

- (1) Falls möglich, wird die Anfrage aus dem statischen oder dynamischen Cache direkt mit IP-Adresse oder negativer Antwort beantwortet.
- (2) Ansonsten wird, falls ein passender Forwarding-Eintrag vorhanden ist, der entsprechende DNS-Server befragt, je nach Konfiguration von Internet- oder Einwahlverbindungen 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 Einwahlverbindung als Standard-Schnittstelle ausgewählt ist, die dazugehörigen DNS-Server befragt, je nach Konfiguration von Internet- oder Einwahl-

verbindungen 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.

17.1.1 Globale Einstellungen

Globale Einstellungen		DNS-Server	Statische Hosts	Domänenweiterleitung	Cache	Statistik
Basisparameter						
Domänenname	<input type="text"/>					
WINS-Server	Primär	<input type="text" value="0.0.0.0"/>				
	Sekundär	<input type="text" value="0.0.0.0"/>				
Erweiterte Einstellungen						
Positiver Cache	<input checked="" type="checkbox"/> Aktiviert					
Negativer Cache	<input checked="" type="checkbox"/> Aktiviert					
Cache-Größe	<input type="text" value="100"/>	Einträge				
Maximale TTL für positive Cacheeinträge	<input type="text" value="86400"/>	Sekunden				
Maximale TTL für negative Cacheeinträge	<input type="text" value="300"/>	Sekunden				
Alternative Schnittstelle, um DNS-Server zu erhalten	Automatisch ▼					
Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse						
Als DHCP-Server	<input type="radio"/> Keiner <input checked="" type="radio"/> Eigene IP-Adresse <input type="radio"/> DNS-Einstellung					
Als IPCP-Server	<input type="radio"/> Keiner <input type="radio"/> Eigene IP-Adresse <input checked="" type="radio"/> DNS-Einstellung					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>						

Abb. 140: Lokale Dienste->DNS->Globale Einstellungen

Das Menü **Lokale Dienste->DNS->Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard-Domain-Namen Ihres Geräts ein.
WINS-Server	Geben Sie die IP-Adresse des ersten und, falls erforderlich, des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.
Primär	
Sekundär	

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	<p>Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Negativer Cache	<p>Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Cache-Größe	<p>Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein.</p> <p>Wird dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird Cache-Größe vom Benutzer heruntergesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. Cache-Größe kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden.</p> <p>Mögliche Werte: 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.

Feld	Beschreibung
	<ul style="list-style-type: none">• <i>DNS-Einstellung</i>: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	<p>Wählen Sie aus, welche Name-Server-Adressen von Ihrem Gerät bei einer dynamischen Name-Server-Aushandlung übermittelt werden, wenn Ihr Gerät als IPCP-Server für PPP-Verbindungen genutzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Keiner</i>: Es wird keine Name-Server-Adresse übermittelt.• <i>Eigene IP-Adresse</i>: Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt.• <i>DNS-Einstellung</i> (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

17.1.2 DNS-Server

Im Menü **Lokale Dienste->DNS->DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

17.1.2.1 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.

Globale EinstellungenDNS-ServerStatische HostsDomänenweiterleitungCacheStatistik

Basisparameter

Admin-Status	<input checked="" type="checkbox"/> Aktiviert
Beschreibung	<input type="text"/>
Priorität	6 ▾
Schnittstellenmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> Dynamisch
Schnittstelle	Keine ▾
IP-Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6

OKAbbrechen

Abb. 141: Lokale Dienste->DNS->DNS-Server->Neu

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<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	<p>Geben Sie eine Beschreibung für den DNS-Server ein.</p>

Feld	Beschreibung
Priorität	<p>Weisen Sie dem DNS-Server eine Priorität zu.</p> <p>Sie können einer Schnittstelle (d.h. zum Beispiel einem Ethernet-Port oder einem PPPoE-WAN-Partner) mehrere Paare von DNS-Servern (Primärer DNS-Server und Sekundärer DNS-Server) zuweisen. Verwendet wird das Paar mit der höchsten Priorität, wenn die Schnittstelle im Zustand "up" ist.</p> <p>Mögliche Werte von <i>0</i> (höchste Priorität) bis <i>9</i> (niedrigste Priorität).</p> <p>Der Standardwert ist <i>5</i>.</p>
Schnittstellenmodus	<p>Wählen Sie aus, ob die IP-Adressen von Name-Servern für die Namensauflösung von Internet-Adressen automatisch bezogen oder ob abhängig von der Priorität bis zu zwei feste DNS-Server-Adressen eingetragen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> • <i>Dynamisch</i> (Standardwert)
Schnittstelle	<p>Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll.</p> <p>Bei Schnittstellenmodus = <i>Dynamisch</i></p> <p>Mit der Einstellung <i>Keine</i> wird ein globaler DNS-Server angelegt.</p> <p>Bei Schnittstellenmodus = <i>Statisch</i></p> <p>Mit der Einstellung <i>Beliebig</i> wird ein DNS-Server für alle Schnittstellen konfiguriert.</p>
IP-Version	<p>Wählen Sie die verwendete IP-Version aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IPv4</i> • <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>

17.1.3 Statische Hosts

Im Menü **Lokale Dienste->DNS->Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

17.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

Globale EinstellungenDNS-ServerStatische HostsDomänenweiterleitungCacheStatistik

Basisparameter

Standarddomäne

DNS-Hostname

Antwort

Positiv

IPv4-Adresse

0.0.0.0

Hinzufügen

IPv6-Adresse

Hinzufügen

OK

Abbrechen

Abb. 142: Lokale Dienste->DNS->Statische Hosts->Neu

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü BasisparameterStandarddomäne

Feld	Beschreibung
DNS-Hostname	<p>Geben Sie den Host-Namen ein, dem die in diesem Menü definierte IP-Adresse zugeordnet werden soll, wenn eine DNS-Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage negativ beantwortet wird, wird keine Adresse mitgeteilt.</p> <p>Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.bintec-elmeg.com.</p> <p>Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK "<Name.> " ergänzt.</p> <p>Einträge mit Leerzeichen sind nicht erlaubt.</p>
Antwort	<p>Wählen Sie die Art der Antwort auf DNS-Anfragen zu diesem Eintrag aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"><i>Negativ</i>: Eine DNS-Anfrage nach DNS-Hostname wird negativ beantwortet.<i>Positiv</i> (Standardwert): Eine DNS-Anfrage nach DNS-Hostname wird mit der dazugehörigen IP-Adresse beantwortet.<i>Keine</i>: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IPv4-Adresse	<p>Nur bei Antwort = Positiv</p> <p>Geben Sie die IPv4-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>

Feld	Beschreibung
IPv6-Adresse	Nur bei Antwort = <i>Positiv</i> Geben Sie die IPv6-Adresse ein, die nach DNS-Hostname zugeordnet wird.

17.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste->DNS->Domänenweiterleitung** wird eine Liste aller konfigurierter Weiterleitungen für definierte Domänen angezeigt.

17.1.4.1 Neu

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

Globale EinstellungenDNS-ServerStatische HostsDomänenweiterleitungCacheStatistik

Weiterleitungsparameter

Weiterleiten	<input checked="" type="radio"/> Host <input type="radio"/> Domäne
Host	<input type="text"/>
Weiterleiten an	<input checked="" type="radio"/> Schnittstelle <input type="radio"/> DNS-Server
Schnittstelle	Automatisch ▾

OKAbbrechen

Abb. 143: Lokale Dienste->DNS->Domänenweiterleitung ->Neu

Das Menü **Lokale Dienste->DNS->Domänenweiterleitung ->Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	Wählen Sie aus, ob Anfragen bezüglich eines Hosts oder einer Domäne weitergeleitet werden soll. Mögliche Werte: <ul style="list-style-type: none">• <i>Host</i> (Standardwert)• <i>Domäne</i>
Host	Nur für Weiterleiten = <i>Host</i> und Weiterleiten an = <i>DNS-Server</i> Geben Sie den Namen des Hosts ein, für den Anfragen weitergeleitet werden sollen. 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.
Domäne	Nur für Weiterleiten = <i>Domäne</i> und Weiterleiten an = <i>DNS-Server</i> Geben Sie den Namen der Domäne ein, für die Anfragen weitergeleitet werden sollen. Der Eintrag kann mit der Wildcard "*" beginnen, z. B. "*.mustermann.lan". Bei Eingabe eines Namens ohne führende Wildcard "*" wird nach Bestä-

Feld	Beschreibung
	tigung mit OK automatisch eine führende Wildcard "*" eingefügt.
Weiterleiten an	<p>Wählen Sie aus, ob zutreffende DNS-Anfragen an den DNS-Server einer Schnittstelle oder an einen manuell konfigurierten DNS-Server weitergeleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnittstelle</i> (Standardwert): Anfragen werden an den DNS-Server entweder einer automatisch gewählten oder einer manuell konfigurierten Schnittstelle weitergeleitet. • <i>DNS-Server</i>: Anfragen werden an den definierten DNS-Server weitergeleitet.
Schnittstelle	<p>Nur für Weiterleiten an = <i>Schnittstelle</i></p> <p>Wählen Sie die Schnittstelle aus, an deren DNS-Server Anfragen weitergeleitet werden sollen.</p>
IPv4-DNS-Server	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie IPv4-Adresse des primären und sekundären DNS-Servers ein.</p>
IPv6-DNS-Server	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie IPv6-Adresse des primären und sekundären DNS-Servers ein.</p>

17.1.5 Cache

Im Menü **Lokale Dienste->DNS->Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

Abb. 144: **Lokale Dienste->DNS->Cache**

Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** markieren.

Durch Markieren eines Eintrags und Bestätigen mit **Als statisch festlegen** wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet aus dieser Liste und wird in der Liste im Menü **Statische Hosts** angezeigt. Die TTL wird übernommen.

17.1.6 Statistik

Globale Einstellungen
DNS-Server
Statische Hosts
Domänenweiterleitung
Cache
Statistik

Automatisches Aktualisierungsintervall Sekunden

DNS-Statistiken	
Empfangene DNS-Pakete	2201
Ungültige DNS-Pakete	0
DNS-Anfragen	2201
Cache-Treffer	0
Weitergeleitete Anfragen	2201
Cache-Trefferrate (%)	0
Erfolgreich beantwortete Anfragen	0
Serverfehler	2201

Abb. 145: Lokale Dienste->DNS->Statistik

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der Cache-Treffer pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

17.2 HTTPS

Die Benutzeroberfläche Ihres Geräts können Sie von jedem PC aus mit einem aktuellen Web-Browser auch über eine HTTPS-Verbindung bedienen.

HTTPS (HyperText Transfer Protocol Secure) ist hierbei das Verfahren, um zwischen dem Browser, der zur Konfiguration verwendet wird, und dem Gerät eine verschlüsselte und authentifizierte Verbindung mittels SSL aufzubauen.

17.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

HTTPS-Server

HTTPS-Parameter

HTTPS-TCP-Port

443

Lokales Zertifikat

Intern ▾

Übernehmen

Abbrechen

Abb. 146: Lokale Dienste->HTTPS->HTTPS-Server

Das Menü **Lokale Dienste->HTTPS->HTTPS-Server** besteht aus folgenden Feldern:

Felder im Menü HTTPS-Parameter

Feld	Beschreibung
HTTPS-TCP-Port	<p>Geben Sie den Port ein, über den die HTTPS-Verbindung aufgebaut werden soll.</p> <p>Möglich sind Werte von 0 bis 65535.</p> <p>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">Intern (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möchten.<Zertifikatsname>: Wählen Sie ein unter Systemverwaltung->Zertifikate->Zertifikatsliste eingetragenes Zertifikat aus.

17.3 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.

17.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

17.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

DynDNS-Aktualisierung DynDNS-Provider

Basisparameter	
Hostname	<input type="text"/>
Schnittstelle	Eine auswählen ▼
Benutzername	<input type="text"/>
Passwort	<input type="password"/>
Provider	dyndns ▼
Aktualisierung aktivieren	<input type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Mail-Exchanger (MX)	<input type="text"/>
Wildcard	<input type="checkbox"/> Aktiviert
OK Abbrechen	

Abb. 147: Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Hostname	Geben Sie den vollständigen Hostnamen ein, wie er beim DynDNS-Provider registriert ist.
Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, deren IP-Adresse über den DynDNS-Service propagiert werden soll (z. B. die Schnittstelle des Internet Service Providers).
Benutzername	Geben Sie den Benutzernamen ein, wie er beim DynDNS-Provider registriert ist.
Passwort	Geben Sie das Passwort ein, wie es beim DynDNS-Provider registriert ist.
Provider	<p>Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind.</p> <p>Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden.</p> <p>Weitere DynDNS-Provider können im Menü Lokale 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 werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Mail-Exchanger (MX)	<p>Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll.</p> <p>Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.</p>
Wildcard	<p>Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von Hostname zur aktuellen IP-Adresse von Schnittstelle aktiviert werden soll (Erweiterte Namensauflösung).</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

17.3.2 DynDNS-Provider

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

17.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

DynDNS-Aktualisierung

DynDNS-Provider

Basisparameter

Providername

Server

Aktualisierungspfad

Port

80

Protokoll

DynDNS

Aktualisierungsintervall

300

Sekunden

OK

Abbrechen

Abb. 148: Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	<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	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll.

Feld	Beschreibung
	<p>Erfragen Sie den entsprechenden Port bei Ihrem Provider.</p> <p>Der Standardwert ist <i>80</i>.</p>
Protokoll	<p>Wählen Sie eines der implementierten Protokolle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DynDNS</i> (Standardwert) • <i>Static DynDNS</i> • <i>ODS</i> • <i>HN</i> • <i>DYNS</i> • <i>GnuDIP-HTML</i> • <i>GnuDIP-TCP</i> • <i>Custom DynDNS</i> • <i>DnsExit</i>
Aktualisierungsintervall	<p>Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf.</p> <p>Der Standardwert ist <i>300</i> Sekunden.</p>

17.4 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 288) finden Sie am Ende des Kapitels unter [DHCP - Konfigurationsbeispiel](#) auf Seite 288.

17.4.1 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.

17.4.1.1 Bearbeiten oder Neu

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

IP-Pool-Konfiguration

DHCP-Konfiguration

IP/MAC-Bindung

DHCP-Relay-Einstellungen

Basisparameter

IP-Poolname

IP-Adressbereich

-

DNS-Server

Primär

Sekundär

OK

Abbrechen

Abb. 149: Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll. Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.

17.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.


Im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration** wird eine Liste aller konfigurierter 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 192.168.2.100 bis 192.168.2.199 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

17.4.2.1 Bearbeiten oder Neu

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

IP-Pool-Konfiguration
DHCP-Konfiguration
IP/MAC-Bindung
DHCP-Relay-Einstellungen

Basisparameter	
Schnittstelle	<div style="border: 1px solid black; padding: 2px;">Eine auswählen ▼</div>
IP-Poolname	<div style="border: 1px solid black; padding: 2px;">Noch nicht definiert ▼</div>
Pool-Verwendung	<div style="border: 1px solid black; padding: 2px;">Lokal ▼</div>

Erweiterte Einstellungen:

Gateway	<div style="border: 1px solid black; padding: 2px;">Router als Gateway verwenden ▼</div>
Lease Time	<div style="border: 1px solid black; padding: 2px;">120 Minuten</div>
DHCP-Optionen	<div style="border: 1px solid black; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; flex: 1;">Option</div> <div style="border: 1px solid black; padding: 2px; flex: 1;">Wert</div> </div> <div style="text-align: center; margin-top: 5px;"> <div style="border: 1px solid black; padding: 2px 10px; display: inline-block;">Hinzufügen</div> </div> </div>

OK

Abbrechen

Abb. 150: Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die in IP-Adressbereich definierten Adressen an anfragende DHCP-Clients vergeben werden.</p> <p>Wenn eine DHCP-Anfrage über diese Schnittstelle eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.</p>
IP-Poolname	Wählen Sie einen im Menü Lokale Dienste->DHCP-Server->IP-Pool-Konfiguration konfigurierten IP-Poolnamen aus.
Pool-Verwendung	<p>Wählen Sie aus, ob der DHCP-Pool für Anfragen von DHCP-Clients in einem direkt an Schnittstelle angeschlossenen Ethernet verwendet werden soll oder für DHCP-Anfragen, die aus einem abgesetzt liegenden 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 Schnittstelle angeschlossenen Ethernet verwendet. <i>Relais</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus einem abgesetzt liegenden Ethernet verwendet. <i>Lokal/Relais</i>: Der DHCP-Pool kann für lokale und für weitergeleitete DHCP-Anfragen aus direkt angeschlossenen bzw. abgesetzt liegenden Ethernets verwendet werden.

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


Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Gateway	<p>Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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-Domänenname</i>: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • <i>WINS/NBNS-Server</i>: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • <i>WINS/NBT Node Type</i>: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • <i>TFTP-Server</i>: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • <i>CAPWAP Controller</i>: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • <i>URL (Provisionierungsserver)</i>: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. <p>Verwenden Sie diese Option, um anfragenden IP1x0-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form <i>http://<IP-Adresse des Provisionierungsservers>/eq_prov</i> haben.</p> <ul style="list-style-type: none"> • <i>Herstellergruppe</i> (Vendor Specific Information): Mit dieser Option können Sie dem Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen übermitteln. • <i>Vendor String</i>: Mit dieser Option können die Konfigurationsparameter (z. B. PIN und Access Point Name (APN) der SIM-Karte) übertragen werden. <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche Hinzufügen ein.</p>

Herstellergruppe

Im Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Konfiguration** -> **Erweiterte Einstellungen** können Sie einen Eintrag im Feld **DHCP-Optionen** bearbeiten, wenn **Option** = *Herstellergruppe* gewählt ist.


Wählen Sie das Symbol , um einen vorhandenen Eintrag zu bearbeiten. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server zum Beispiel für bestimmte Telefone.

Felder im Menü Basisparameter

Feld	Beschreibung
Hersteller auswählen	<p>Sie können hier auswählen, für welchen Hersteller spezifische Werte für den DHCP-Server übermittelt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Siemens</i> (Standardwert) • <i>Sonstige</i>
Provisioning-Server	<p>Nur für Hersteller auswählen = <i>Siemens</i></p> <p>Geben Sie ein, welcher herstellerspezifische Wert übermittelt werden soll.</p> <p>Für die Einstellung Hersteller auswählen = <i>Siemens</i> wird der Standardwert <i>sdlp</i> angezeigt.</p> <p>Sie können die IP-Adresse des gewünschten Servers ergänzen.</p>
Herstellerbeschreibung	<p>Nur für Hersteller auswählen = <i>Sonstige</i></p> <p>Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.</p>
Benutzerdefinierte DHCP-Optionen	<p>Nur für Hersteller auswählen = <i>Sonstige</i></p> <p>Fügen Sie mit Hinzufügen weitere Einträge hinzu.</p> <p>Sie können DHCP-Optionen hinzufügen.</p>

Vendor String

Gehen Sie im Menü **Lokale Dienste->DHCP-Server->DHCP-Konfiguration->Erweiterte Einstellungen** folgendermaßen vor, um die entsprechenden Parameter einzugeben:

Klicken Sie im Feld **DHCP-Optionen** auf die Schaltfläche **Hinzufügen** und wählen Sie **Option** = *Vendor String*. Klicken Sie auf die Schaltfläche , um den Eintrag zu bearbeiten.

Felder im Menü Basisparameter

Feld	Beschreibung
Hersteller auswählen	<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	<p>Nur für Hersteller auswählen = <i>-bintec-</i></p> <p>Geben Sie den Access Point Namen (APN) der SIM-Karte ein.</p>
PIN	<p>Nur für Hersteller auswählen = <i>-bintec-</i></p> <p>Geben Sie die PIN der SIM-Karte ein.</p>
Herstellerbeschreibung	<p>Nur für Hersteller auswählen = <i>Sonstige</i></p> <p>Geben Sie den Namen des Herstellers ein, für den Sie spezifische Werte für den DHCP-Server übermitteln wollen.</p>

Feld	Beschreibung
Vendor Option String	Nur für Hersteller auswählen = <i>Sonstige</i> Geben Sie die Hersteller spezifischen Konfigurationsparameter ein.

17.4.3 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.

17.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

IP-Pool-Konfiguration

DHCP-Konfiguration

IP/MAC-Bindung

DHCP-Relay-Einstellungen

Basisparameter

Beschreibung	<input type="text"/>
IP-Adresse	<input type="text"/>
MAC-Adresse	<input type="text"/>

OK

Abbrechen

Abb. 151: Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu

Das Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Hosts ein, an dessen MAC-Adresse die IP-Adresse gebunden wird. Möglich ist eine Zeichenkette mit bis zu 256 Zeichen.
IP-Adresse	Geben Sie die IP-Adresse ein, die der in MAC-Adresse angegebenen MAC-Adresse zugewiesen werden soll.
MAC-Adresse	Geben Sie die MAC-Adresse ein, der die in IP-Adresse angegebene IP-Adresse zugewiesen werden soll.

17.4.4 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

Abb. 152: Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

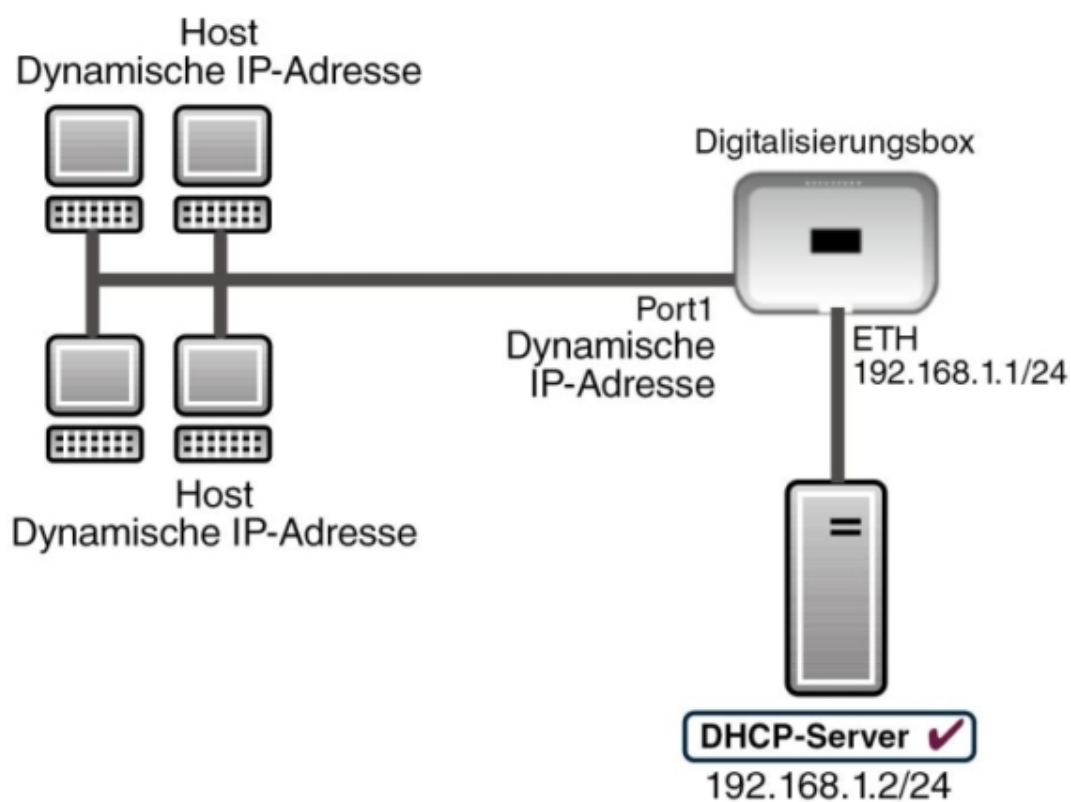
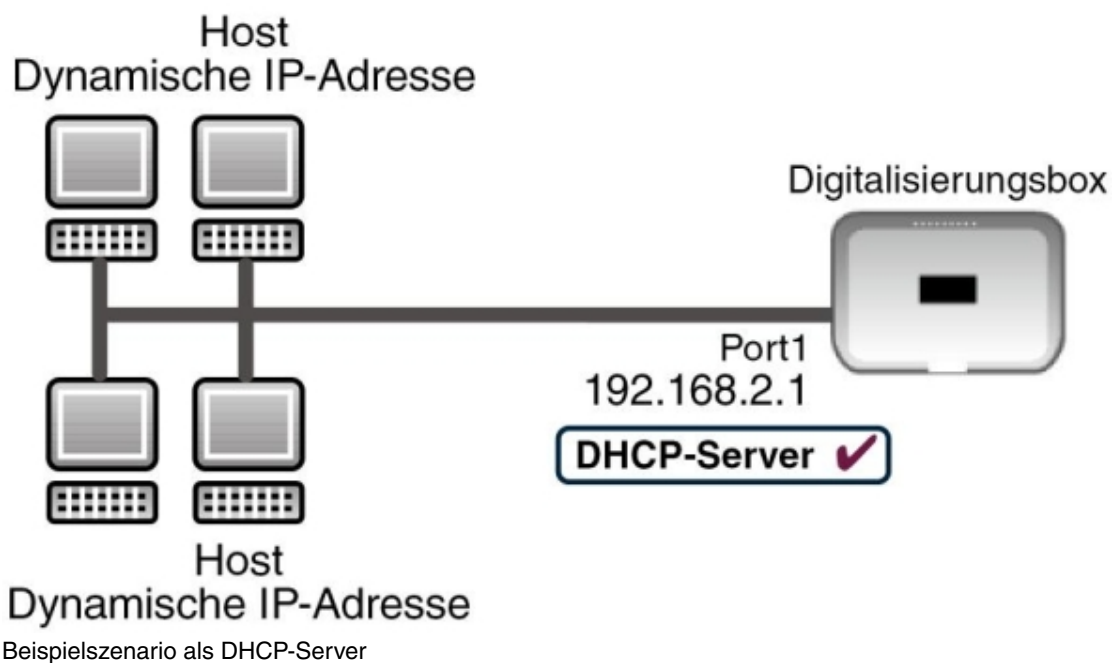
Feld	Beschreibung
Primärer DHCP-Server	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen. Der Standardwert ist 0.0.0.0.
Sekundärer DHCP-Server	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein. Der Standardwert ist 0.0.0.0.

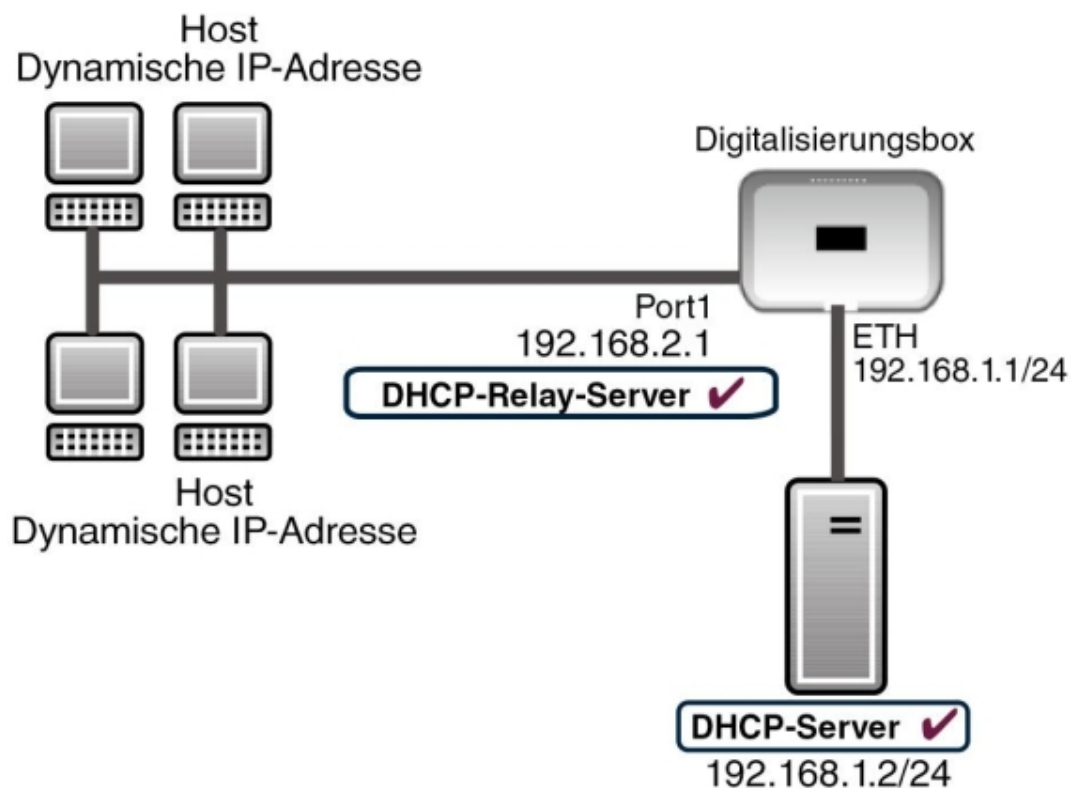
17.4.5 DHCP - Konfigurationsbeispiel

Voraussetzungen

- Optional ein DHCP-Server

Beispiel-Szenarien





Beispielszenario als DHCP-Relay-Server

Konfigurationsziel

Sie können Ihr Gerät als DHCP-Server, als DHCP-Client oder als DHCP-Relay-Server einsetzen.


Konfigurationsschritte im Überblick

DHCP-Server

Feld	Menü	Wert
IP-Poolname	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>IP-Pool-1</i>
IP-Adressbereich	Lokale Dienste -> DHCP-Server -> IP-Pool-Konfiguration -> Neu	z. B. <i>192.168.2.2</i> und <i>192.168.2.10</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 Pool -> 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: Als DHCP-Server	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. 192.168.1.2
Sekundärer DHCP-Server (optional)	Lokale Dienste -> DHCP-Server -> DHCP-Relay-Einstellungen	falls vorhanden

17.5 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 304.



Achtung

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der **Digitalisierungsbox**. 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.

17.5.1 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.

17.5.1.1 Neu

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

AuslöserAktionenOptionen

Basisparameter

Ereignisliste

Neu ▼

Beschreibung

Ereignistyp

Zeit ▼

Zeitintervall auswählen

Bedingungstyp

☐ Wochentag

☒ Perioden

☐ Tag des Monats

Bedingungseinstellungen

Montag ▼

Täglich ▼

1 ▼

Startzeit

Stunde

Minute

Stoppzeit

Stunde

Minute

OK

Abbrechen

Abb. 153: Lokale Dienste->Scheduling->Auslöser->Neu

Das Menü **Lokale Dienste->Scheduling->Auslöser->Neu** besteht aus folgenden Feldern:

Felder im Menü **Basisparameter**

Feld	Beschreibung
Ereignisliste	<p>Mit <i>Neu</i> (Standardwert) können Sie eine neue Ereignisliste anlegen. Mit Beschreibung geben Sie dieser Liste einen Namen. Mit Hilfe der übrigen Parameter legen Sie das erste Ereignis in der Liste an.</p> <p>Wenn Sie eine bestehende Ereignisliste erweitern wollen, wählen Sie die gewünschte Ereignisliste aus und fügen ihr mindestens ein Ereignis hinzu.</p> <p>Über Ereignislisten können auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden. Die Ereignisse werden in derseben 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 zugewiesene Aktionen werden zu bestimmten Zeitpunkten ausgelöst.• <i>MIB/SNMP</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen.• <i>Schnittstellenstatus</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierten Schnittstellen einen bestimmten Status annehmen.• <i>Schnittstellenverkehr</i>: Die in Aktionen konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn der Datenverkehr auf den angegebenen Schnittstellen den definierten Wert unter- oder überschreitet.• <i>Ping-Test</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist.• <i>Lebensdauer eines Zertifikats</i>: Die in Aktionen konfigurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierte

Feld	Beschreibung
	<p>Gültigkeitsdauer erreicht ist.</p> <ul style="list-style-type: none"> <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.
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> <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>

Feld	Beschreibung
	<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 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>
Versuche	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis Ziel-IP-Adresse als <i>Nicht erreichbar</i> gilt.</p> <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>
Verbleibende Gültigkeitsdauer	<p>Nur für Ereignistyp <i>Lebensdauer eines Zertifikats</i></p> <p>Geben Sie den gewünschten Wert für die noch verbleibende Gültigkeit des Zertifikats in Prozent ein.</p>

Feld	Beschreibung
Status der Funktionstaste	<p>Nur für Ereignistyp <i>Funktionstaste</i></p> <p>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.</p>

Felder im Menü Zeitintervall auswählen

Feld	Beschreibung
Zeitbedingung	<p>Nur für Ereignistyp <i>Zeit</i></p> <p>Wählen Sie zunächst die Art der Zeitangabe in Bedingungstyp aus.</p> <p>Mögliche Werte:</p> <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. <p>Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Wochentag</i>:</p> <p><i>Montag</i> (Standardwert) ... <i>Sonntag</i>.</p> <p>Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Perioden</i>:</p> <ul style="list-style-type: none"> • <i>Täglich</i>: Der Auslöser wird täglich aktiv (Standardwert). • <i>Montag-Freitag</i>: Der Auslöser wird täglich von Montag bis Freitag aktiv. • <i>Montag-Samstag</i>: Der Auslöser wird täglich von Montag bis Samstag aktiv. • <i>Samstag-Sonntag</i>: Der Auslöser wird Samstag und Sonntag aktiv. <p>Mögliche Werte für Bedingungseinstellungen bei Bedingungstyp = <i>Tag des Monats</i>:</p> <p><i>1... 31</i>.</p>
Startzeit	<p>Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.</p>
Stoppzeit	<p>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.</p>

17.5.2 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.

17.5.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Aktionen zu konfigurieren.

Auslöser
Aktionen
Optionen

Basisparameter	
Beschreibung	<input style="width: 90%;" type="text"/>
Befehlstyp	Neustart ▼
Ereignisliste	Eine auswählen ▼
Bedingung für Ereignisliste	Alle ▼
Neustart des Geräts nach	<input style="width: 40%;" type="text" value="60"/> Sekunden
OK Abbrechen	

Abb. 154: Lokale Dienste->Scheduling->Aktionen->Neu

Das Menü **Lokale Dienste->Scheduling->Aktionen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Bezeichnung für die Aktion ein.
Befehlstyp	<p>Wählen Sie die gewünschte Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Neustart</i> (Standardwert): Ihr Gerät wird neu gestartet. • <i>MIB/SNMP</i>: Für eine MIB-Variable wird der gewünschte Wert eingetragen. • <i>Schnittstellenstatus</i>: Der Status einer Schnittstelle wird verändert. • <i>WLAN-Status</i>: Nur für Geräte mit Wireless LAN. Der Status einer WLAN-SSID wird verändert. • <i>Softwareaktualisierung</i>: Es wird ein Software-Update initiiert. • <i>Konfigurationsmanagement</i>: Eine Konfigurationsdatei wird in Ihr Gerät geladen oder von Ihrem Gerät gesichert. • <i>Ping-Test</i>: Die Erreichbarkeit einer IP-Adresse wird überprüft. • <i>Zertifikatverwaltung</i>: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • <i>5 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt. • <i>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.

Feld	Beschreibung
Ereignisliste	Wählen Sie die gewünschte Ereignisliste aus, die in Lokale Dienste->Scheduling->Auslöser angelegt ist.
Bedingung für Ereignisliste	<p>Wählen Sie für die gewählte Ereignisliste aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten. • <i>Eins</i>: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt. • <i>Keiner</i>: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt. • <i>Eins nicht</i>: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.
Neustart des Geräts nach	<p>Nur bei Befehlstyp = <i>Neustart</i></p> <p>Geben Sie die Zeitspanne in Sekunden an, die nach dem Eintreten des Ereignisses gewartet werden soll, bis das Gerät neu gestartet wird.</p> <p>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>
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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Beide</i>: Der Wert der MIB-Variable wird unterschiedlich verändert, wenn der Status des Auslösers sich ändert.
MIB-Variablen	<p>Nur bei Befehlstyp = <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren Wert, abhängig vom Status des Auslösers, verändert werden soll.</p> <p>Ist der Auslöser aktiv (Status des Auslösers <i>Aktiv</i>), wird die MIB-Variable mit dem in Aktiver Wert eingetragenen Wert beschrieben.</p> <p>Ist der Auslöser inaktiv, Status des Auslösers <i>Inaktiv</i>), wird die MIB-Variable mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Soll die MIB-Variable verändert werden, je nachdem ob der Auslöser aktiv oder inaktiv ist (Status des Auslösers <i>Beide</i>), wird sie mit einem aktiven Auslöser mit dem in Aktiver Wert eingetragenen Wert und mit einem inaktiven Auslöser mit dem in Inaktiver Wert eingetragenen Wert beschrieben.</p> <p>Legen Sie weitere Einträge mit Hinzufügen an.</p>
Schnittstelle	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie die Schnittstelle aus, deren Status verändert werden soll.</p>
Schnittstellenstatus festlegen	<p>Nur bei Befehlstyp = <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, auf den die Schnittstelle gesetzt werden soll.</p> <p>Mögliche Werte:</p> <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 ge-

Feld	Beschreibung
	laden, den Sie über die <i>Server-URL</i> festlegen.
Server-URL	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i> wenn Quelle nicht <i>Aktuelle Software vom Update-Server</i></p> <p>Geben Sie die URL des Servers ein, von dem die gewünschte Softwareversion geholt werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> mit Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Konfigurationsdatei geholt oder auf den die Konfigurationsdatei gesichert werden soll.</p>
Dateiname	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i></p> <p>Geben Sie den Dateinamen der Softwareversion ein.</p> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> mit Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie den Dateinamen der Zertifikatsdatei ein.</p>
Aktion	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, welche Aktion auf eine Konfigurationsdatei angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Konfiguration importieren</i> (Standardwert) • <i>Konfiguration exportieren</i> • <i>Konfiguration umbenennen</i> • <i>Konfiguration löschen</i> • <i>Konfiguration kopieren</i> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i></p> <p>Wählen Sie aus, welche Aktion Sie auf eine Zertifikatsdatei anwenden möchten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zertifikat importieren</i> (Standardwert) • <i>Zertifikat löschen</i> • <i>SCEP</i>
Protokoll	<p>Nur für Befehlstyp = <i>Zertifikatverwaltung</i> und <i>Konfigurationsmanagement</i> wenn Aktion = <i>Konfiguration importieren</i></p> <p>Wählen Sie das Protokoll für die Dateiübertragung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>HTTP</i> (Standardwert) • <i>HTTPS</i> • <i>TFTP</i>
CSV-Dateiformat	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p>

Feld	Beschreibung
	<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> <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>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Nach Ausführung neu starten	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, ob Ihr Gerät nach der gewünschten Aktion neu gestartet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Versionsprüfung	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i></p> <p>Wählen Sie aus, ob beim Import einer Konfigurationsdatei überprüft werden soll, ob auf dem Server eine aktuellere Version der schon geladenen Konfiguration vorhanden ist. Wenn nicht, wird der Datei-Import abgebrochen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Ziel-IP-Adresse	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
Quell-IP-Adresse	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen. • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Intervall	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>Der Standardwert ist 1 Sekunde.</p>
Versuche	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis Ziel-IP-Adresse als unerreichbar gilt.</p> <p>Der Standardwert ist 3.</p>
Serveradresse	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.</p>
Lokale Zertifikatsbeschreibung	<p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie eine Beschreibung für das Zertifikat ein, unter der es im Gerät gespeichert werden soll.</p>

Feld	Beschreibung
	<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. <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 = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie einen Subjektnamen mit Attributen ein.</p> <p>Beispiel: <code>"CN=VPNServer, DC=mydomain, DC=com, c=DE"</code></p>
CA-Name	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Passwort	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Um Zertifikate zu erhalten, benötigen Sie möglicherweise ein Passwort von der Zertifizierungsstelle. Tragen Sie das Passwort, welches Sie von Ihrer Zertifizierungsstelle erhalten haben, hier ein.</p>
Schlüsselgröße	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Wählen Sie die Länge des zu erzeugenden Schlüssels aus. Mögliche Werte sind <i>1024</i> (Standardwert), <i>2048</i> und <i>4096</i>.</p>

Feld	Beschreibung
Autospeichermodus	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CRL verwenden	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats ausgestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Werte:</p> <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</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> befindet. Hierfür stehen alle Betriebsarten zur Auswahl, die von Ihrem Gerät unterstützt werden. Die Auswahl kann also von Gerät zu Gerät abweichen.</p>

17.5.3 Optionen

Im Menü **Lokale Dienste->Scheduling->Optionen** konfigurieren Sie das Schedule-Intervall.

Auslöser
Aktionen
Optionen

Scheduling-Optionen

Schedule-Intervall

☐ Aktiviert

OK
Abbrechen

Abb. 155: Lokale Dienste->Scheduling->Optionen

Das Menü **Lokale Dienste->Scheduling->Optionen** besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

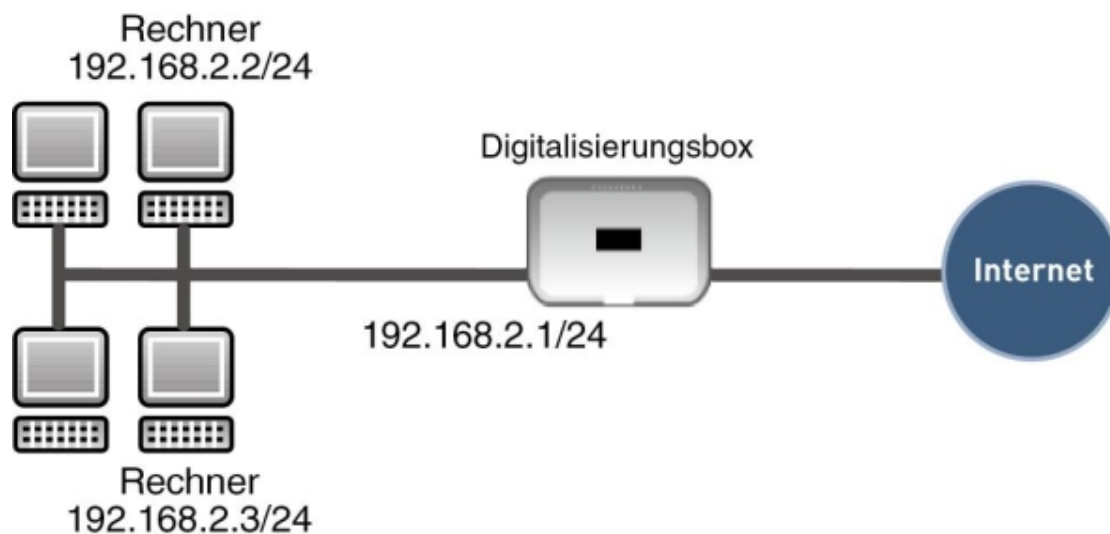
Feld	Beschreibung
Schedule-Intervall	<p>Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll.</p> <p>Standardmäßig ist das Schedule-Intervall nicht aktiv.</p> <p>Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind.</p> <p>Möglich sind Werte zwischen 0 und 65535.</p> <p>Empfohlen wird der Wert 300 (5 Minuten Genauigkeit).</p>

17.5.4 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	<i>Neu</i>
Beschreibung	Lokale Dienste -> Scheduling -> Auslöser -> Neu	<i>z. B. Neustart auslösen</i>
Ereignistyp	Lokale Dienste -> Scheduling -> Auslöser -> Neu	<i>Zeit</i>
Zeitbedingung	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Bedingungstyp = <i>Perioden</i> , Bedingungseinstellungen = <i>Täglich</i>
Startzeit	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Stunde <i>02</i> Minute <i>00</i>
Beschreibung	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>z. B. Neustart des Geräts</i>
Befehlstyp	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>Neustart</i>
Ereignisliste	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>Neustart auslösen</i>
Bedingung für Ereignisliste	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>Alle</i>
Neustart des Geräts nach	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>z. B. 60 Sekunden</i>
Schedule-Intervall	Lokale Dienste -> Scheduling -> Optionen	<i>Aktiviert, 55 sec</i>

WLAN-Schnittstelle abschalten

Feld	Menü	Wert
Ereignisliste	Lokale Dienste -> Scheduling -> Auslöser -> Neu	<i>Neu</i>
Beschreibung	Lokale Dienste -> Scheduling -> Auslöser -> Neu	<i>z. B. WLAN-Schnittstelle abschalten auslösen</i>
Ereignistyp	Lokale Dienste -> Scheduling -> Auslöser -> Neu	<i>Zeit</i>
Zeitbedingung	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Bedingungstyp = <i>Perioden</i> , Bedingungseinstellungen = <i>Samstag</i> <i>Sonntag</i>
Startzeit	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Stunde <i>00</i> Minute <i>00</i>
Stoppzeit	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Stunde <i>23</i> Minute <i>59</i>
Beschreibung	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>z. B. WLAN-Schnittstelle abschalten</i>
Befehlstyp	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>Schnittstellenstatus</i>
Ereignisliste	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>WLAN-Schnittstelle abschalten auslösen</i>
Bedingung für Ereignisliste	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>Alle</i>
Schnittstelle	Lokale Dienste -> Scheduling -> Aktionen -> Neu	<i>z. B. vss1-0</i>
Schnittstellenstatus festle-	Lokale Dienste -> Scheduling -> Aktionen	<i>Inaktiv</i>

Feld	Menü	Wert
gen	nen -> Neu	
Schedule-Intervall	Lokale Dienste -> Scheduling -> Optionen	Aktiviert, 55 sec

Konfiguration monatlich sichern

Feld	Menü	Wert
Ereignisliste	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Neu
Beschreibung	Lokale Dienste -> Scheduling -> Auslöser -> Neu	z. B. Konfigurationssicherung auslösen
Ereignistyp	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Zeit
Zeitbedingung	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Bedingungstyp = Tag des Monats, Bedingungseinstellungen = 1
Startzeit	Lokale Dienste -> Scheduling -> Auslöser -> Neu	Stunde 03 Minute 00
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. tftp://192.168.2.5
CSV-Dateiformat	Lokale Dienste -> Scheduling -> Aktionen -> Neu	Aktiviert
Dateiname auf Server	Lokale Dienste -> Scheduling -> Aktionen -> Neu	z. B. monthly-backup.cf
Dateiname in Flash	Lokale Dienste -> Scheduling -> Aktionen -> Neu	boot
Konfiguration enthält Zertifikate/Schlüssel	Lokale Dienste -> Scheduling -> Aktionen -> Neu	Aktiviert
Schedule-Intervall	Lokale Dienste -> Scheduling -> Optionen	Aktiviert, 55 sec

17.6 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.




Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

17.6.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

17.6.1.1 Bearbeiten oder Neu

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

HostsSchnittstellenPing-Generator

Hostparameter

Gruppen-ID

Neue ID ▼

Trigger

Überwachte IP-Adresse

Standard-Gateway ▼

Quell-IP-Adresse

Automatisch ▼

Intervall

10

Sekunden

Erfolgreiche Versuche

3

Fehlgeschlagene Versuche

3

Auszuführende Aktion

Aktion

Schnittstelle

Deaktivieren ▼

Eine auswählen ▼

Hinzufügen

OK

Abbrechen

Abb. 156: Lokale Dienste->Überwachung->Hosts->Neu

Das Menü **Lokale Dienste->Überwachung->Hosts->Neu** besteht aus folgenden Feldern:

Feld im Menü Hostparameter

Feld	Beschreibung
Gruppen-ID	<p>Wenn die Erreichbarkeit einer Gruppe von Hosts bzw. des Standard-Gateways von Ihrem Gerät überwacht werden soll, wählen Sie eine ID für die Gruppe bzw. für das Standard-Gateway.</p> <p>Die Gruppen-IDs werden automatisch von 0 bis 255 angelegt. Ist noch kein Eintrag angelegt, wird durch die Option <i>Neue ID</i> eine neue Gruppe angelegt. Sind Einträge vorhanden, kann man aus den angelegten Gruppen auswählen.</p> <p>Jeder zu überwachende Host muss einer Gruppe zugeordnet werden.</p> <p>Die in Schnittstelle konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied erreichbar ist.</p>

Felder im Menü Trigger


Feld	Beschreibung
Überwachte IP-Adresse	<p>Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.</p> <p>Mögliche Werte:</p> <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</p>

Feld	Beschreibung
	<p>als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse ein.
Intervall	<p>Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 10.</p> <p>Innerhalb einer Gruppe wird das kleinste Intervall der Gruppenmitglieder verwendet.</p>
Erfolgreiche Versuche	<p>Geben Sie ein, wieviele Pings beantwortet werden müssen, 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>Wählen Sie aus, welche Aktion ausgeführt werden soll. Für die meisten Aktionen wählen Sie eine Schnittstelle, auf die sich die Aktion bezieht.</p> <p>Auswählbar sind alle physikalischen und virtuellen Schnittstellen.</p> <p>Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (<i>Aktivieren</i>), deaktiviert (<i>Deaktivieren</i>, Standardwert) oder zurückgesetzt (<i>Zurücksetzen</i>) werden soll oder ob die Verbindung erneut aufgebaut (<i>Erneut wählen</i>) werden soll.</p> <p>Mit Aktion = <i>Überwachen</i> können Sie die IP-Adresse überwachen, die unter Überwachte IP-Adresse angegeben ist.</p>

17.6.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

17.6.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

Hosts

Schnittstellen

Ping-Generator

Basisparameter

Überwachte Schnittstelle

Eine auswählen ▾

Trigger

Schnittstelle wird aktiviert. ▾

Schnittstellenaktion

Aktivieren ▾

Schnittstelle

Eine auswählen ▾

OK

Abbrechen

Abb. 157: Lokale Dienste->Überwachung->Schnittstellen->Neu

Das Menü **Lokale Dienste->Überwachung->Schnittstellen->Neu** besteht aus folgenden Feldern:


Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstelle	Wählen Sie die Schnittstelle auf Ihrem Gerät aus, die überwacht werden soll.
Trigger	Wählen Sie den Status bzw. Statusübergang von Überwachte Schnittstelle aus, der eine bestimmte Schnittstellenaktion auslösen soll. Mögliche Werte: <ul style="list-style-type: none"><i>Schnittstelle wird aktiviert.</i> (Standardwert)<i>Schnittstelle wird deaktiviert.</i>
Schnittstellenaktion	Wählen Sie die Aktion aus, welche dem in Trigger definierten Status bzw. Statusübergang folgen soll. Die Aktion wird auf die in Schnittstelle ausgewählte(n) Schnittstelle(n) angewendet. Mögliche Werte: <ul style="list-style-type: none"><i>Aktivieren</i> (Standardwert): Aktivierung der Schnittstelle(n)<i>Deaktivieren</i>: Deaktivierung der Schnittstelle(n)
Schnittstelle	Wählen Sie aus, für welche Schnittstelle(n) die unter Schnittstelle festgelegte Aktion ausgeführt werden soll. Wählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle IPSec-Schnittstellen</i> .

17.6.3 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

17.6.3.1 Bearbeiten oder Neu

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

Hosts Schnittstellen **Ping-Generator**

Basisparameter	
Ziel-IP-Adresse	<input style="width: 90%;" type="text"/>
Quell-IP-Adresse	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Spezifisch ▼</div> <input style="width: 80%;" type="text"/> </div>
Intervall	<div style="display: flex; align-items: center;"> <input style="width: 40px; text-align: center;" type="text" value="10"/> <div style="margin-left: 10px;">Sekunden</div> </div>
Versuche	<input style="width: 40px; text-align: center;" type="text" value="3"/>
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> OK Abbrechen </div>	

Abb. 158: Lokale Dienste->Überwachung->Ping-Generator->Neu

Das Menü **Lokale Dienste->Überwachung->Ping-Generator->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	<p>Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein.</p> <p>Mögliche Werte:</p> <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	<p>Geben Sie das Intervall in Sekunden ein, während dessen der Ping an die in Entfernte IP-Adresse angegebene Adresse abgesetzt werden soll.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Der Standardwert ist 10.</p>
Versuche	<p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden sollen, bis die Ziel-IP-Adresse als <i>Nicht erreichbar</i> gilt.</p> <p>Der Standardwert ist 3.</p>

17.7 UPnP

Universal Plug and Play (UPnP) ermöglicht die Nutzung aktueller Messenger-Dienste (z. B. Realtime-Video/Audiokonferenzen) als Peer-to-Peer Kommunikation, wobei einer der Peers hinter einem Gateway mit aktiver NAT-Funktion liegt.

UPnP befähigt (meist) Windows-basierte Betriebssysteme, die Kontrolle über andere Geräte im lokalen Netzwerk mit UPnP Funktionalität zu übernehmen und diese zu steuern. Dazu zählen u.a. Gateways, Access Points und Printserver. Es sind keine speziellen Gerätetreiber notwendig, da gemeinsame und bekannte Protokolle genutzt werden wie TCP/IP, HTTP und XML.

Ihr Gateway ermöglicht die Nutzung des Subsystems des Internet Gateway Devices (IGD) aus dem UPnP-Funktionsspektrum.

In einem Netzwerk hinter einem Gateway mit aktiver NAT Funktion agieren die UPnP-konfigurierten Rechner als LAN UPnP Clients. Dazu muss die UPnP Funktion auf dem PC aktiviert sein.

Der auf dem Gateway voreingestellte Port, über den die UPnP-Kommunikation zwischen LAN UPnP Clients und dem Gateway läuft, ist 5678. Der LAN UPnP Client dient hierbei als sogenannter Service Control Point, d.h. er erkennt und kontrolliert die UPnP-Geräte im Netzwerk.

Die z. B. vom MSN Messenger dynamisch zugewiesenen Ports liegen im Bereich von 5004 bis 65535. Die Ports werden gatewayintern bei Anforderung freigegeben, d.h. beim Start einer Audio-/Videoübertragung im Messenger. Nach Beenden der Anwendung werden die Ports sofort wieder geschlossen.

Die Peer-to-Peer-Kommunikation wird über öffentliche SIP Server initiiert, wobei lediglich die Informationen beider Clients weitergereicht werden. Anschließend kommunizieren die Clients direkt miteinander.

Weitere Informationen zu UPnP erhalten Sie auf www.upnp.org.

17.7.1 Schnittstellen

In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Sie können festlegen, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle angenommen werden (für Anfragen aus dem lokalen Netzwerk) und/oder ob die Schnittstelle über UPnP-Anfragen kontrolliert werden kann.

SchnittstellenAllgemein

Ansicht20 pro Seite<<>>Filtern inKeiner gleichLos

Schnittstelle	Auf Client-Anfrage antworten	Schnittstelle ist UPnP-kontrolliert
en1-4	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert
efm35-60	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert
en1-0-1	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert
br0	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert
sta7-90	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert
ethoa35-5	<input type="checkbox"/> Aktiviert	<input type="checkbox"/> Aktiviert

Seite: 1, Objekte: 1 - 6

OKAbbrechen

Abb. 159: Lokale Dienste->UPnP->Schnittstellen

Das Menü **Lokale Dienste->UPnP->Schnittstellen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der Schnittstelle an, für welche die UPnP-Einstellungen vorgenommen werden. Der Eintrag kann nicht verändert werden.
Auf Client-Anfrage antworten	Legen Sie fest, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle (aus dem lokalen Netzwerk) beantwortet werden. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Schnittstelle ist UPnP-kontrolliert	Legen Sie fest, ob die NAT Konfiguration dieser Schnittstelle von UPnP kontrolliert wird. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.

17.7.2 Allgemein

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

SchnittstellenAllgemein

Basisparameter

UPnP-Status

☐ Aktiviert

UPnP TCP Port

5678

OK

Abbrechen

Abb. 160: Lokale Dienste->UPnP->Allgemein

Das Menü **Lokale Dienste->UPnP->Allgemein** besteht aus folgenden Feldern:

Felder im Menü Allgemein

Feld	Beschreibung
UPnP-Status	<p>Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv. Das Gateway nimmt die UPnP-Freigaben gemäß der in der Anfrage des LAN UPnP Clients beinhalteten Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.</p>
UPnP TCP Port	<p>Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>, der Standardwert ist <i>5678</i>.</p>

Kapitel 18 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.

18.1 Diagnose

Im Menü **Wartung->Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

18.1.1 Ping-Test

Ping-TestDNS-TestTraceroute-Test

Ping-Test

Test-Ping-Modus

☒ IPv4☐ IPv6

Ping-Befehl testweise an Adresse senden

Ausgabe

Los

Abb. 161: Wartung->Diagnose->Ping-Test

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind.

Felder im Menü Ping-Test

Feld	Beschreibung
Test-Ping-Modus	Wählen Sie die für den Ping-Test verwendete IP-Version. Mögliche Werte: <ul style="list-style-type: none">IPv4IPv6
Ping-Befehl testweise an Adresse senden	Geben Sie die zu testende IP-Adresse ein.
Zu verwendende Schnittstelle	Nur für Test-Ping-Modus = IPv6 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.

18.1.2 DNS-Test

Ping-TestDNS-TestTraceroute-Test

DNS-Test

DNS-Adresse

Ausgabe

Los

Abb. 162: Wartung->Diagnose->DNS-Test

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domänennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

18.1.3 Traceroute-Test

Ping-TestDNS-TestTraceroute-Test

Traceroute-Test

Traceroute-Modus

☒ IPv4 ☐ IPv6

Traceroute-Adresse

Ausgabe

Los

Abb. 163: Wartung->Diagnose->Traceroute-Test

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese erreichbar ist.

Felder im Menü Traceroute-Test

Feld	Beschreibung
Traceroute-Modus	<div>Wählen Sie die für den Traceroute-Test verwendete IP-Version.</div> <div>Mögliche Werte:</div> <div><ul style="list-style-type: none">IPv4IPv6</div>
Traceroute-Adresse	<div>Geben Sie die zu testende IP-Adresse ein.</div>

Durch Anklicken der **Los**-Schaltfläche wird der Traceroute-Test gestartet. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an.

18.2 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

18.2.1 Optionen

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Daher müssen Sie gegebenenfalls ein Software-Update durchführen.

Jede neue Systemsoftware beinhaltet neue Funktionen, bessere Leistung und bei Bedarf Fehlerkorrekturen der vorhergehenden Version. Die aktuelle Systemsoftware finden Sie unter www.bintec-elmeg.com. Hier finden Sie auch aktuelle Dokumentationen.



Wichtig

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörigen Release Notes. Hier sind alle Änderungen beschrieben, die mit der neuen Systemsoftware eingeführt werden.

Die Folge von unterbrochenen Update-Vorgängen (z. B. Stromausfall während des Updates) könnte sein, dass Ihr Gerät nicht mehr bootet. Schalten Sie Ihr Gerät nicht aus, während die Aktualisierung durchgeführt wird.

In seltenen Fällen ist zusätzlich eine Aktualisierung von BOOTmonitor und/oder Logic empfohlen. In diesem Fall wird ausdrücklich in den entsprechenden Release Notes darauf hingewiesen. Führen Sie bei BOOTmonitor oder Logic nur ein Update durch, wenn bintec elmeg GmbH eine explizite Empfehlung dazu ausspricht.

Flash

Ihr Gerät speichert seine Konfiguration in Konfigurationsdateien im Flash EEPROM (electrically erasable programmable read-only memory). Auch wenn Ihr Gerät ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

RAM

Im Arbeitsspeicher (RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf Ihrem Gerät einstellen. Der Inhalt des RAM geht verloren, wenn Ihr Gerät ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start Ihres Geräts beibehalten wollen, müssen Sie die geänderte Konfiguration im Flash speichern: Schaltfläche **Konfiguration speichern** über dem Navigationsbereich des **GUIs**. Dadurch wird die Konfiguration in eine Datei mit dem Namen *boot* im Flash gespeichert. Beim Starten Ihres Geräts wird standardmäßig die Konfigurationsdatei *boot* verwendet.

Aktionen

Die Dateien im Flash-Speicher können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen Ihrem Gerät und einem Host per HTTP zu transferieren.

Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außer-

dem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden. So können Sie mit den Aktionen "Konfiguration exportieren", "Konfiguration mit Statusinformationen exportieren" und "Konfiguration laden" Dateien sichern bzw. einspielen. Wenn Sie mit der Aktion "Konfiguration exportieren" oder "Konfiguration mit Statusinformationen exportieren" eine Konfigurationsdatei sichern wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll.



Achtung

Sollten Sie über die SNMP-Shell mit dem Kommando `put` eine Konfigurationsdatei in einem alten Format gesichert haben, kann ein Wiedereinspielen auf das Gerät nicht garantiert werden. Daher wird das alte Format nicht mehr empfohlen.

Optionen

Aktuell Installierte Software	
BOSS	V.10.1 Rev. 1 (Beta 9) IPv6, IPSec from 2014/11/25 00:00:00
Systemlogik	1.4
Optionen zu Software und Konfiguration	
Aktion	Keine Aktion ▼
<input type="button" value="Start"/>	

Abb. 164: Wartung->Software &Konfiguration ->Optionen

Das Menü **Wartung->Software &Konfiguration ->Optionen** besteht aus folgenden Feldern:

Felder im Menü Aktuell Installierte Software

Feld	Beschreibung
BOSS	Zeigt die aktuelle Softwareversion an, die auf Ihrem Gerät geladen ist.
Systemlogik	Zeigt die aktuelle Systemlogik an, die auf Ihrem Gerät geladen ist.
ADSL-Logik	Zeigt die aktuelle Version der ADSL-Logik an, die auf Ihrem Gerät geladen ist.

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	<p>Wählen Sie die Aktion aus, die Sie ausführen möchten.</p> <p>Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Keine Aktion</i> (Standardwert): <i>Konfiguration exportieren</i>: Die Konfigurationsdatei Aktueller Dateiname im Flash wird zu Ihrem lokalen Host transferiert. Wenn Sie die Los-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. <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.

Feld	Beschreibung
	<p>Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben!</p> <ul style="list-style-type: none"> • <i>Konfiguration kopieren</i>: Die Konfigurationsdatei im Feld Name der Quelldatei wird als Name der Zieldatei gespeichert. • <i>Konfiguration löschen</i>: Die Konfiguration im Feld Datei auswählen wird gelöscht. • <i>Konfiguration umbenennen</i>: Die Konfigurationsdatei im Feld Datei auswählen wird zu Neuer Dateiname umbenannt. • <i>Sicherung wiederherstellen</i>: Nur, wenn unter Konfiguration speichern mit der Einstellung <i>Konfiguration speichern und vorhergehende Boot-Konfiguration sichern</i> die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen. • <i>Software/Firmware löschen</i>: Die Datei im Feld Datei auswählen wird gelöscht. • <i>Sprache importieren</i>: Sie können weitere Sprachversionen des GUI auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von http://hilfe.telekom.de auf Ihren PC herunterladen und von dort aus in Ihr Gerät einspielen. • <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware, der ADSL-Logik und des BOOTmonitors initiieren. • <i>Voice Mail Wave-Dateien importieren</i>: Wählen Sie in Dateiname die Datei <i>vms_wavfiles.zip</i> aus, die Sie importieren wollen. • <i>Konfiguration mit Statusinformationen exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die Los-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.
Aktueller Dateiname im Flash	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.</p>
Zertifikate und Schlüssel einschließen	<p>Für Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Verschlüsselung der Konfiguration	<p>Nur für Aktion = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Passwort eingeben.</p>
Dateiname	<p>Nur für Aktion = <i>Konfiguration importieren, Sprache impor-</i></p>

Feld	Beschreibung
	<p><i>tieren, 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 oder 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>

18.3 Neustart

18.3.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **GUI** neu aufrufen und sich wieder anmelden.

Beobachten Sie dazu die LEDs an Ihrem Gerät. Für die Bedeutung der LEDs lesen Sie bitte in dem Handbuch-Kapitel **Technische Daten**.



Hinweis

Stellen Sie vor einem Neustart sicher, dass Sie Ihre Konfigurationsänderungen durch Klicken auf die Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.

Systemneustart

Möchten Sie das System jetzt wirklich neu starten?

Abb. 165: **Wartung->Neustart->Systemneustart**

Wenn Sie Ihr Gerät neu starten wollen, klicken Sie auf die **OK**-Schaltfläche. Der Neustart wird ausgeführt.

Kapitel 19 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.

19.1 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.

19.1.1 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.

19.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.

Syslog-Server

Basisparameter	
IP-Adresse	<input type="text"/>
Level	Information ▼
Facility	local0 ▼
Zeitstempel	<input checked="" type="radio"/> Keiner <input type="radio"/> Zeit <input type="radio"/> Datum & Uhrzeit
Protokoll	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Nachrichtentyp	<input type="radio"/> System <input type="radio"/> Accounting <input checked="" type="radio"/> System & Accounting
<div style="display: flex; justify-content: space-around;"> <div style="border: 1px solid black; padding: 5px 15px; border-radius: 5px;">OK</div> <div style="border: 1px solid black; padding: 5px 15px; border-radius: 5px;">Abbrechen</div> </div>	

Abb. 166: **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** -> **Neu**

Das Menü **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	<p>Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <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> <p><i>local0</i>.</p>
Zeitstempel	<p>Wählen Sie das Format des Zeitstempels im Systemprotokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Keine Systemzeitangabe. • <i>Zeit</i>: Systemzeit ohne Datum. • <i>Datum & Uhrzeit</i>: Systemzeit mit Datum.
Protokoll	<p>Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>UDP</i> (Standardwert) • <i>TCP</i>
Nachrichtentyp	<p>Wählen Sie den Nachrichtentyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System & Accounting</i> (Standardwert) • <i>System</i> • <i>Accounting</i>

19.2 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.

19.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

Nr.	Schnittstelle	IP-Accounting Alle auswählen Alle deaktivieren
1	en1-4	<input type="checkbox"/>
2	efm35-60	<input type="checkbox"/>
3	en1-0-1	<input type="checkbox"/>
4	br0	<input type="checkbox"/>
5	sta7-90	<input type="checkbox"/>
6	ethoa35-5	<input type="checkbox"/>

Abb. 167: Externe Berichterstellung->IP-Accounting->Schnittstellen

Im Menü **Externe Berichterstellung->IP-Accounting->Schnittstellen** wird eine Liste aller auf Ihrem Gerät konfigurierten Schnittstellen angezeigt. Für jeden Eintrag kann durch Setzen eines Hakens die Funktion IP-Accounting aktiviert werden. In der Spalte **IP-Accounting** müssen Sie nicht jeden Eintrag einzeln anklicken. Über die Optionen **Alle auswählen** oder **Alle deaktivieren** können Sie die Funktion IP-Accounting für alle Schnittstellen gleichzeitig aktivieren bzw. deaktivieren.

19.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

Abb. 168: Externe Berichterstellung->IP-Accounting->Optionen

Im Menü **Externe Berichterstellung->IP-Accounting->Optionen** können Sie das **Protokollformat** der IP-Accounting-Meldungen festlegen. Die Meldungen können Zeichenketten in beliebiger Reihenfolge, durch umgekehrten Schrägstrich abgetrennte Sequenzen, z. B. `\t` oder `\n` oder definierte Tags enthalten.

Mögliche Format-Tags:

Format-Tags für IP-Accounting Meldungen

Feld	Beschreibung
%d	Datum des Sitzungsbeginns im Format DD.MM.YY
%t	Uhrzeit des Sitzungsbeginns im Format HH:MM:SS
%a	Dauer der Sitzung in Sekunden
%c	Protokoll
%i	Quell-IP-Adresse
%r	Quellport
%f	Quell-Schnittstellen-Index
%l	Ziel-IP-Adresse
%R	Zielport
%F	Ziel-Schnittstellen-Index
%p	Ausgegangene Pakete
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen: *INET:*

```
%d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

19.3 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.

19.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

19.3.1.1 Neu

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

Benachrichtigungsempfänger
Benachrichtigungseinstellungen

Benachrichtigungsempfänger hinzufügen/bearbeiten	
Benachrichtigungsdienst	E-Mail
Empfänger	<input style="width: 90%;" type="text"/>
Nachrichtenkomprimierung	<input checked="" type="checkbox"/> Aktiviert
Betreff	<input style="width: 90%;" type="text"/>
Ereignis	Systemmeldung enthält Zeichenfolge ▼
Enthaltene Zeichenfolge	<input style="width: 90%;" type="text"/> (Wildcards zulässig)
Schweregrad	Notfall ▼
Überwachte Subsysteme	<div style="border: 1px solid black; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> Subsystem + </div> <div style="border: 1px solid black; height: 15px; margin-top: 2px;"></div> <div style="text-align: center; margin-top: 2px;">Hinzufügen</div> </div>
Timeout für Nachrichten	<input style="width: 50px;" type="text" value="60"/>
Anzahl Nachrichten	<input style="width: 50px;" type="text" value="1"/>
OK Abbrechen	

Abb. 169: Externe

Berichterstellung->Benachrichtigungsdienst->Benachrichtigungsempfänger->Neu

Das Menü Externe

Berichterstellung->Benachrichtigungsdienst->Benachrichtigungsempfänger->Neu besteht aus folgenden Feldern:

Felder im Menü Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Benachrichtigungsdienst	<p>Zeigt den Benachrichtigungsdienst an. Für Geräte mit UMTS können Sie den Benachrichtigungsdienst auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> E-Mail SMS
Empfänger	<p>Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.</p>
Nachrichtenkomprimierung	<p>Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse.</p> <p>Aktivieren oder deaktivieren Sie das Feld.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Betreff	<p>Sie können einen Betreff eingeben.</p>
Ereignis	<p>Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar.</p> <p>Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Systemmeldung enthält Zeichenfolge</i> (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. <i>Neuer Neighbor-AP gefunden</i>: Ein neuer benachbarter AP wurde gefunden. <i>Neuer Rogue-AP gefunden</i>: Ein neuer Rough AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein

Feld	Beschreibung
	<p>Bestandteil dieses Netzes ist.</p> <ul style="list-style-type: none"> • <i>Neuer Slave-AP (WTP) gefunden</i>: Eine neuer unkonfiguriertes AP hat sich beim WLAN Controller gemeldet. • <i>Verwalteter AP offline</i>: Ein managed AP ist nicht mehr erreichbar.
Enthaltene Zeichenfolge	<p>Sie müssen eine "Enthaltene Zeichenfolge" eingeben. Ihr Vorkommen in einer Syslog Meldung ist die notwendige Bedingung für das Auslösen eines Alarms.</p> <p>Die Eingabe ist auf 55 Zeichen begrenzt. Bedenken Sie, dass ohne die Verwendung von Wildcards (z. B. "**") nur diejenigen Strings die Bedingung erfüllen, die exakt der Eingabe entsprechen. In der Regel wird die eingegebene "Enthaltene Zeichenfolge" also Wildcards enthalten. Um grundsätzlich über alle Syslog-Meldungen des gewählten Levels informiert zu werden, geben Sie lediglich "*" ein.</p>
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>

19.3.2 Benachrichtigungseinstellungen

Benachrichtigungsempfänger
Benachrichtigungseinstellungen

Basisparameter	
Benachrichtigungsdienst	<input checked="" type="checkbox"/> Aktiviert
Maximale E-Mails pro Minute	6 ▼
E-Mail-Parameter	
E-Mail-Adresse des Senders	<input type="text"/>
SMTP-Server	<input type="text"/>
SMTP-Port	25 <input checked="" type="checkbox"/> SSL
SMTP-Authentifizierung	<input checked="" type="radio"/> Keiner <input type="radio"/> ESMTP <input type="radio"/> SMTP after POP
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 170: Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungseinstellungen

Das Menü **Externe Berichterstellung->Benachrichtigungsdienst->Benachrichtigungseinstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	<p>Wählen Sie aus, ob der Benachrichtigungsdienst aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Maximale E-Mails pro Minute	<p>Begrenzen Sie die Anzahl der ausgehenden Mails pro Minute. Zur Verfügung stehen Werte von 1 bis 15, der Standardwert ist 6.</p>

Felder im Menü E-Mail-Parameter

Feld	Beschreibung
E-Mail-Adresse des Senders	<p>Geben Sie die Mailadresse ein, die in das Absenderfeld der E-Mail eingetragen werden soll.</p>
SMTP-Server	<p>Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mail-servers 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 25 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.

Feld	Beschreibung
Benutzername	Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i> Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.
Passwort	Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i> Geben Sie das Passwort dieses Benutzers an.
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.

Kapitel 20 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.

20.1 Internes Protokoll

20.1.1 Systemmeldungen

Im Menü **Monitoring->Internes Protokoll->Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die konfigurierten Werte der Felder **Maximale Anzahl der Syslog-Protokolleinträge** und **Maximales Nachrichtenlevel von Systemprotokolleinträgen**. Diese Werte können im Menü **Systemverwaltung->Globale Einstellungen->System** verändert werden.

Systemmeldungen

Automatisches Aktualisierungsintervall 60 Sekunden Übernehmen

Maximale Anzahl der Syslog-Protokolleinträge 50

Maximales Nachrichtenlevel von Systemprotokolleinträgen Information

Ansicht 20 pro Seite << >> Filtern in Keiner gleich Los

Nr.	Datum	Zeit	Level	Subsystem	Nachricht
1	2000-03-13	05:59:17	Fehler	VoIP	IWU: @1: send request
2	2000-03-13	05:59:17	Fehler	VoIP	IWU: no route to remote registrar
3	2000-03-13	05:59:17	Fehler	VoIP	IWU: no transport found
4	2000-03-13	05:59:10	Fehler	VoIP	IWU: @test@test: send request
5	2000-03-13	05:59:10	Fehler	VoIP	IWU: no route to remote registrar
6	2000-03-13	05:59:10	Fehler	VoIP	IWU: no transport found
7	2000-03-13	05:59:07	Fehler	VoIP	IWU: @test@tsst: send request
8	2000-03-13	05:59:07	Fehler	VoIP	IWU: no route to remote registrar
9	2000-03-13	05:59:07	Fehler	VoIP	IWU: no transport found
10	2000-03-13	05:58:47	Fehler	VoIP	IWU: @1: send request
11	2000-03-13	05:58:47	Fehler	VoIP	IWU: no route to remote registrar
12	2000-03-13	05:58:47	Fehler	VoIP	IWU: no transport found
13	2000-03-13	05:58:40	Fehler	VoIP	IWU: @test@test: send request
14	2000-03-13	05:58:40	Fehler	VoIP	IWU: no route to remote registrar
15	2000-03-13	05:58:40	Fehler	VoIP	IWU: no transport found
16	2000-03-13	05:58:37	Fehler	VoIP	IWU: @test@tsst: send request
17	2000-03-13	05:58:37	Fehler	VoIP	IWU: no route to remote registrar
18	2000-03-13	05:58:37	Fehler	VoIP	IWU: no transport found
19	2000-03-13	05:58:17	Fehler	VoIP	IWU: @1: send request
20	2000-03-13	05:58:17	Fehler	VoIP	IWU: no route to remote registrar

Seite: 1, Objekte: 1 - 20, Summe der Objekte: 50

Abb. 171: Monitoring->Internes Protokoll->Systemmeldungen

Werte in der Liste Systemmeldungen

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der System-Meldung an.
Datum	Zeigt das Datum der Aufzeichnung an.
Zeit	Zeigt die Uhrzeit der Aufzeichnung an.
Level	Zeigt die hierarchische Einstufung der Meldung an.
Subsystem	Zeigt an, welches Subsystem Ihres Geräts die Meldung generiert hat.
Nachricht	Zeigt den Meldungstext an.

20.2 IPSec

20.2.1 IPSec-Tunnel

Im Menü **Monitoring->IPSec->IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel ange-
zeigt.

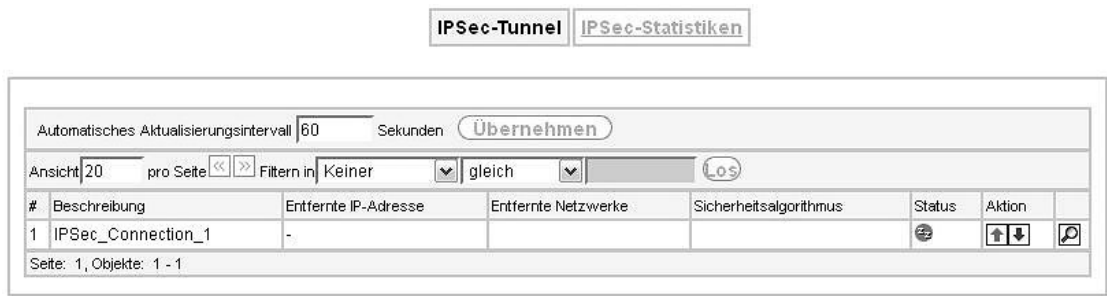


Abb. 172: **Monitoring->IPSec->IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

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

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

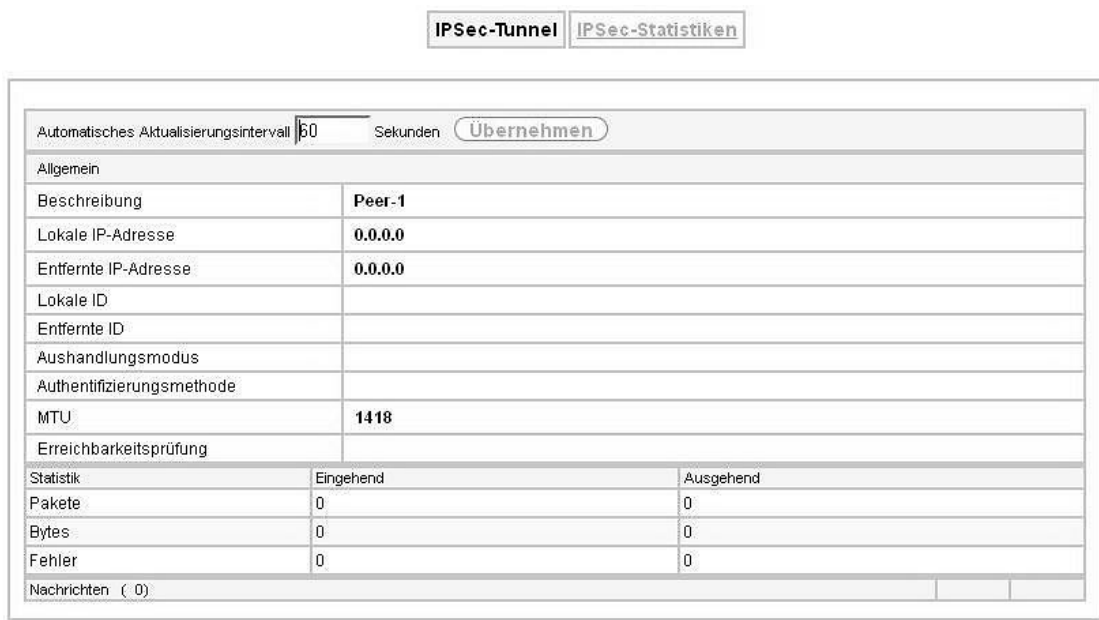


Abb. 173: **Monitoring->IPSec->IPSec-Tunnel->**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Peers an.
Lokale IP-Adresse	Zeigt die WAN-IP-Adresse Ihres Geräts an.
Entfernte IP-Adresse	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
Lokale ID	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
Entfernte ID	Zeigt die ID des Peers an.
Aushandlungsmodus	Zeigt den Aushandlungsmodus an.
Authentifizierungsmethode	Zeigt die Authentifizierungsmethode an.
MTU	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
Erreichbarkeitsprüfung	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
NAT-Erkennung	Zeigt die NAT-Erkennungsmethode an.
Lokaler Port	Zeigt den lokalen Port an.
Entfernter Port	Zeigt den entfernten Port an.
Pakete	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
Bytes	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
Fehler	Zeigt die Anzahl der Fehler an.
IKE (Phase-1) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IKE (Phase 1) SAs an.
IPSec (Phase-2) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

20.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

IPSec-Tunnel

IPSec-Statistiken

Automatisches Aktualisierungsintervall

300

Sekunden

Übernehmen

Lizenzen		In Verwendung		Maximal	
IPSec-Tunnel		0		2	
Peers	Aktiv	Aktivieren	Blockiert	Ruhend	Konfiguriert
Status	0	0	0	0	0
SAs			Hergestellt	Gesamt	
IKE (Phase-1)			0	0	
IPSec (Phase-2)			0	0	
Paketstatistiken			Eingehend	Ausgehend	
Gesamt			0	0	
Weitergeleitet			0	0	
Verworfen			0	0	
Verschlüsselt			0	0	
Fehler			0	0	

Abb. 174: Monitoring->IPSec->IPSec-Statistiken

Das Menü **Monitoring->IPSec->IPSec-Statistiken** besteht aus folgenden Feldern:

Feld im Menü Lizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (In Verwendung) und die Anzahl der maximal verwendbaren Lizenzen (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.

20.3 ISDN/Modem

20.3.1 Aktuelle Anrufe

Im Menü **Monitoring->ISDN/Modem->Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

Aktuelle Anrufe Anrufliste

Automatisches Aktualisierungsintervall 300 Sekunden
Übernehmen

Ansicht 20 pro Seite
<< >>
Filtern in Keiner
gleich
Los

#	Dienst	Entfernte Nummer	Schnittstelle	Richtung	Kosten	Dauer	Stack	Kanal	Status
Seite: 1									

Abb. 175: **Monitoring->ISDN/Modem->Aktuelle Anrufe**

Werte in der Liste Aktuelle Anrufe

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden ist: <i>PPP, IPsec, X.25, POTS</i> .
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: <i>Eingehend, Ausgehend</i> .
Kosten	Zeigt die Kosten der laufenden Verbindung an.
Dauer	Zeigt die Dauer der laufenden Verbindung an.
Stack	Zeigt den zugehörigen ISDN-Port (STACK) an.
Kanal	Zeigt die Nummer des ISDN-B-Kanals an.
Status	Zeigt den Status der Verbindung an: <i>null, c-initiated, ovl-send, oc-procd, c-deliverd, c-present, c-recvd, ic-procd, aktiv, discon-req, discon-ind, suspd-req, resum-req, ovl-recv</i> .

20.3.2 Anrufliste

Im Menü **Monitoring->ISDN/Modem->Anrufliste** wird eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) angezeigt.



Abb. 176: **Monitoring->ISDN/Modem->Anrufliste**

Werte in der Liste Anrufliste

Feld	Beschreibung
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden war: <i>PPP, IPsec, X.25, POTS</i> .
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: <i>Eingehend, Ausgehend</i> .
Kosten	Zeigt die Kosten der Verbindung an.
Startzeit	Zeigt die Uhrzeit an, zu welcher der Ruf aus- bzw. einging.
Dauer	Zeigt die Dauer der Verbindung an.

20.4 Schnittstellen

20.4.1 Statistik

Im Menü **Monitoring->Schnittstellen->Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. In der Anzeige **Transferdurchsatz** werden die Werte pro Sekunde angezeigt.

Statistik

Anzeigen: Gesamttransfer ▼ Automatisches Aktualisierungsintervall: 60 Sekunden Übernehmen												
Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los												
Nr.	Beschreibung	Typ	Tx-Pakete	Tx-Bytes	Tx-Fehler	Rx-Pakete	Rx-Bytes	Rx-Fehler	Status	Nicht geändert seit	Aktion	
1	en1-4	Ethernet	0	0	0	0	0	0	⬆	1d 21h 42m 40s	⬆ ⬇ 🔍	
2	efm35-60	Ethernet	0	0	0	0	0	0	⬆	1d 21h 42m 38s	⬆ ⬇ 🔍	
3	en1-0-1	VLAN	0	0	0	0	0	0	⬆	1d 0h 45m 10s	⬆ ⬇ 🔍	
4	br0	Ethernet	88.10K	21.65M	0	38.33K	7.95M	0	⬆	1d 0h 45m 10s	⬆ ⬇ 🔍	
5	en1-0	Ethernet	88.10K	23.59M	0	39.01K	8.70M	0	⬆	1d 0h 45m 10s	⬆ ⬇ 🔍	
6	sta7-90	802.11	0	0	0	0	0	0	⬆	1d 2h 49m 38s	⬆ ⬇ 🔍	
7	ethoa35-5	Ethernet	0	0	0	0	0	0	⬆	0d 4h 9m 48s	⬆ ⬇ 🔍	


Seite: 1, Objekte: 1 - 7

Abb. 177: Monitoring->Schnittstellen->Statistik

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

Werte in der Liste Statistik

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der Schnittstelle an.
Beschreibung	Zeigt den Namen der Schnittstelle an.
Typ	Zeigt den Schnittstellentyp an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Tx-Fehler	Zeigt die Gesamtzahl der gesendeten Fehler an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.
Rx-Fehler	Zeigt die Gesamtzahl der erhaltenen Fehler an.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Nicht geändert seit	Zeigt an, wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

Statistik

Anzeigen: Gesamttransfer ▼ Automatisches Aktualisierungsintervall: 60 Sekunden Übernehmen				
Beschreibung	en1-4			
MAC-Adresse	00:a0:f9:ff:a4:f6			
IP-Adresse / Netzmaske				
NAT	Nein			
Tx-Pakete	0			
Tx-Bytes	0			
Rx-Pakete	0			
Rx-Bytes	0			
TCP-Verbindungen				
Status	Lokale Adresse	Lokaler Port	Remote-Adresse	Entfernter Port

Abb. 178: Monitoring->Schnittstellen->Statistik-> 

Werte in der Liste Statistik

Feld	Beschreibung
Beschreibung	Zeigt den Namen der Schnittstelle an.
MAC-Adresse	Zeigt den Schnittstellentyp an.
IP-Adresse/Netzmaske	Zeigt die IP-Adresse und die Netzmaske an.
NAT	Zeigt an, ob NAT für diese Schnittstelle aktiviert ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Tx-Bytes	Zeigt die Gesamtzahl der gesendeten Oktetts an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Rx-Bytes	Zeigt die Gesamtzahl der erhaltenen Bytes an.

Feld im Menü TCP-Verbindungen

Feld	Beschreibung
Status	Zeigt den Status einer aktiven TCP-Verbindung an.
Lokale Adresse	Zeigt die lokale IP-Adresse der Schnittstelle für eine aktive TCP-Verbindung an.
Lokaler Port	Zeigt den lokalen Port der IP-Adresse für eine aktive TCP-Verbindung an.
Remote-Adresse	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

20.5 WLAN

20.5.1 WLAN1

Im Menü **Monitoring->WLAN->WLAN** werden die aktuellen Werte und Aktivitäten der WLAN-Schnittstelle angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1

YSS

Client-Verwaltung

Client Links

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden <input type="button" value="Übernehmen"/>		
WLAN1 Statistik		
Mbit/s	Tx-Pakete	Rx-Pakete
802.11a/b/g		
54	0	0
48	0	0
36	0	0
24	0	0
18	0	0
12	0	0
11	0	0
9	0	0
6	0	0
5	0	0
2	0	0
1	0	0
802.11n		
144,4	0	0
139	0	0
115,6	0	0
86,7	0	0
72,2	0	0
65	0	0
57,8	0	0
43,3	0	0
28,9	0	0
21,7	0	0
14,4	0	0
7,2	0	0
Gesamt	0	0
<input type="button" value="Erweitert"/>		

Abb. 179: Monitoring->WLAN->WLAN

Werte in der Liste WLAN

Feld	Beschreibung
Mbit/s	Zeigt die möglichen Datenraten auf diesem Funkmodul an.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete für die in Mbit/s angezeigte Datenrate an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete für die in Mbit/s angezeigte Datenrate an.

Über die Schaltfläche **Erweitert** gelangen Sie in eine Übersicht über weitere Details.

WLAN1

VSS

Client-Verwaltung

Client Links

Automatisches Aktualisierungsintervall Sekunden

Übernehmen

#	Beschreibung	Wert
1	Unicast MSDUs erfolgreich übertragen	0
2	Erfolgreich übertragene Multicast-MSDUs	0
3	Übertragene MPDUs	0
4	Erfolgreich empfangene Multicast-MSDUs	0
5	Unicast MPDUs erfolgreich erhalten	0
6	MSDUs, die nicht übertragen werden konnten	0
7	Doppelte empfangene MSDUs	0
8	CTS Frames als Antwort auf RTS empfangen	0
9	Nicht entschlüsselbare MPDUs erhalten	0
10	RTS Frames ohne CTS	0
11	Fehlerhafte Erhaltene Pakete	3093684

Zurück

Abb. 180: Monitoring->WLAN->WLAN->Erweitert

Werte in der Liste Erweitert

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des angezeigten Werts an.
Wert	Zeigt den entsprechenden statistischen Wert an.

Bedeutung der Listeneinträge

Beschreibung	Bedeutung
Unicast MSDUs erfolgreich übertragen	Zeigt die Anzahl der erfolgreich an Unicast-Adressen versandten MSDUs seit dem letzten Reset an. Zu jedem dieser Pakete wurde ein Acknowledgement empfangen.
Erfolgreich übertragene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich an Multicast-Adressen (inklusive der Broadcast MAC-Adresse) versandten MSDUs an.
Übertragene MPDUs	Zeigt die Anzahl der erfolgreich empfangenen MPDUs an.
Erfolgreich empfangene Multicast-MSDUs	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die mit einer Multicast-Adresse versandt wurden.
Unicast MPDUs 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.
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.

20.5.2 VSS

Im Menü **Monitoring->WLAN->VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.

WLAN1

VSS

Client-Verwaltung

Client Links

Automatisches Aktualisierungsintervall Sekunden

Übernehmen

Client-Node-Tabelle

MAC-Adresse	IP-Adresse	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s	Rx Discards	Tx Discards	
F55_intern (vss7-10)										
98:d6:f7:61:06:48	0.0.0.0	0 Tag(e) 0:0:6	2	6	-95(-96,-104,-109)	-109	2	0	0	

Abb. 181: Monitoring->WLAN->VSS

Werte in der Liste VSS

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	<p>Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an.</p> <p>Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s.</p> <p>Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.</p>
Rx Discards	Zeigt die Anzahl der empfangenen Datenpakete, die verworfen wurden, wenn im Menü Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)-> im Feld Rx Shaping die Bandbreite für eingehenden Datenverkehr begrenzt wurde.
Tx Discards	Zeigt die Anzahl der gesendeten Datenpakete, die verworfen wurden, wenn im Menü Wireless LAN->WLAN->Drahtlosnetzwerke (VSS)-> im Feld Rx Shaping die Bandbreite für ausgehenden Datenverkehr begrenzt wurde.

VSS - Details für Verbundene Clients

Im Menü **Monitoring->WLAN->VSS-><Verbundener Client>->** werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1

VSS

Client-Verwaltung

Client Links

Automatisches Aktualisierungsintervall

60

Sekunden

Übernehmen

Client-MAC-Adresse	IP-Adresse	Uptime	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	SNR dB	Datenrate Mbit/s	Rx Discards	Tx Discards
98:d6:f7:61:06:48	0.0.0.0	0 Tag(e) 0:0:23	-97(-97,-107,-109)	-109	12	1	0	0
Rate		Tx-Pakete			Rx-Pakete			
802.11a/b/g								
54		0			0			
48		0			0			
36		0			0			
24		0			0			
18		0			0			
12		0			0			
11		0			0			
9		0			0			
6		0			0			
5		0			0			
2		0			1			
1		2			8			
802.11n								
144,4		0			0			
139		0			0			
115,6		0			0			
86,7		0			0			
72,2		0			0			
65		0			0			
57,8		0			0			
43,3		0			0			
28,9		0			0			
21,7		0			0			
14,4		0			0			
7,2		0			0			
Gesamt		2			9			

Zurück

Abb. 182: Monitoring->WLAN->VSS-><Verbundener Client>->

Werte in der Liste <Verbundener Client>

Feld	Beschreibung
Client-MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen Indikator für die Qualität der Verbindung im Funk dar. Werte: <ul style="list-style-type: none">> 25 dB exzellent15 – 25 dB gut2 – 15 dB grenzwertig0 – 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.

Feld	Beschreibung
Rate	Zeigt die möglichen Datenraten auf dem Funkmodul an.
Rx Discards	Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.
Tx Discards	Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.

20.5.3 Client-Verwaltung

Im Menü **Monitoring->WLAN+Client-Verwaltung** wird eine Übersicht des **Client-Verwaltung** angezeigt. Sie sehen für jedes VSS u. a. die Anzahl der verbundenen Clients, die Anzahl der Clients, die in vom **2,4/5-GHz-Übergang** betroffen sind, sowie die Anzahl der abgewiesenen Clients.

WLAN1VSSClient-VerwaltungClient Links

Ansicht20 pro Seite<<>> Filtern inKeiner gleich Los

VSS-Beschreibung	Netzwerkname (SSID)	MAC-Adresse	Aktive Clients	2,4/5-GHz-Übergang	Abgewiesene Clients soft/hard	
vss7-10	default	00:a0:f9:ff:a4:fb	0	0	0 / 0	

Seite: 1, Objekte: 1 - 1

Abb. 183: Monitoring->WLAN+Client-Verwaltung

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.

20.6 Bridges

20.6.1 br<x>

Im Menü **Monitoring->Bridges-> br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

br0

Automatisches Aktualisierungsintervall600 Sekunden Übernehmen

MAC-AdressePort

Abb. 184: Monitoring->Bridges

Werte in der Liste br<x>

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adressen der assoziierten Bridges an.
Port	Zeigt den Port an, auf dem die Bridge aktiv ist.

20.7 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

20.7.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.



Abb. 185: **Monitoring->QoS->QoS**

Werte in der Liste QoS

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, für die QoS konfiguriert wurde.
QoS-Queue	Zeigt die QoS-Queue an, die für diese Schnittstelle konfiguriert wurde.
Senden	Zeigt die Anzahl der gesendeten Pakete mit der entsprechenden Paket-Klasse an.
Verworfen	Zeigt die Anzahl der verworfenen Pakete mit der entsprechenden Paket-Klasse bei Überlast an.
Queued	Zeigt die Anzahl der wartenden Pakete mit der entsprechenden Paket-Klasse bei Überlast an.

Index

- Administrativer Status 244 , 252 , 263 , 264
- Adressen 257
- Analoge Schnittstelle auswählen 247
- Angerufene Adresse 252
- Angerufene Adresse 263 , 265
- Angerufene Leitung 265
- Ankommende Rufnummer 211
- Anrufende Adresse 263
- Anrufende Leitung 263
- Ausgehende Rufnummer 211
- Ausgehender Proxy 252
- Authentifizierungs-ID 247 , 252
- Bandbreitenbegrenzung Downstream 257
- Bandbreitenbegrenzung Upstream 257
- Beinhalteter Standort (Parent) 257
- Benutzer 48
- Benutzer muss das Passwort ändern 48
- Benutzerdefinierte DHCP-Optionen 286
- Benutzername 252
- Beschreibung 45 , 244 , 247 , 252 , 257 , 259 , 263 , 265 , 267
- Codec-Reihenfolge 249 , 255
- Comfort Noise Generation (CNG) 250 , 256
- DSCP-Einstellungen für RTP-Daten 258
- Echounterdrückung 250 , 256
- Eigene IP-Adresse per ISDN/GSM übertragen 211
- Endpunktyp 246
- Entfernter Port 246
- Externe Adresse 267
- Externer Port 246
- Gültigkeit 247 , 252
- Herstellerbeschreibung 286 , 286
- Interne IP-Adresse 246
- Interner Port 246
- ISDN-Konfigurationstyp 61
- ISDN-Modus 259
- ISDN-Schnittstelle auswählen 247
- Konfiguration speichern 45
- Leitung 264
- Level Nr. 45
- Lizenzschlüssel 34
- Lizenzseriennummer 34
- Lokale Adresse 267
- Low Latency Transmission 244
- Maximale Downstream-Bandbreite 257
- Maximale Upstream-Bandbreite 257
- Menüs 46
- Metrik 129
- Mitglieder 259
- Modus 211
- Modus des D-Kanals 211
- Paketgröße 250 , 256
- Passwort 48 , 247 , 252
- Port 247
- Port-Verwendung 61
- Portname 61
- Priorität 264
- Protokoll 129 , 244 , 246 , 247 , 252
- Realm 252
- Registrar 252
- Registrierung 247 , 252
- Richtung 267
- Route 129
- Rufnummer 254 , 265
- Schnittstelle 129
- Schnittstellen 257
- Schnittstellentyp 247
- SIP-Endpunkt-IP-Adresse 247 , 252
- SIP-Header-Feld(er) für Anruferadresse 254
- Sortierreihenfolge 249 , 255
- Teilnehmer / Benutzername 247
- Timeout der Sitzung 244
- Transformation der gerufenen Adresse 264
- Transformation der rufenden Adresse 265
- Trunk-Modus 252
- Typ 257 , 263
- Übertragungsmodus 211
- X.31 (X.25 im D-Kanal) 61
- X.31 TEI-Dienst 61
- X.31 TEI-Wert 61
- Zugangs-Level 48
- Zugeordnete Leitung 267
- Aktuelle Ortszeit 32
- Anrufrkontrolle für lokale Nummern 260
- Datum einstellen 32
- Dauer 332 , 332
- Dienst 332 , 332
- Dritter Zeitserver 32
- Entfernte Nummer 332 , 332
- Erster Zeitserver 32
- Firewall auf Werkseinstellungen zurücksetzen 234
- Kanal 332
- Kontakt 28
- Kosten 332 , 332
- Kurzwahl 262
- LED-Modus 28
- Maximale Anzahl der Accounting-Protokolleinträge 28
- Maximale Anzahl der Syslog-Protokolleinträge 28
- Maximales Nachrichtenlevel von Systemprotokolleinträgen 28
- Media Stream Termination 260
- Passwörter und Schlüssel als Klartext anzeigen 31
- Richtung 332 , 332
- RTSP-Port 268
- RTSP-Proxy 268
- Schnittstelle 332 , 332
- Session Border Controller Modus 260
- SNMP Read Community 30
- SNMP Write Community 30
- Stack 332
- Standard-Abwurfnebenstelle 260
- Standardverhalten 257
- Standort 28
- Startzeit 332
- Status 332

- Status des Media Gateways 260
- System als Zeitserver 32
- Systemadministrator-Passwort 30
- Systemadministrator-Passwort bestätigen 30
- Systemname 28
- Wahlpause 260
- Zeit einstellen 32
- Zeitaktualisierungsintervall 32
- Zeitaktualisierungsrichtlinie 32
- Zeitzone 32
- Zweiter Zeitserver 32
- Aktive IPSec-Tunnel 27
- Aktive Sitzungen (SIF, RTP, etc...) 27
- Aktuelle Anrufe 331
- Anrufrkontrolle 262
- Anrufliste 332
- Arbeitsspeichernutzung 27
- Benutzer 46
- BOSS-Version 27
- CLID-Umwandlung 265
- CPU-Nutzung 27
- Datum 31
- DSP-Modul 28
- Interner Speicher 27
- ISDN Verwendung Intern 27
- ISDN-Konfiguration 60
- ISDN-Trunks 259
- Letzte gespeicherte Konfiguration 27
- Optionen 260
- Passwörter 30
- RTSP-Proxy 268
- Rufnummertransformation 266
- Seriennummer 27
- SIP-Endpunkte 245
- SIP-Konten 251
- SIP-Proxys 244
- Standorte 256
- Status Nachtbetrieb 27
- System 28
- Systemdatum 27
- Systemlizenzen 34
- Teilnehmer 247
- Uptime 27
- Zeit 31
- Zugriffsprofile 43
- Application Level Gateway 244
- Globale Einstellungen 28
- ISDN-Ports 60
- ISDN/Modem 331
- Konfigurationszugriff 43
- Media Gateway 262
- RTSP 268
- Status 26
- Assistenten 25
- Monitoring 328
- Physikalische Schnittstellen 58
- Schnittstellen 58
- Systemverwaltung 26
- VoIP 244
- Wartung 313
- DHCP-Client (Konfigurationsbeispiel) 288
- DHCP-Relay-Server (Konfigurationsbeispiel) 288
- DHCP-Server (Konfigurationsbeispiel) 288
- NAT (Konfigurationsbeispiel) 138
- SIF (Konfigurationsbeispiel) 241
- #
- #1 #2, #3 54
- 2
- 2,4/5-GHz-Übergang 339
- A**
- Abfrage Intervall 168
- Abgewiesene Clients soft/hard 339
- ACCESS_ACCEPT 38
- ACCESS_REJECT 38
- ACCESS_REQUEST 38
- ACCOUNTING_START 38
- ACCOUNTING_STOP 38
- Admin-Status 144
- Administrativer Status 200 , 273
- Administrativer Zugriff 37
- Adressbereich 236
- Adresse/Präfix 236
- Adresse/Subnetz 236
- Adressen 236
- Adressliste 236
- Adressmodus 67 , 190
- Adresstyp 236
- ADSL-Leitungsprofil 63
- ADSL-Logik 316
- Ähnliches Zertifikat überschreiben 296
- Airtime Fairness 81 , 104
- Aktion 120 , 135 , 163 , 229 , 232 , 296 , 316 , 329 , 333
- Aktionen 296
- Aktive Clients 339
- Aktive Clients 115
- Aktiver Allgemeiner Präfix 131
- Aktives Funkmodulprofil 101
- Aktualisierung aktivieren 280
- Aktualisierungsintervall 281
- Aktualisierungspfad 281
- Aktuelle Geschwindigkeit / Aktueller Modus 59
- Aktueller Dateiname im Flash 316
- Alle Multicast-Gruppen 171
- Allgemein 97 , 167 , 312
- Allgemeine IPv6-Präfixe 131
- Allgemeiner Name 54
- Allgemeiner Präfix 70
- Als DHCP-Server 272
- Als IPCP-Server 272
- Alternative Schnittstelle, um DNS-Server zu erhalten 271
- Andere Inaktivität 233
- Angegriffener Access Point 119
- Ankündigen 69
- Antwort 275

Antwortintervall (Letztes Mitglied) 168
 Anzahl Nachrichten 324
 Anzahl der Spatial Streams 79 , 103
 Anzahl erlaubter Verbindungen 207
 AP gefunden 113
 AP offline 113
 AP verwaltet 113
 APN 286
 ARP Processing 108
 Art der Einrichtung 70
 Art des Datenverkehrs 134
 Art des Angriffs 119
 Assistent für Netzwerkeinstellung 15
 ATM 187
 ATM PVC 183
 ATM-Dienstkategorie 192
 ATM-Schnittstelle 189
 Auf Client-Anfrage antworten 311
 Ausgehende Schnittstelle 156
 Ausgewählte Kanäle 82
 Ausgewählter Kanal 79
 Aushandlungsmodus 329
 Auslöser 291
 Ausstehende Ende-zu-Ende-Anforderungen 195
 Ausstehende Segment-Anforderungen 195
 Auswahl 237
 Auswahl des Client-Bands 87 , 110
 Auszuführende Aktion 307
 Authentifizierung 177 , 181 , 186
 Authentifizierung für PPP-Einwahl 43
 Authentifizierungsmethode 200 , 213 , 329
 Authentifizierungstyp 40
 Automatische Subnetzerstellung 70
 Automatische Konfiguration 12
 Autonomous Flag 71
 Autospeichermodus 55 , 296

B

Bandbreite 79 , 103
 Basierend auf Ethernet-Schnittstelle 66
 Beacon Period 89 , 105
 Bedienelemente 19
 Bedingung des Schnittstellenverkehrs 292
 Bedingung für Ereignisliste 296
 Befehlsmodus 296
 Befehlstyp 296
 Benachbarte APs 117
 Benachrichtigungsdienst 323 , 324 , 326
 Benachrichtigungseinstellungen 326
 Benachrichtigungsempfänger 323
 Benutzer 222
 Benutzerdefiniert 54
 Benutzerdefinierter Kanalplan 105
 Benutzername 174 , 179 , 183 , 280 , 326
 Benutzerzugang 16
 Benutzter Präfix/Länge 131
 Berichtsmethode 164
 Berücksichtigen 141
 Beschreibung 50 , 57 , 100 , 103 , 125 , 127 , 134 , 144 , 148 , 151 , 156 , 160 , 163 ,

174 , 179 , 183 , 189 , 200 , 206 , 213 , 218 , 222 , 235 , 235 , 236 , 237 , 238 , 240 , 273 , 287 , 292 , 296 , 329 , 329 , 333 , 334 , 336
 Beschreibung - Verbindungsinformation - Link 28
 Betreff 324
 Betreibermodus 40
 Betriebsmodus 79 , 101 , 103
 Betriebsmodus (Aktiv) 296
 Betriebsmodus (Inaktiv) 296
 Bevorzugte Gültigkeitsdauer 71
 Blockieren nach Verbindungsfehler für 177 , 181 , 186
 Blockzeit 216
 Bohrschablone 8
 BOSS 316
 Bridges 339
 Burst-Größe 156
 Burst-Mode 104
 Bytes 329

C

CA-Name 296
 CA-Zertifikat 52
 CA-Zertifikate 216
 Cache 277
 Cache-Größe 271
 Cache-Treffer 278
 Cache-Trefferrate (%) 278
 CAPWAP-Verschlüsselung 100
 Client-MAC-Adresse 338
 Client-Typ 191
 Client-Verwaltung 117 , 339
 Code 238
 Continuity Check (CC) Ende-zu-Ende 195
 Continuity Check (CC) Segment 195
 Controller-Konfiguration 97
 COS-Filter (802.1p/Layer 2) 148 , 160
 CPU-Last [%] 113
 CRL verwenden 296
 CRLs 56
 CRLs senden 226
 CSV-Dateiformat 296
 CTS Frames als Antwort auf RTS empfangen 336

D

Datei auswählen 316
 Dateikodierung 55 , 56
 Dateiname 296 , 316
 Dateiname auf Server 296
 Dateiname in Flash 296
 Datenrate Mbit/s 337 , 338
 Datum 328
 Details 329
 DH-Gruppe 213
 DHCP Broadcast Flag 72
 DHCP-Client 67 , 177 , 185
 DHCP-Hostname 72 , 190

- DHCP-Konfiguration 283
- DHCP-MAC-Adresse 72 , 190
- DHCP-Modus 72
- DHCP-Optionen 284
- DHCP-Relay-Einstellungen 288
- DHCP-Relay-Server 288
- DHCP-Server 67 , 97 , 282
- Diagnose 313
- Dienst 135 , 144 , 148 , 160 , 229 , 232
- Dienste 237
- Diensteliste 238
- Dienstkategorien 192
- DNS 270
- DNS-Anfragen 278
- DNS-Aushandlung 177 , 181 , 186
- DNS-Hostname 275
- DNS-Propagation 72
- DNS-Server 187 , 223 , 273 , 283
- DNS-Test 314
- Domäne 276
- Domänenname 271
- Domänenweiterleitung 276
- Doppelte empfangene MSDUs 336
- Downstream 62
- Drahtloser Modus 81 , 104
- Drahtlosnetzwerke (VSS) 83 , 107 , 116
- Dropping-Algorithmus 157
- DSCP / Traffic Class Filter (Layer 3) 148 , 160
- DSCP-/TOS-Wert 125
- DSCP/Traffic-Class-Filter setzen (Layer 3) 151
- DSL-Chipsatz 62
- DSL-Konfiguration 62
- DSL-Modem 62
- DSL-Modus 63
- DTIM Period 89 , 105
- Durchsatz 114 , 116
- Durchsatz/Client 115
- Dynamische RADIUS-Authentifizierung 225
- Dynamische Black List 111
- DynDNS-Aktualisierung 279
- DynDNS-Client 279
- DynDNS-Provider 281

E

- E-Mail 54
- E-Mail-Adresse 326
- EAP-Vorabauthentifizierung 86 , 109
- Einstellungen Funkmodul 78
- Eintrag aktiv 40
- Empfangene DNS-Pakete 278
- Empfänger 324
- Ende-zu-Ende-Sendeintervall 195
- Enkapsulierung 189
- Entfernte PPTP-IP-Adresse 181
- Entfernte IP-Adresse 329 , 329
- Entfernte Netzwerke 329
- Entfernte ID 329
- Entfernter Port 329 , 334
- Entferntes IPv6-Netzwerk 204

- Enthaltene Zeichenfolge 324
- Ereignis 324
- Ereignisliste 292 , 296
- Ereignistyp 292
- Erfolgreich empfangene Multicast-MSDUs 336
- Erfolgreich übertragene Multicast-MSDUs 336
- Erfolgreich beantwortete Anfragen 278
- Erfolgreiche Versuche 307
- Erlaubte Adressen 88 , 111
- Erreichbarkeitsprüfung 41 , 216 , 220 , 329
- Erweiterte Route 128
- Erzeugungsmethode 70
- Ethernet-Ports 58
- Ethernet-Schnittstellenauswahl 59
- Externe Berichterstellung 320
- Externer Dateiname 55 , 56

F

- Facility 321
- Fehler 120 , 329 , 331
- Fehlerhafte Erhaltene Pakete 336
- Fehlgeschlagene Versuche 307
- Fehlversuche per Zeitraum 111
- Fertig 120
- Filter 151
- Firewall 227
- Firmware-Wartung 120
- Fragmentation Threshold 82 , 105
- Frames ohne Tag verwerfen 76
- Frequenzband 79 , 103
- Funkmodul1 115
- Funkmodulprofile 102

G

- Gateway 128 , 284
- Gateway-Adresse 127
- Gateway-IP-Adresse 124
- Gerät 100
- Gesamt 331
- Gewichtung 156
- Globale Einstellungen 271
- Größe der Zero Cookies 225
- Größe des Protokoll-Headers unterhalb Layer 3 153
- Grundeinstellungen bei Auslieferung 5
- Grundkonfiguration 12
- Gruppen 237 , 239
- Gruppen-ID 307
- Gruppenbeschreibung 40 , 141 , 142
- Gültigkeitsdauer 71

H

- Hersteller auswählen 286 , 286
- High-Priority-Klasse 151
- Hinzuzufügende/zu bearbeitende MIB/
SNMP-Variable 296
- Host 276
- Hostname 280

Hosts 307
 HTTP 37
 HTTPS 37, 278
 HTTPS-Server 278
 HTTPS-TCP-Port 279

I

IGMP 167
 IGMP Proxy 169
 IGMP Snooping 89
 IGMP-Status 170
 IKE (Phase-1) 331
 IKE (Internet Key Exchange) 200
 IKE (Phase-1) SAs 329
 Image bereits vorhanden. 120
 Immer aktiv 174, 179, 183
 Importieren 55, 56
 Indexvariablen 292, 296
 Initial Contact Message senden 225
 Interner ISDN-Anschluss 8
 Internes Protokoll 328
 Internet + Einwählen 172
 Intervall 292, 296, 307, 310
 Intra-cell Repeating 85, 108
 IP Pools 186, 223
 IP-Accounting 322
 IP-Adressbereich 97, 187, 223, 283
 IP-Adresse 13, 190, 191, 287, 321, 337, 338
 IP-Adresse / Netzmaske 67
 IP-Adresse zur Nachverfolgung 142
 IP-Adresse/Netzmaske 334
 IP-Adressmodus 176, 180, 184
 IP-Komprimierung 220
 IP-Konfiguration 64
 IP-Pool-Konfiguration 282
 IP-Poolname 187, 223, 283, 284
 IP-Version 237, 273
 IP-Version des Tunnelnetzwerks 200
 IP-Zuordnungspool 202
 IP/MAC-Bindung 287
 IPSec 198, 328
 IPSec (Phase-2) 331
 IPSec aktivieren 224
 IPSec (Phase-2) SAs 329
 IPSec über TCP 225
 IPSec-Debug-Level 224
 IPSec-Peers 199
 IPSec-Statistiken 330
 IPSec-Tunnel 329, 331
 IPv4 236
 IPv4 Proxy ARP 208
 IPv4-Adresse 275
 IPv4-Adressvergabe 202
 IPv4-DNS-Server 276
 IPv4-Filterregeln 228
 IPv4-Gruppen 234
 IPv4-Quelladresse/-netzmaske 148, 160
 IPv4-Routing-Tabelle 128
 IPv4-Zieladresse/-netzmaske 148, 160
 IPv4/IPv6-Filter 148

IPv6 67, 177, 185, 236
 IPv6-Adresse 275
 IPv6-Adressen 67
 IPv6-DNS-Server 276
 IPv6-Modus 67, 177, 185
 IPv6-Quelladresse/-länge 148, 160
 IPv6-Routenkonfiguration 127
 IPv6-Routingtabelle 129
 IPv6-Zieladresse/-länge 148, 160
 ISDN-Login 37

K

Kanal 79, 101
 Kanalplan 82, 105
 Kennwort für geschütztes Zertifikat 296
 Key Hash Payloads senden 226
 Klassen-ID 151, 156
 Klassenplan 151
 Konfiguration 18
 Konfiguration verschlüsseln 296
 Konfiguration eines Allgemeinen Präfixes 131
 Konfiguration enthält Zertifikate/Schlüssel 296
 Konfiguration von IPv4-Routen 122
 Konfigurationsbeispiel - DHCP-Client 288
 Konfigurationsbeispiel - DHCP-Relay-Server 288
 Konfigurationsbeispiel - DHCP-Server 288
 Konfigurationsbeispiel - Lastverteilung 146
 Konfigurationsbeispiel - NAT 138
 Konfigurationsbeispiel - Scheduling 304
 Konfigurationsbeispiel - SIF 241
 Konfigurationsbeispiel - WLAN 90
 Konfigurationsbeispiel - Zeitgesteuerte Aufgaben 304
 Konfigurationsdaten sammeln 13
 Konfigurationsmodus 202
 Konfigurationsoberfläche aufrufen 19
 Konfigurationsschnittstelle 36
 Konfigurierte Geschwindigkeit/konfigurierter Modus 59
 Kontrollmodus 153, 197

L

LAN 64
 Land 54
 Lastverteilung 140
 Lastverteilung (Konfigurationsbeispiel) 146
 Lastverteilungsgruppen 140
 Layer 4-Protokoll 125
 LCP-Erreichbarkeitsprüfung 177, 181, 186
 LDAP-URL-Pfad 57
 Lease Time 284
 Lebensdauer 213, 218
 Level 321, 328
 Link-Präfix 70
 Lokale IP-Adresse 124, 176, 180, 184, 202
 Lokale PPTP-IP-Adresse 181

Lokale WLAN-SSID 296
 Lokale Zertifikatsbeschreibung 55, 56, 296
 Lokale Adresse 334
 Lokale IP-Adresse 329
 Lokale Dienste 270
 Lokale ID 200, 329
 Lokaler Dateiname 296
 Lokaler ID-Typ 200, 213
 Lokaler ID-Wert 213
 Lokaler Port 329, 334
 Lokales IPv6-Netzwerk 204
 Lokales Zertifikat 213
 Lokales Zertifikat 279
 Long Retry Limit 105
 Loopback Ende-zu-Ende 195
 Loopback aktiv 133
 Loopback-Segment 195
 Löschen 119, 128

M

MAC-Adresse 66, 190, 287, 334, 337, 339, 339
 MAC-Adresse des Rogue Clients 119
 Mail-Exchanger (MX) 281
 Max. Queue-Größe 157
 Max. Übertragungsrate 104
 Max. Anzahl Clients - Hard Limit 87, 110
 Max. Anzahl Clients - Soft Limit 87, 110
 Maximale Antwortzeit 168
 Maximale Anzahl der erneuten Einwählversuche 177, 181, 186
 Maximale Upload-Geschwindigkeit 153, 156, 197
 Maximale Gruppen 170
 Maximale Quellen 170
 Maximale Upstream-Bandbreite 63
 Maximale Anzahl der
 IGMP-Statusmeldungen 168
 Maximale Anzahl der
 IGMP-Statusmeldungen 170
 Maximale Burst-Größe (MBS) 192
 Maximale E-Mails pro Minute 326
 Maximale TTL für negative Cacheeinträge 271
 Maximale TTL für positive Cacheeinträge 271
 Mbit/s 335
 Metrik 124, 128, 202
 MIB-Variablen 296
 Min. Queue-Größe 157
 Mitglieder 235, 235, 240
 MobIKE 208
 Modus 52, 125, 130, 168, 170, 213, 222
 Modus / Bridge-Gruppe 36
 Monitoring 112
 MSDUs, die nicht übertragen werden konnten 336
 MTU 178, 329
 Multicast 166
 Multicast-Gruppen-Adresse 171
 Multicast-Routing 167

N

Nach Ausführung neu starten 296
 Nachricht 328
 Nachrichten 329
 Nachrichtenkomprimierung 324
 Nachrichtentyp 321
 Name 100, 131, 222
 Name der Quelldatei 316
 Name der Zieldatei 316
 NAT 132, 334
 NAT aktiv 133
 NAT-Eintrag erstellen 176, 180, 184
 NAT-Erkennung 329
 NAT-Konfiguration 133
 NAT-Methode 134
 NAT-Schnittstellen 132
 NAT-Traversal 216
 Negativer Cache 271
 Netzmaske 13, 128, 190, 191
 Netzwerk 122
 Netzwerkeinstellung 15
 Netzwerkname (SSID) 85, 108
 Netzwerkname (SSID) 339
 Neue Quell-IP-Adresse/Netzmaske 137
 Neue Ziel-IP-Adresse/Netzmaske 137
 Neuer Quell-Port 137
 Neuer Ziel-Port 137
 Neuer Dateiname 316
 Neustart 318
 Neustart des Geräts nach 296
 Nicht entschlüsselbare MPDUs erhalten 336
 Nicht geändert seit 333
 Nicht-Mitglieder verwerfen 76
 Nr. 130, 328, 333
 Nutzungsbereich 79

O

OAM-Fluss-Level 194
 OAM-Regelung 193
 Öffentliche IPv4-Quelladresse 208
 Öffentliche Schnittstelle 208
 Öffentlicher Schnittstellenmodus 208
 On Link Flag 71
 Optionen 43, 129, 170, 224, 232, 303, 315, 322
 Organisation 54
 Organisationseinheit 54
 Original Quell-Port/Bereich 135
 Original Ziel-IP-Adresse/Netzmaske 135
 Original Ziel-Port/Bereich 135
 Originale Quell-IP-Adresse/Netzmaske 135
 Ort 54

P

Pakete 329
 Passwort 52, 55, 56, 174, 179, 183, 222, 280, 296, 326
 Passwort ändern 14
 PC einrichten 14

Peak Cell Rate (PCR) 192
 Peer-Adresse 200
 Peer-ID 200
 PFS-Gruppe verwenden 218
 Phase-1-Profil 207
 Phase-1-Profile 212
 Phase-2-Profil 207
 Phase-2-Profile 218
 Physikalische Verbindung 62
 PIN 286
 Pin-Belegungen 9
 Ping 37
 Ping-Befehl testweise an Adresse senden 313
 Ping-Generator 309
 Ping-Test 313
 PMTU propagieren 220
 Pool-Verwendung 284
 POP3-Server 326
 POP3-Timeout 326
 Port 281, 339
 Portkonfiguration 58, 75
 Portweiterleitungen 133
 Positiver Cache 271
 PPPoA 182
 PPPoE 174
 PPPoE-Ethernet-Schnittstelle 174
 PPPoE-Modus 174
 PPPoE-Schnittstelle für Mehrfachlink 174
 PTP 179
 PTP-Adressmodus 181
 PTP-Ethernet-Schnittstelle 179
 PTP-Inaktivität 233
 PTP-Passthrough 133
 Preshared Key 86, 109, 200
 Primärer IPv4-DNS-Server 273
 Primärer IPv6-DNS-Server 273
 Primärer DHCP-Server 288
 Priorisierungsalgorithmus 153
 Priorität 40, 156, 273
 Priority Queueing 156
 Privaten Schlüssel generieren 52
 Profile 188
 Proposals 213, 218
 Protokoll 128, 135, 144, 148, 160, 206, 238, 281, 296, 321
 Protokollformat 323
 Protokollierte Aktionen 233
 Provider 189, 280
 Providername 281
 Provisioning-Server 286
 Proxy ARP 72
 Proxy-Schnittstelle 169
 PVID 76

Q

QoS 148, 340
 QoS-Klassifizierung 151
 QoS-Queue 340
 QoS-Schnittstellen/Richtlinien 153
 Quell-IP-Adresse 292, 296, 307, 310

Quell-IP-Adresse/Netzmaske 125, 135, 144, 206
 Quell-Port 125, 206
 Quell-Port/Bereich 135, 144, 148, 160
 Quelladresse/Länge 127
 Quelle 120, 229, 232, 296, 316
 Quellportbereich 238
 Quellschnittstelle 125, 144, 171
 Queued 340
 Queues/Richtlinien 153

R

RA-Signierungszertifikat 52
 RA-Verschlüsselungszertifikat 52
 RADIUS 38
 RADIUS-Dialout 41
 RADIUS-Passwort 40
 RADIUS-Server 109
 RADIUS-Server Gruppen-ID 222
 Rate 338
 Rauschen dBm 337, 338
 Real Time Jitter Control 153
 Real Time Jitter Control 196
 Regelkette 163, 164
 Regelketten 162
 Region 90, 97
 Regulierte Schnittstellen 197
 Remote Authentifizierung 38
 Remote-Adresse 334
 Reset 5
 Reset-Taster 8
 Richtlinie 41
 Richtlinien 228
 Richtung 151
 Richtung des Datenverkehrs 292
 Robustheit 168
 Rogue Clients 118
 Rogue APs 118
 Rolle 222
 Route aktiv 127
 Routen 122
 Routeneinträge 176, 180, 184, 202
 Routenklasse 123
 Routenselektor 142
 Routentyp 123, 127, 128
 Router Advertisement annehmen 67, 177, 185
 Router Advertisement übertragen 67
 Router-Gültigkeitsdauer 72
 Router-Präferenz 72
 RTS Threshold 82, 105
 RTS Frames ohne CTS 336
 RTT-Modus (Realtime-Traffic-Modus) 156
 Rx Shaping 88, 112
 Rx Discards 338
 Rx-Bytes 333, 334
 Rx-Fehler 333
 Rx-Pakete 333, 334, 335, 337

S

SAs mit dem Status der ISP-Schnittstelle syn-
 chronisieren 225
 SCEP-Server-URL 296
 SCEP-URL 52
 Schedule-Intervall 304
 Scheduling 291
 Scheduling (Konfigurationsbeispiel) 304
 Schlüsselgröße 296
 Schnittstelle 37, 38, 76, 97, 123, 128,
 130, 134, 142, 153, 164, 168, 197,
 273, 276, 280, 284, 296, 309, 311,
 340
 Schnittstelle ist UPnP-kontrolliert 311
 Schnittstelle - Verbindungsinformation - Link
 28
 Schnittstellen 36, 64, 151, 234, 308, 311
 , 322, 332
 Schnittstellenaktion 309
 Schnittstellenbeschreibung 36
 Schnittstellenmodus 66, 273
 Schnittstellenmodus / Bridge-Gruppen 35
 Schnittstellenstatus 292
 Schnittstellenstatus festlegen 296
 Schnittstellenzuweisung 164
 Schweregrad 324
 Segment-Sendeintervall 195
 Sekundärer IPv4-DNS-Server 273
 Sekundärer IPv6-DNS-Server 273
 Sekundärer DHCP-Server 288
 Sendeleistung 79, 101
 Senden 340
 Server 281
 Server Timeout 41
 Server-IP-Adresse 40
 Server-URL 296
 Serveradresse 296
 Serverfehler 278
 Setze COS Wert (802.1p/Layer 2) 151
 Short Guard Interval 82, 105
 Short Retry Limit 105
 Sicherheitsalgorithmus 329
 Sicherheitsmodus 86, 109
 Sicherheitsrichtlinie 67, 67, 176, 177, 180
 , 184, 185, 202, 204
 Signal 116
 Signal dBm 119, 337
 Signal dBm (RSSI1, RSSI2, RSSI3) 338
 Slave Access Points 99, 114
 Slave-AP-Konfiguration 99
 Slave-AP-LED-Modus 97
 Slave-AP-Standort 97
 SMTP-Authentifizierung 326
 SMTP-Port 326
 SMTP-Server 326
 SNR dB 338
 Software & Konfiguration 315
 Softwareaktualisierung 16
 Special Handling Timer 144
 Special Session Handling 143
 Speicherverbrauch [%] 113
 Sperrzeit für Black List 111
 SSID 119

Staat/Provinz 54
 Standard-Benutzerpasswort 40
 Standard-Ethernet für PPPoE-Schnittstellen
 190
 Standardeinstellungen wiederherstellen 37
 Standardroute 176, 180, 184, 202
 Standort 100
 Startmodus 207
 Startzeit 295
 Statische Adressen 70
 Statische Hosts 275
 Statische Black List 119
 Statistik 278, 332
 Status 292, 329, 331, 333, 334
 Status festlegen 296
 Status der Funktionstaste 292
 Status der IPv4-Firewall 233
 Status des Auslösers 296
 Stoppzeit 295
 Subjektnamen 296
 Subnetz-ID 70
 Subsystem 328
 Support 7
 Sustained Cell Rate (SCR) 192
 Switch-Port 59
 Syslog-Server 320
 System-Voraussetzungen 12
 Systemlogik 316
 Systemmeldungen 328
 Systemneustart 318
 Systempasswort ändern 14
 Systemprotokoll 320
 Systemsoftware 12

T

TCP-ACK-Pakete priorisieren 177, 181,
 186, 191
 TCP-Inaktivität 233
 TCP-MSS-Clamping 72
 Terminierung 8
 Test-Ping-Modus 313
 Timeout bei Inaktivität 174, 179, 183
 Timeout für Nachrichten 324
 Traceroute-Adresse 314
 Traceroute-Modus 314
 Traceroute-Test 314
 Traffic Shaping 153, 156
 Transmit Shaping 63
 Trigger 309
 Tx Shaping 88, 112
 Tx Discards 338
 Tx-Bytes 333, 334
 Tx-Fehler 333
 Tx-Pakete 333, 334, 335, 337
 Typ 131, 148, 160, 189, 238, 333

U

U-APSD 85
 Überbuchen zugelassen 156
 Überprüfung anhand einer Zertifikatsperrliste

- (CRL) 50
- Überprüfung der IPv4-Rückroute 208
- Überprüfung der Rückroute 130
- Übersicht 114
- Übertragene MPDUs 336
- Übertragener Datenverkehr 292
- Übertragungsschlüssel 86 , 109
- Überwachte IP-Adresse 307
- Überwachte Schnittstelle 292 , 309
- Überwachte Subsysteme 324
- Überwachte Variable 292
- Überwachtes Zertifikat 292
- Überwachung 306
- UDP-Inaktivität 233
- UDP-Port 41
- Umgebungs-Monitoring 117
- Ungültige DNS-Pakete 278
- Unicast MPDUs erfolgreich erhalten 336
- Unicast MSDUs erfolgreich übertragen 336
- Unveränderliche Parameter 145
- UPnP 310
- UPnP TCP Port 312
- UPnP-Status 312
- Upstream 62
- Uptime 337 , 338
- URL 120 , 316

V

- Vendor Option String 286
- Verbindungsstatus 148 , 160
- Verbleibende Gültigkeitsdauer 292
- Verbundene Clients 114
- Verbundene Clients/VSS 113
- Vergleichsbedingung 292
- Vergleichswert 292
- Vermeidung von Datenstau (RED) 157
- Verschlüsselt 331
- Verschlüsselung der Konfiguration 316
- Verschlüsselungsmethode 153
- Versionsprüfung 296
- Versuche 292 , 296 , 310
- Verteilungsmodus 141
- Verteilungsrichtlinie 141 , 142
- Verteilungsverhältnis 142
- Vertrauenswürdigkeit des Zertifikats erzwingen 50
- Verwaltung 76 , 89
- Verwaltungs-VID 76
- Verwendeter Kanal 101
- Verwerfen ohne Rückmeldung 164
- Verwerfen ohne Rückmeldung 133
- Verworfen 331 , 340
- Virtual Channel Identifier (VCI) 189
- Virtual Channel Connection (VCC) 192 , 194
- Virtual Path Connection (VPC) 194
- Virtual Path Identifier (VPI) 189
- VLAN 74 , 112 , 174
- VLAN Identifier 75
- VLAN aktivieren 76
- VLAN-ID 66 , 112 , 174
- VLAN-Mitglieder 75

- VLAN-Name 75
- VLANs 75
- Vollständige IPSec-Konfiguration löschen 224
- Vollständige IPv4-Filterung 233
- Von Schnittstelle 131
- Vorbereitungen 12
- VPN 198
- VSS 336
- VSS-Beschreibung 339

W

- WAN 172
- Wandmontage 8
- Wartung 119
- Weitergeleitet 331
- Weitergeleitete Anfragen 278
- Weiterleiten 171 , 276
- Weiterleiten an 276
- WEP-Schlüssel 1-4 86 , 109
- Wert 336
- Wiederholungen 41
- Wiederkehrender Hintergrund-Scan 105
- Wildcard 281
- WINS-Server 271
- Wird ausgeführt 120
- Wireless LAN 78
- Wireless LAN Controller 93
- Wizard 93
- WLAN 78 , 334
- WLAN Controller 113
- WLAN (Konfigurationsbeispiel) 90
- WLAN Controller: VSS-Durchsatz 113
- WLAN-Modul auswählen 296
- WLAN1 334
- WLC-SSID 296
- WMM 85 , 108
- WPA Cipher 86 , 109
- WPA-Modus 86 , 109
- WPA2 Cipher 86 , 109

X

- XAUTH-Profil 207
- XAUTH-Profile 221

Z

- Zeit 328
- Zeitbedingung 295
- Zeitgesteuerte Aufgaben (Konfigurationsbeispiel) 304
- Zeitstempel 321
- Zero Cookies verwenden 225
- Zertifikat in Konfiguration schreiben 296
- Zertifikat ist ein CA-Zertifikat 50
- Zertifikate 48
- Zertifikate und Schlüssel einschließen 316
- Zertifikatsanforderung 51
- Zertifikatsanforderungs-Payloads nicht beachten 226
- Zertifikatsanforderungs-Payloads senden

226
Zertifikatsanforderungsbeschreibung 52 ,
296
Zertifikatsketten senden 226
Zertifikatsliste 49
Zertifikatsserver 57
Ziel 229 , 232
Ziel-IP-Adresse 128 , 292 , 296 , 310
Ziel-IP-Adresse/Netzmaske 124 , 135 , 144 ,
206
Ziel-Port/Bereich 135 , 144 , 148 , 160
Zieladresse/Länge 127
Zielport 125 , 206
Zielportbereich 238
Zielschnittstelle 127 , 171
Zu verwendende Schnittstelle 313
Zuerst gesehen 119
Zugang über LAN 18
Zugewiesene Drahtlosnetzwerke (VSS) 101
Zugriffsfilter 159 , 163
Zugriffskontrolle 88 , 111
Zugriffsregeln 158
Zuletzt gesehen 119
Zusammenfassend 54
Zusätzlicher Filter des IPv4-Datenverkehrs
204 , 206