

Benutzerhandbuch bintec WLAN und Industrial WLAN

Referenz

Copyright© Version 14.0, 2013 Teldat GmbH

Rechtlicher Hinweis

Ziel und Zweck

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

Haftung

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

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Release Notes für Teldat-Gateways finden Sie unter www.teldat.de.

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

Marken

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

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

Copyright

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

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter www.teldat.de.

Wie Sie Teldat GmbH erreichen

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

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

Internet: www.teldat.de

Inhaltsverzeichnis

Kapitel 1	Einleitung	1
Kapitel 2	Zum Handbuch	3
Kapitel 3	Inbetriebnahme	6
3.1	bintec W1003n, W2003n, W2003n-ext und W2004n	6
3.1.1	Aufstellen und Anschließen	6
3.1.2	Anschlüsse	9
3.1.3	LEDs	10
3.1.4	Lieferumfang	11
3.1.5	Allgemeine Produktmerkmale	12
3.1.6	Reset	13
3.2	bintec W1002n	14
3.2.1	Aufstellen und Anschließen	14
3.2.2	Anschlüsse	17
3.2.3	Antennenanschlüsse	18
3.2.4	LEDs	18
3.2.5	Lieferumfang	19
3.2.6	Allgemeine Produktmerkmale	19
3.2.7	Reset	21
3.3	bintec WI1040n und WI2040n	22
3.3.1	Aufstellen und Anschließen	22
3.3.2	Anschlüsse	25
3.3.3	Antennenanschlüsse	26
3.3.4	LEDs	26
3.3.5	Lieferumfang	28
3.3.6	Allgemeine Produktmerkmale	30
3.3.7	Reset	31

3.4	bintec WI1065n und WI2065n	33
3.4.1	Aufstellen und Anschließen	33
3.4.2	Anschlüsse	36
3.4.3	Antennenanschlüsse	37
3.4.4	LEDs	38
3.4.5	Lieferumfang	39
3.4.6	Allgemeine Produktmerkmale	41
3.4.7	Reset	42
3.5	Reinigen.	43
3.6	Pin-Belegung	43
3.6.1	Ethernet-Schnittstelle	43
3.6.2	Serielle Schnittstelle	45
3.6.3	Buchse für die Stromversorgung	46
3.7	Frequenzen und Kanäle	46
3.8	Support Information	46
3.9	WEEE-Information	47
Kapitel 4	Grundkonfiguration	48
4.1	Voreinstellungen	48
4.1.1	Vorkonfigurierte Daten	48
4.1.2	Software-Update	49
4.2	System-Voraussetzungen	50
4.3	Vorbereitung	50
4.3.1	Daten sammeln	50
4.3.2	PC einrichten	52
4.4	IP-Konfiguration	53
4.5	Systempasswort ändern	56
4.6	Drahtlosnetzwerk einrichten	57

4.7	Bridge Link einrichten	58
4.8	Softwareaktualisierung	59
Kapitel 5	Zugang und Konfiguration	61
5.1	Zugangsmöglichkeiten	61
5.1.1	Zugang über LAN.	61
5.1.2	Zugang über die serielle Schnittstelle	65
5.2	Anmelden	66
5.2.1	Benutzernamen und Passwörter im Auslieferungszustand	66
5.2.2	Anmelden zur Konfiguration	67
5.3	Konfigurationsmöglichkeiten	68
5.3.1	GUI (Graphical User Interface) für Fortgeschrittene	69
5.3.2	SNMP-Shell	79
5.4	BOOTmonitor	79
Kapitel 6	Assistenten	82
Kapitel 7	Systemverwaltung	83
7.1	Status.	83
7.2	Globale Einstellungen	86
7.2.1	System	86
7.2.2	Passwörter	89
7.2.3	Datum und Uhrzeit	91
7.2.4	Systemlizenzen	95
7.3	Schnittstellenmodus / Bridge-Gruppen	98
7.3.1	Schnittstellen.	100
7.4	Administrativer Zugriff	103
7.4.1	Zugriff.	103

7.4.2	SSH	105
7.4.3	SNMP.	109
7.5	Remote Authentifizierung	111
7.5.1	RADIUS	111
7.5.2	TACACS+	117
7.5.3	Optionen	121
7.6	Zertifikate	122
7.6.1	Zertifikatsliste	122
7.6.2	CRLs	132
7.6.3	Zertifikatsserver	133
Kapitel 8	Physikalische Schnittstellen	135
8.1	Ethernet-Ports	135
8.1.1	Portkonfiguration	135
8.2	Serieller Port	137
8.2.1	Serieller Port	137
8.3	Relais	141
8.3.1	Relaiskonfiguration	142
Kapitel 9	LAN	143
9.1	IP-Konfiguration	143
9.1.1	Schnittstellen	143
9.2	VLAN	147
9.2.1	VLANs	149
9.2.2	Portkonfiguration	150
9.2.3	Verwaltung	151
Kapitel 10	Wireless LAN	152
10.1	WLAN.	153

10.1.1	Einstellungen Funkmodul	153
10.1.2	Drahtlosnetzwerke (VSS)	169
10.1.3	WDS-Links.	178
10.1.4	Client Link	181
10.1.5	Bridge-Links	185
10.2	Verwaltung	194
10.2.1	Grundeinstellungen	194
Kapitel 11	Wireless LAN Controller	196
11.1	Wizard	196
11.1.1	Grundeinstellungen	197
11.1.2	Funkmodulprofil	198
11.1.3	Drahtlosnetzwerk	198
11.1.4	Automatische Installation starten	200
11.2	Controller-Konfiguration	202
11.2.1	Allgemein	203
11.3	Slave-AP-Konfiguration	205
11.3.1	Slave Access Points	205
11.3.2	Funkmodulprofile	210
11.3.3	Drahtlosnetzwerke (VSS)	217
11.4	Monitoring	224
11.4.1	Aktive Clients	225
11.4.2	Drahtlosnetzwerke (VSS)	225
11.4.3	Lastverteilung	226
11.4.4	Benachbarte APs	226
11.4.5	Rogue APs	227
11.4.6	Rogue Clients	228
11.5	Wartung	230
11.5.1	Firmware-Wartung	230

Kapitel 12	Netzwerk	232
12.1	Routen	232
12.1.1	Konfiguration von IPv4-Routen	232
12.1.2	IPv4-Routing-Tabelle	239
12.1.3	Optionen	240
12.2	NAT.	242
12.2.1	NAT-Schnittstellen	242
12.2.2	NAT-Konfiguration	243
12.3	Lastverteilung	250
12.3.1	Lastverteilungsgruppen	250
12.3.2	Special Session Handling	255
12.4	QoS	259
12.4.1	QoS-Filter	259
12.4.2	QoS-Klassifizierung	263
12.4.3	QoS-Schnittstellen/Richtlinien	266
12.5	Zugriffsregeln	274
12.5.1	Zugriffsfiler	275
12.5.2	Regelketten	279
12.5.3	Schnittstellenzuweisung	281
12.6	Drop-In	283
12.6.1	Drop-In-Gruppen	283
Kapitel 13	Routing-Protokolle	286
13.1	RIP	286
13.1.1	RIP-Schnittstellen.	286
13.1.2	RIP-Filter	289
13.1.3	RIP-Optionen	291

Kapitel 14	Multicast.	295
14.1	Allgemein	297
14.1.1	Allgemein	297
14.2	IGMP	297
14.2.1	IGMP	298
14.2.2	Optionen	301
14.3	Weiterleiten	302
14.3.1	Weiterleiten	302
14.4	PIM	303
14.4.1	PIM-Schnittstellen	304
14.4.2	PIM-Rendezvous-Punkte	307
14.4.3	PIM-Optionen	309
Kapitel 15	WAN.	311
15.1	Internet + Einwählen	311
15.1.1	PPPoE	313
15.1.2	PPTP	319
15.1.3	IP Pools	324
15.2	Real Time Jitter Control	326
15.2.1	Regulierte Schnittstellen	326
Kapitel 16	VPN	328
16.1	IPSec	328
16.1.1	IPSec-Peers	330
16.1.2	Phase-1-Profile	346
16.1.3	Phase-2-Profile	355
16.1.4	XAUTH-Profile	360
16.1.5	IP Pools	362

16.1.6	Optionen	364
16.2	L2TP	368
16.2.1	Tunnelprofile	368
16.2.2	Benutzer	372
16.2.3	Optionen	379
16.3	GRE	379
16.3.1	GRE-Tunnel	380
Kapitel 17	Firewall	383
17.1	Richtlinien	385
17.1.1	Filterregeln	385
17.1.2	QoS	388
17.1.3	Optionen	390
17.2	Schnittstellen.	391
17.2.1	Gruppen.	392
17.3	Adressen	392
17.3.1	Adressliste.	393
17.3.2	Gruppen.	394
17.4	Dienste	394
17.4.1	Diensteliste	395
17.4.2	Gruppen.	397
Kapitel 18	Lokale Dienste	399
18.1	DNS	399
18.1.1	Globale Einstellungen	401
18.1.2	DNS-Server	403
18.1.3	Statische Hosts.	405
18.1.4	Domänenweiterleitung.	407
18.1.5	Cache.	409
18.1.6	Statistik	409

18.2	HTTPS	411
18.2.1	HTTPS-Server	411
18.3	DynDNS-Client	412
18.3.1	DynDNS-Aktualisierung	412
18.3.2	DynDNS-Provider.	414
18.4	DHCP-Server	416
18.4.1	IP-Pool-Konfiguration	416
18.4.2	DHCP-Konfiguration	417
18.4.3	IP/MAC-Bindung	421
18.4.4	DHCP-Relay-Einstellungen	422
18.5	Scheduling.	423
18.5.1	Auslöser.	424
18.5.2	Aktionen	429
18.5.3	Optionen	441
18.6	Überwachung	442
18.6.1	Hosts	442
18.6.2	Schnittstellen.	445
18.6.3	Temperatur	446
18.6.4	Ping-Generator.	448
18.7	Teldat Discovery	449
18.7.1	Gerätesuche	449
18.7.2	Optionen	452
18.8	Hotspot-Gateway	453
18.8.1	Hotspot-Gateway	455
18.8.2	Optionen	459
Kapitel 19	Wartung	460
19.1	Diagnose	460
19.1.1	Ping-Test	460
19.1.2	DNS-Test	460

19.1.3	Traceroute-Test	461
19.2	Software & Konfiguration	462
19.2.1	Optionen	462
19.3	Neustart	467
19.3.1	Systemneustart.	467
Kapitel 20	Externe Berichterstellung.	469
20.1	Systemprotokoll	469
20.1.1	Syslog-Server	470
20.2	IP-Accounting	472
20.2.1	Schnittstellen.	472
20.2.2	Optionen	473
20.3	Benachrichtigungsdienst	474
20.3.1	Benachrichtigungsempfänger	474
20.3.2	Benachrichtigungseinstellungen	477
20.4	SNMP.	479
20.4.1	SNMP-Trap-Optionen	479
20.4.2	SNMP-Trap-Hosts	481
20.5	Activity Monitor	481
20.5.1	Optionen	482
Kapitel 21	Monitoring.	484
21.1	Internes Protokoll	484
21.1.1	Systemmeldungen	484
21.2	IPSec	485
21.2.1	IPSec-Tunnel	486
21.2.2	IPSec-Statistiken	488
21.3	Schnittstellen.	489
21.3.1	Statistik	489

21.4	WLAN	492
21.4.1	WLANx	492
21.4.2	VSS	495
21.4.3	WDS	498
21.4.4	Bridge-Links	501
21.4.5	Client Links	503
21.4.6	Lastverteilung	505
21.5	Bridges	506
21.5.1	br<x>	506
21.6	Hotspot-Gateway	506
21.6.1	Hotspot-Gateway	506
21.7	QoS	507
21.7.1	QoS	507
21.8	PIM	508
21.8.1	Allgemeine Statusangaben	508
21.8.2	Nicht-schnittstellen-spezifischer Status	509
21.8.3	Schnittstellenspezifische Zustände	512
	Glossar	516
	Index	547

Kapitel 1 Einleitung

Die Access Points der neuen Generation sind umweltfreundlich hergestellt und entsprechen der RoHS-Richtlinie. Sie unterstützen die aktuellste WLAN-Technologie und sind insbesondere für den Einsatz im professionellen Umfeld konzipiert.

Sicherheitshinweise

Was Sie im Umgang mit Ihrem Access Point beachten müssen, erfahren Sie in der Broschüre **Sicherheitshinweise**, die im Lieferumfang Ihres Gerätes enthalten ist.

Installation

Wie Sie Ihr Gerät anschließen, erfahren Sie im Kapitel *Inbetriebnahme* auf Seite 6.

Konfiguration

Das Kapitel *Grundkonfiguration* auf Seite 48 sagt Ihnen, welche Vorbereitungen zur Konfiguration nötig sind. Anschließend zeigen wir Ihnen, wie Sie Ihr Gerät mit einem aktuellen Web-Browser von einem Windows-PC aus erreichen und grundlegende Einstellungen vornehmen können.

Passwort

Wenn Sie sich mit der Konfiguration von Teldat-Geräten gut auskennen und gleich beginnen möchten, fehlen Ihnen eigentlich nur noch der werkseitig eingestellte Benutzername und das Passwort.

Benutzername: *admin*

Passwort: *admin*



Hinweis

Denken Sie daran, das Passwort sofort zu ändern, wenn Sie sich das erste Mal auf Ihrem Gerät einloggen. Alle Teldat-Geräte werden mit gleichem Passwort ausgeliefert. Sie sind daher erst gegen einen unauthorisierten Zugriff geschützt, wenn Sie das Passwort ändern. Die Vorgehensweise bei der Änderung von Passwörtern ist im Kapitel *Systempasswort ändern* auf Seite 56 beschrieben.

Workshops

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

Dime Manager

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

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

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

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

Kapitel 2 Zum Handbuch

Dieses Dokument ist gültig für Teldat-Geräte mit einer System-Software ab Software-Version 9.1.2.

Die Referenz, die Sie vor sich haben, enthält folgende Kapitel:





Benutzerhandbuch - Referenz

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

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

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

Symbolübersicht

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

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

Auszeichnungselemente

Auszeichnung	Verwendung
•	Kennzeichnet Listen.
Menü -> Untermenü Datei -> Öffnen	Kennzeichnet Menüs und Untermenüs.
nicht-proportional, z. B. <code>ping 192.168.0.252</code>	Kennzeichnet Kommandos die Sie wie dargestellt eingeben müssen.
fett, z. B. Windows-Startmenü	Kennzeichnet Tasten, Tastenkombinationen und Windows-Begriffe.
fett, z. B. Lizenzschlüssel	Kennzeichnet Felder.
kursiv, z. B. <i>keiner</i>	Kennzeichnet Werte, die Sie eintragen bzw. die eingestellt werden können.
Online: blau und kursiv, z. B. www.teldat.de	Kennzeichnet Hyperlinks.

Kapitel 3 Inbetriebnahme



Hinweis

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

3.1 bintec W1003n, W2003n, W2003n-ext und W2004n

3.1.1 Aufstellen und Anschließen



Hinweis

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

Die Geräte **bintec W1003n**, **bintec W2003n** und **bintec W2004n** besitzen integrierte Antennen, deren Abstrahlcharakteristik für die Deckenmontage optimiert ist.

Das Gerät **bintec W2003n-ext** verwendet externe Antennen, die im Lieferumfang enthalten sind.

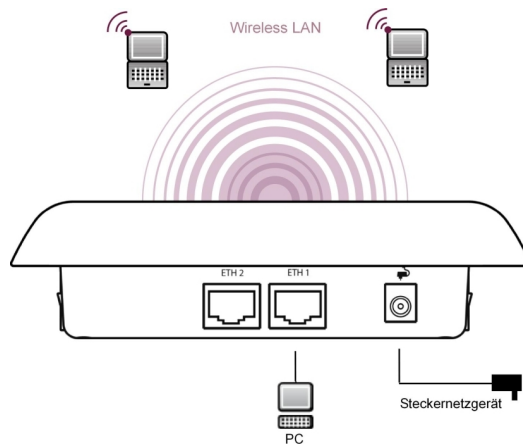


Abb. 2: Anschlussmöglichkeiten **bintec W2003n**, **bintec W2003n-ext**, **bintec W2004n**

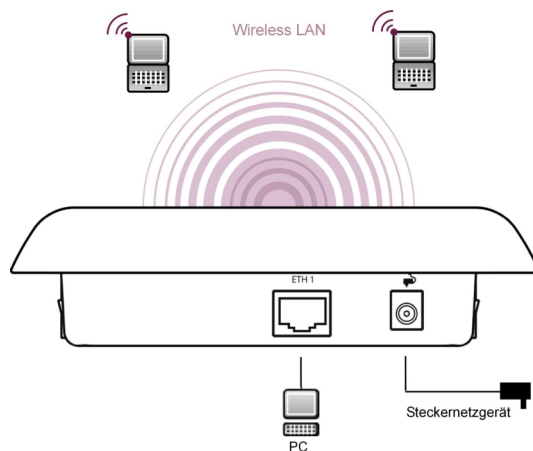


Abb. 3: Anschlussmöglichkeiten **bintec W1003n**

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

(1) Antennen

Bei **bintec W2003n-ext** schrauben Sie die mitgelieferten Standardantennen auf die dafür vorgesehenen Anschlüsse. Falls Sie andere Antennen verwenden, beachten Sie, dass SIMO-Antennen am Anschluss Ant1 und MIMO-Antennen an den Anschlüssen Ant1 und Ant2 anzuschließen sind.

(2) LAN

Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. **bintec W1003n** hat nur einen Gigabit-Ethernet-Port, **ETH1**.

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

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

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

(3) Stromanschluss



Hinweis

Die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** werden ohne Steckernetzteil geliefert. Das Steckernetzteil mit EU-Stecker (Artikelnummer 5500001254) ist als Zubehör erhältlich.

Schließen Sie das Gerät an eine Steckdose an. Nehmen Sie dazu das Steckernetzteil und stecken Sie es in die dafür vorgesehene Buchse Ihres Geräts. Stecken Sie

nun den Netzstecker in eine Steckdose (100–240 V). Durch die Status-LED wird Ihnen signalisiert, dass Ihr Gerät korrekt an die Stromversorgung angeschlossen ist. Optional kann die Stromversorgung über ein Standard PoE-Injector (Artikelnummer 5530000082) erfolgen.

Montage

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

Verwendung als Tischgerät

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

Wand- / Deckenmontage

Um die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** oder **bintec W2004n** an der Wand bzw. Decke zu montieren, verwenden Sie die Halterung, die im Lieferumfang enthalten ist (Artikelnummer 5500001278).



Warnung

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

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

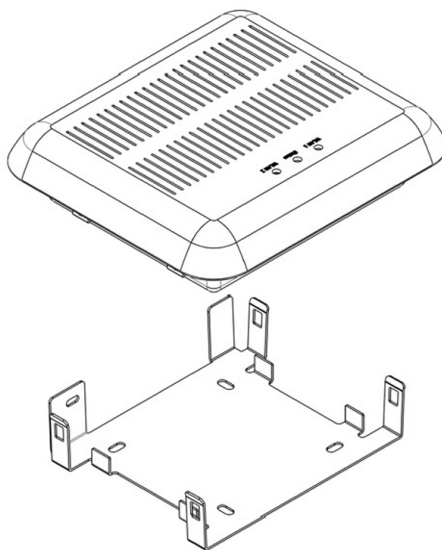


Abb. 4: Deckenmontage **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n**

3.1.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

bintec W1003n verfügt über einen Ethernet-Anschluss, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** verfügen über zwei Ethernet-Anschlüsse.

Die Anschlüsse sind folgendermaßen angeordnet:

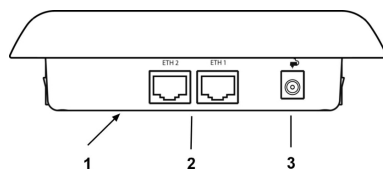


Abb. 5: Unterseite **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n**

bintec W2003n, **bintec W2003n-ext** und **bintec W2004n** Unterseite

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

		Bei bintec W1003n ist nur ETH1 vorhanden!
3	POWER	Buchse für Steckernetzteil

3.1.3 LEDs

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



Hinweis

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

Die LEDs von **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** sind folgendermaßen angeordnet:



Abb. 6: LEDs von **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Status (grün)	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.
	an (statisch)	Fehler
	an (blinkend)	Betriebsbereit
WLAN 1/2 (grün)	aus	Radiomodul oder alle zugeordneten VSS deaktiviert
	an (langsam blinkend)	VSS ist aktiv, kein Client angemeldet
	an (schnell blinkend)	VSS ist aktiv, mindestens 1 Client ist angemeldet
	an (flackernd)	VSS ist aktiv, mindestens 1 Client ist angemeldet, es besteht Datenverkehr

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



Hinweis

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

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

3.1.4 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
bintec W1003n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße Wand- bzw. Deckenbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise
bintec W2003n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße Wand- bzw. Deckenbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise
bintec W2003n-ext	Ethernet-Kabel (RJ-45, STP) 4 externe RSMA-Standardantennen Selbstklebende Füße Wand- bzw. Deckenbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise
bintec W2004n	Ethernet-Kabel (RJ-45, STP) Selbstklebende Füße	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
	Wand- bzw. Deckenbefestigung		on (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise

3.1.5 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	ca. 162 x 145 x 45 mm
Gewicht	ca. 1000 g (mit WLAN-Modulen)
LEDs	Für bintec W1003n : 3 (1x Status, 1x WLAN, 1x Ethernet) Für bintec W2003n , bintec W2003n-ext und bintec W2004n : 4 (1x Status, 2x WLAN, 2x Ethernet)
Leistungsaufnahme Gerät	max. 12 W
Spannungsversorgung	9 V, 1.3 A (Das Steckernetzteil mit der Artikelnummer 5500001254 ist als Zubehör erhältlich) PoE an Ethernet 1 Class 0, gemäß 802.3af (max. 12,4 W). Der Gigabit PoE Injector mit der Artikelnummer 5530000082 ist als Zubehör erhältlich.
Umweltanforderungen:	
Lagertemperatur	-40 °C bis +85 °C
Betriebstemperatur	0 °C bis +40 °C
Relative Luftfeuchtigkeit	10 % bis 100 %
Verfügbare Schnittstellen:	
WLAN	bintec W1003n : 1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2

Eigenschaft	Wert
	<p>bintec W2003n: 1 Radiomodul 802.11bgn 2,4GHz Mimo 2x2; 1 Radiomodul 802.11an 5GHz Mimo 2x2</p> <p>bintec W2003n-ext: 1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2; 1 Radiomodul 802.11abgn 2,4 oder 5GHz Mimo 2x2</p> <p>bintec W2004n: 1 Radiomodul 802.11bgn 2,4GHz Mimo 3x3; 1 Radiomodul 802.11an 5GHz Mimo 3x3</p>
Ethernet IEEE 802.3 LAN	10/100/1000 MBit/s
Vorhandene Buchsen:	
Ethernet-Schnittstelle	<p>bintec W1003n: 1 RJ45-Buchse</p> <p>bintec W2003n, bintec W2003n-ext und bintec W2004n: 2 RJ45-Buchsen</p>
Antennen:	
Antennenanschluss	<p>bintec W1003n: 2 interne Antennen</p> <p>bintec W2003n: 4 interne Antennen</p> <p>bintec W2003n-ext: 4 externe Dualband-Antennen</p> <p>bintec W2004n: 6 interne Antennen</p>
Sendeleistung (WLAN)	max. 100 mW (20 dBm) EIRP
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371
Taster	Reset-Taster für Neustart oder Reset

3.1.6 Reset

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

Dabei werden alle bestehenden Konfigurationsdaten gelöscht.

Bei **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** gehen Sie folgendermaßen vor:

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

(3) Achten Sie auf die LEDs:

Die Status-LED leuchtet, das Gerät durchläuft die Boot-Sequenz.

Lassen Sie **Reset**-Taste los, wenn die Status-LED wieder zu blinken beginnt.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 48 beschrieben.



Hinweis

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



Hinweis

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

3.2 bintec W1002n

3.2.1 Aufstellen und Anschließen



Hinweis

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



Achtung

Die Verwendung eines falschen Netzadapters kann zum Defekt Ihres Geräts führen! Verwenden Sie ausschließlich den mitgelieferten Netzadapter! Falls Sie ausländische Adapter/Netzteile benötigen, wenden Sie sich bitte an unseren Teldat Service.

bintec W1002n ist mit einem Funkmodul und 3 externen Standardantennen zum Aufschrauben ausgestattet. Die Stromversorgung erfolgt durch ein Steckernetzteil oder über PoE (Power over Ethernet).

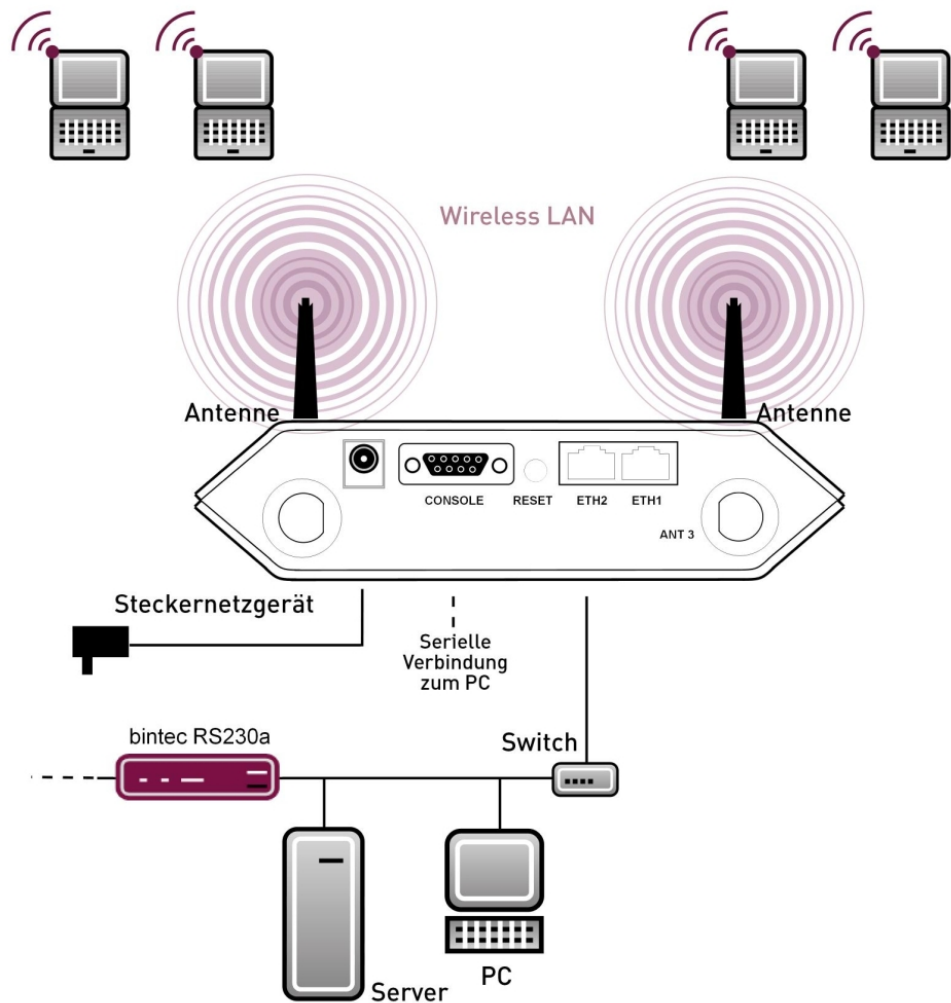


Abb. 7: Anschlussmöglichkeit **bintec W1002n**

Gehen Sie beim Aufstellen und Anschließen folgendermaßen vor:

- (1) Antennen
Schrauben Sie die mitgelieferten Standardantennen auf die dafür vorgesehenen Anschlüsse.
- (2) LAN
Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.
Wählen Sie hier lediglich einen der Anschlüsse **ETH1** oder **ETH2**, der zweite An-

schluss dient der Kaskadierung mehrerer Geräte. Bei Verwendung beider Ethernet-Anschlüsse am selben Switch können sich Loops bilden.
Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(3) Stromanschluss

Schließen Sie das Gerät an eine Steckdose an.

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

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- Serielle Verbindung: Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs (**COM1** oder **COM2**) mit der seriellen Schnittstelle des Geräts (**Console**). Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

Montage

Die Access Points sind wahlweise durch Laschen im Gehäuse an die Wand zu montieren oder als Tischgerät einzusetzen.

Verwendung als Tischgerät

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

Wandmontage

Um ein Gerät der Serie **bintec W1002n** an der Wand zu montieren, benutzen Sie die Laschen an der Gehäuserückseite. Optional ist eine Wandhalterung inkl. Diebstahlschutz (Artikelnummer 5510000009) als Zubehör erhältlich.



Warnung

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

- Schrauben Sie die Halterung mit den 2 Schrauben an der Wand bzw. Decke fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten

Sie darauf das die Anschlüsse des Gerätes zugänglich sind.

- Sichern Sie das Gerät gegen Diebstahl mit dem Diebstahlschutz.

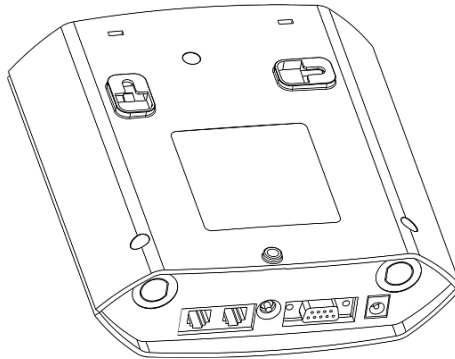


Abb. 8: Wandmontage-Laschen **bintec W1002n**

3.2.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

Bei **bintec W1002n** befindet sich zusätzlich der dritte Antennenanschluss auf der Unterseite des Geräts.

bintec W1002n verfügt über zwei Ethernet-Anschlüsse und einer seriellen Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

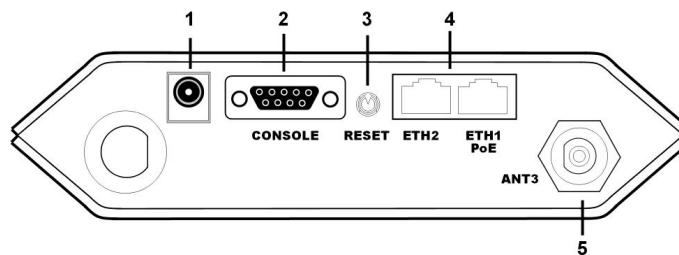


Abb. 9: Unterseite **bintec W1002n**

bintec W1002n Unterseite

1	POWER	Buchse für Steckernetzteil
2	CONSOLE	Serielle Schnittstelle
3	RESET	Reset-Taste
4	ETH1/PoE und	10/100 Base-T Ethernet-Schnittstelle

	ETH2	
5	ANT3	Anschlüsse zum Aufschrauben der externen Antennen ANT3 = RX3
Oberseite ohne Abb.	ANT1/ANT2	Anschlüsse zum Aufschrauben der externen Antennen ANT1 = TX/RX1 (Anschluss erste Richtantenne) ANT2 = TX/RX2 (Anschluss zweite optionale Richtantenne)

3.2.3 Antennenanschlüsse

Die drei Antennen Ihrer Geräte **bintec W1002n** haben in n-Betriebsart MIMO 2T3R, also 2 Transmit und 3 Receive Funktion. WLAN 1 Ant. 1 und WLAN 1 Ant. 2 senden und empfangen, Antenne 3 empfängt nur. Geräte mit 802.11n-Unterstützung können bis zu drei Antennen pro Radiomodul verwenden.

3.2.4 LEDs

Anhand der LEDs können Sie Funk-Status, Funk-Aktivität und Ethernet-Aktivität Ihres Geräts erkennen.

Beim Startvorgang sind alle LEDs an. Dies bedeutet, dass der Monitor gestartet ist und die Firmware geladen wird.

Die LEDs von **bintec W1002n** sind folgendermaßen angeordnet:

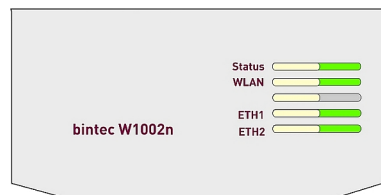


Abb. 10: LEDs von **bintec W1002n**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige bintec W1002n

LED	Status	Information
Status	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind, auch Fehler.

LED	Status	Information
	an (statisch)	Fehler
	an (blinkend)	Betriebsbereit
WLAN 1	an (blinkend langsam)	Frei
	an (statisch)	Mindestens 1 Client ist angemeldet.
	an (flackernd)	Mindestens 1 Client ist angemeldet und es besteht Datenverkehr.
	an (blinkend schnell)	BLD (Broken Link Detection) aktiv
	an (blinkend schnell)	5 GHz Scan aktiv
ETH 1/2	aus	Kein Kabel oder kein Ethernet Link
	an	Kabel eingesteckt und Link
	an (flackernd)	Kabel eingesteckt und Link und Datenverkehr

3.2.5 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
bintec W1002n	Ethernet-Kabel (RJ-45, STP) Steckernetzteil (12 V/ 230 V) 3 externe Standardantennen selbstklebende Füße, um das Gerät als Tischgerät zu verwenden 2 Schrauben und 2 Dübel für Wandbefestigung	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise

3.2.6 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale bintec W1002n

Eigenschaft	Wert
bintec W1002n	Ein internes Funkmodul, 3 externe Antennen
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	163 mm x 168 mm x 50 mm
Gewicht	ca. 430 g
LEDs	4 (1x Status, 1x WLAN, 2x Ethernet)
Leistungsaufnahme Gerät	je nach Ausbau 5-10 Watt
Spannungsversorgung	Externes Schaltnetzteil 12 V DC, 1,25 A PoE an Ethernet 1 Class 0 (isoliert) mit einem WLAN-Modul. Das Gigabit PoE Injector mit der Artikelnummer 5530000082 ist als Zubehör erhältlich.
Umweltanforderungen:	
Lagertemperatur	-10 °C bis +70 °C
Betriebstemperatur	0 °C bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 95 % (nichtkondensierend)
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN (2-Port-Switch)	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, auto-sensing, MDIX
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	9-polige SUB-D-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
Antennen:	
Antennenanschluss	RTNC Buchse
Sendeleistung	max. 100 mW (20 dBm) EIRP
Frequenzbänder	2,4 GHz Indoor/Outdoor (2412-2472 MHz) 5 GHz Indoor (5150-5350 MHz) 5 GHz Outdoor (5470-5725 MHz) 5 GHz BFWA (5755-5875 MHz) nur in Deutschland und Großbritannien (Meldepflicht in Deutschland, Lizenzierungspflicht in Großbritannien).

Eigenschaft	Wert
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG EN 60950-1 (IEC60950); EN 300 328; EN 301 489-17; EN 301 489-1; EN 301 893; EN 60601-1-2 (Medizinische elektrische Geräte - Teil 1-2)
Taster	Ein Monitor-Taster

3.2.7 Reset

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

Dabei werden fast alle bestehenden Konfigurationsdaten ignoriert, nur die aktuellen Benutzer-Passwörter bleiben erhalten. Auf dem Gerät gespeicherte Konfigurationen werden nicht gelöscht und können nach dem Neustart des Geräts ggf. wieder geladen werden.

Bei **bintec W1002n** gehen Sie folgendermaßen vor:

- (1) Trennen Sie Ihr Gerät vom Strom.
- (2) Drücken Sie die **Reset**-Taste Ihres Geräts.
- (3) Halten Sie die **Reset**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.
- (4) Achten Sie auf die LEDs:
 - Zunächst leuchten alle LED auf.
 - Das Gerät durchläuft die Boot-Sequenz.
 - Lassen Sie nach dreimaligem Blinken der LEDs die **Reset**-Taste los.
 - Dann blinkt die *Status*-LED und die *Eth 1* und *Eth 2* leuchten, sofern vorhanden für die Ports, die an das Ethernet angeschlossen sind.

Sollen beim Zurücksetzen des Geräts auch sämtliche Benutzerpasswörter in den Auslieferungszustand zurückgesetzt und gespeicherte Konfigurationen gelöscht werden, gehen Sie wie folgt vor:

- (1) Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Starten Sie Ihr Gerät neu und verfolgen Sie die Boot-Sequenz. Starten Sie den BOOTmonitor und wählen Sie die Option **(4) Konfiguration löschen** und folgen Sie den Anweisungen.
oder
- (2) Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Führen Sie die zuerst beschriebene Reset-Prozedur aus und geben Sie auf der Kommandozeile beim darauf folgenden Anmeldeprompt `erase bootconfig` als **Login** ein. Lassen Sie das Passwort leer und drücken Sie die Eingabetaste. Das Gerät durchläuft erneut die Boot-Sequenz.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 48 beschrieben.



Hinweis

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

3.3 bintec WI1040n und WI2040n

3.3.1 Aufstellen und Anschließen



Hinweis

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



Hinweis

Für die Geräte der **bintec Wix040n**-Serie ist eine Schraubenklemmleiste für die Stromversorgung im Lieferumfang enthalten.

Der Industrie Access Point **bintec WI1040n** ist mit einem Funkmodul und 3 externen Antennen ausgestattet. Der Industrie Access Point **bintec WI2040n** ist mit zwei Funkmodulen und 4 externen Antennen ausgestattet.

Die Geräte der Industrial-WLAN-Serie mit 802.11n-Unterstützung verfügen über eine Vorrichtung, die die Radiomodule bei Temperaturen von unter 10 Grad Celsius zunächst auf Betriebstemperatur aufheizt. Erst wenn diese erreicht ist, fährt das Gerät mit dem eigentlichen Startvorgang fort. Während der Aufwärmphase blinkt die rote Failure-LED.

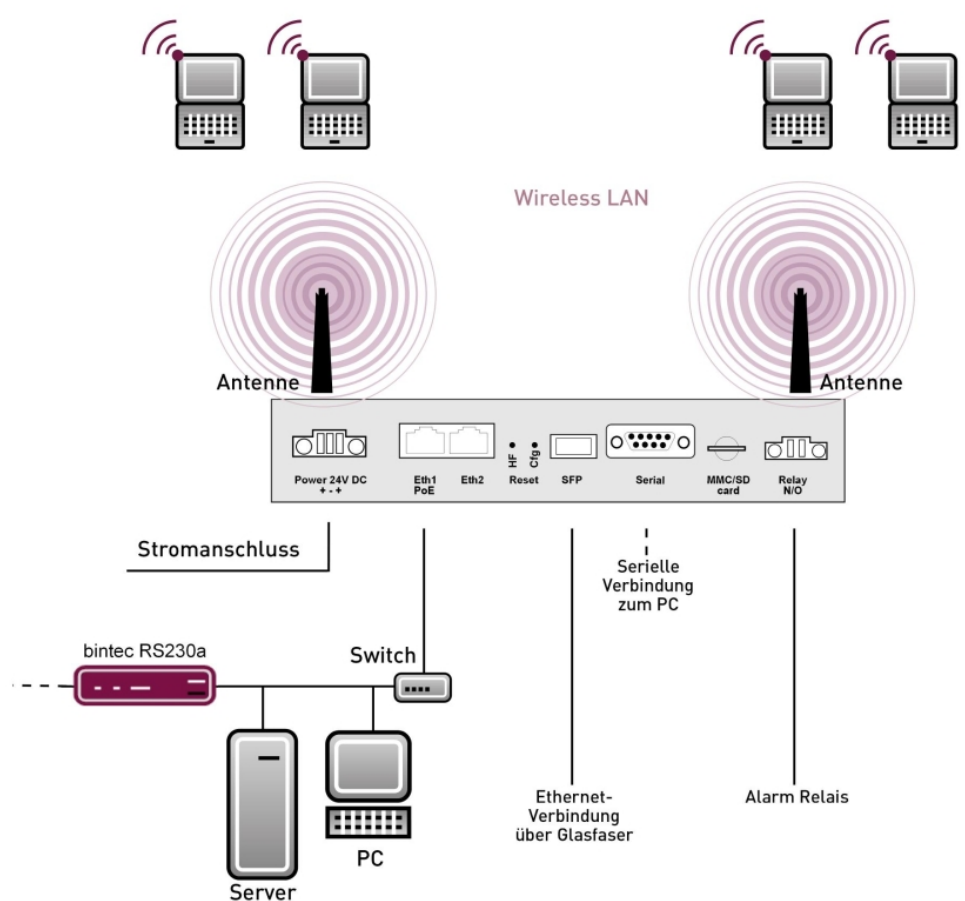


Abb. 11: Anschlussmöglichkeiten **bintec Wlx040n**

Gehen Sie beim Aufstellen und Anschließen folgendermaßen vor:

- (1) Antennen

Schrauben Sie die mitgelieferten Standardantennen auf die dafür vorgesehenen Anschlüsse.
- (2) LAN

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

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

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

(3) Stromanschluss

Schließen Sie das Gerät an eine Steckdose an.

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



Hinweis

Die Produkte der **bintec Wlx040n**-Serie werden ohne Netzteil geliefert. Die Geräte sind zu erden!



Hinweis

Zur Leistungsbegrenzung im Fehlerfall ist der 24 V DC Versorgungsstromkreis installationseitig für **bintec Wlx040n** mit einer externen 2 A-Sicherung abzusichern. Ebenso ist der Relaiskontakt mit einer 1 A-Sicherung (AC) bzw. 2 A-Sicherung (DC) extern abzusichern.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- **Serielle Verbindung:** Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs (**COM1** oder **COM2**) mit der seriellen Schnittstelle des Geräts (**Console**). Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

Montage

Die Access Points sind wahlweise durch Laschen im Gehäuse an die Wand, als Tischgerät oder optional mit Hutschiene montierbar.

Verwendung als Tischgerät

Wahlweise kann der Access Point auch als Tischgerät verwendet werden. Befestigen Sie dazu die vier selbstklebenden Füße auf der unteren Seite des Gerätes. Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.

Wandmontage

Um ein Gerät der **bintec Wlx040n**-Serie an der Wand zu montieren, benutzen Sie die Laschen an der Gehäuserückseite. Optional ist eine Wandhalterung inkl. Diebstahlschutz (Artikelnummer 5020590400), und DIN Hutschienen-Adapter (Artikelnummer 5000592600) als Zubehör erhältlich.



Warnung

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

- Schrauben Sie die Halterung mit den 2 Schrauben an der Wand fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät gegen Diebstahl mit dem mitgelieferten Schloss.

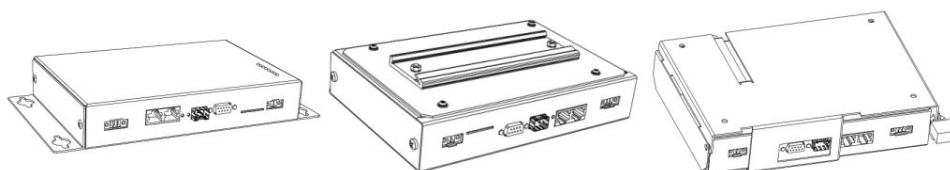


Abb. 12: Wandmontage **bintec WIx040n** (Standardausführung, optional Hutschiene oder mit Diebstahlsicherung)

3.3.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

bintec WI1040n und **bintec WI2040n** verfügen über zwei Ethernet-Anschlüsse und über eine serielle Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

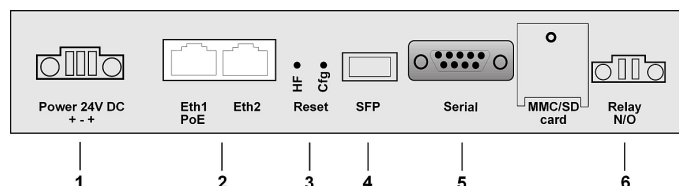


Abb. 13: Unterseite **bintec WI1040n** und **bintec WI2040n**

bintec WI1040n und **bintec WI2040n** Unterseite

1	Power 24V DC	Buchse für die Stromversorgung
2	Eth1 (PoE) / Eth2	10/100 Base-T Ethernet-Schnittstellen
3	Reset (HW und	Reset-Taste und löschen der Konfiguration

	Cfg)	
4	SFP	SFP slot für 100 Mbit/s Fiber-Modul (optional)
5	Serial	Serielle Schnittstelle RS232
6	Relay N/O	Alarm Relais

3.3.3 Antennenanschlüsse



Hinweis

Die drei Antennen Ihrer Geräte **bintec W11040n** haben in n-Betriebsart MIMO 2T3R, also 2 Transmit und 3 Receive Funktion. WLAN 1 Ant. 1 und WLAN 1 Ant. 2 senden und empfangen, Antenne 3 empfängt nur.

Bei den Geräten **bintec W12040n** sind für jedes der zwei Radiomodule nur 2 Antennen verwendet. Das sind die beiden Sende- Empfangsantennen. Die jeweils dritte Empfangsantenne entfällt, hier also MIMO 2T2R Betrieb.

Die 300 Mbit/s Bruttorate sind jedoch möglich. Die Empfangsempfindlichkeit reduziert sich dabei geringfügig. Für den Betrieb von Bridgeline mit Dual-Polarisationsantenne werden nur 2 Antennenanschlüsse benötigt.

Antennen sollten $\lambda/2$ oder ein vielfaches davon auseinanderstehen. Bei **bintec W1x040n** stehen die Antennen 37 mm auseinander.

2,4 GHz $\lambda/2$ entspricht 6,15 cm 5 GHz $\lambda/2$ entspricht 2,72 cm.

Geräte mit 802.11n-Unterstützung können bis zu drei Antennen pro Radiomodul verwenden. Die Belegung der vorhandenen vier Antennenanschlüsse können Sie der folgenden Grafik entnehmen:

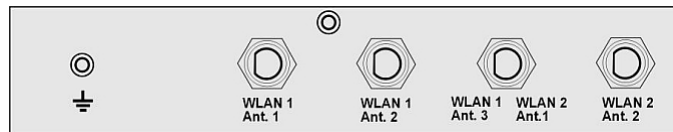


Abb. 14: Antennenbelegung der **bintec W1x040n**-Geräte

3.3.4 LEDs

Anhand der LEDs können Sie Funk-Status, Funk-Aktivität, Ethernet-Aktivität und LED-Zustände Ihres Geräts erkennen. Die LED-Zustände werden über Kombinationen der LEDs angezeigt.

Während der Aufwärmphase blinkt die rote Failure-LED. Erst wenn diese erreicht ist, fährt das Gerät mit dem eigentlichen Startvorgang fort.

Beim Startvorgang sind alle LEDs an. Dies bedeutet, dass der Monitor gestartet ist und die Firmware geladen wird.



Hinweis

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

Die LEDs von **bintec WI1040n** und **bintec WI2040n** sind folgendermaßen angeordnet:

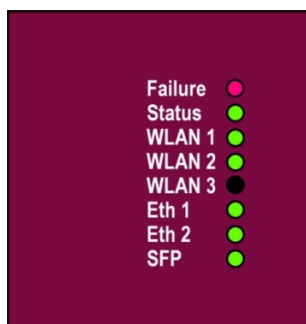


Abb. 15: LEDs von **bintec WI1040n** und **bintec WI2040n**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige bintec WI1040n und bintec WI2040n

LED	Status	Information
Failure (rot)	an	Nach Power-up und während des Bootens oder wenn ein Fehler auftritt.
	blinkt	Während der Aufwärmphase.
	aus	Wenn das Gerät am Login-Prompt steht.
Status (grün)	aus	Stromversorgung ist nicht abgeschlossen. Wenn andere LEDs an sind, auch Fehler.
	an (statisch)	Fehler
	an (blinkend)	Betriebsbereit
WLAN 1/2 (2x grün)	an (blinkend langsam)	Frei

LED	Status	Information
WLAN 3 ohne Funktion		
	an (statisch)	Mindestens 1 Client ist angemeldet.
	an (flackernd)	Mindestens 1 Client ist angemeldet und es besteht Datenverkehr.
	an (blinkend schnell)	BLD (Broken Link Detection) aktiv
	an (blinkend schnell)	5 GHz Scan aktiv
ETH 1/2 (2x grün)	aus	Kein Kabel oder kein Ethernet Link
	an	Kabel eingesteckt und Link
	an (flackernd)	Kabel eingesteckt und Link und Datenverkehr
SFP (grün)	aus	Kein Datenverkehr
	an	Datenverkehr über die SFP-Schnittstelle
	an (flackernd)	Kabel eingesteckt und Datenverkehr

3.3.5 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
bintec WI1040n	Ethernet-Kabel (RJ-45, STP) Serielles Anschlusskabel (D-SUB9) 3 externe Standardantennen selbstklebende Füße, um das Gerät als Tischgerät zu verwenden Blindstopfen für SFP SD-Slot-Abdeckung mit Schraube 3 polige Schrau-	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt) Benutzerhandbuch (auf DVD) Sicherheitshinweise

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
	<p>benklemmleiste für die Stromversorgung</p> <p>2 polige Schraubenklemmleiste für Relais</p> <p>Montagewinkel für die Wandmontage</p> <p>1 Schrauben-Dübelset</p> <p>Blindstopfen für Ethernet-Schnittstellen</p>		
bintec WI2040n	<p>Ethernet-Kabel (RJ-45, STP)</p> <p>Serielltes Anschlusskabel (D-SUB9)</p> <p>4 externe Standardantennen</p> <p>selbstklebende Füße, um das Gerät als Tischgerät zu verwenden</p> <p>Blindstopfen für SFP</p> <p>SD-Slot-Abdeckung mit Schraube</p> <p>3 polige Schraubenklemmleiste für die Stromversorgung</p> <p>2 polige Schraubenklemmleiste für Relais</p> <p>Montagewinkel für die Wandmontage</p> <p>1 Schrauben-Dübelset</p> <p>Blindstopfen für Ethernet-Schnittstellen</p>	Companion DVD	<p>Kurzanleitung (gedruckt)</p> <p>R&TTE Compliance Information (gedruckt)</p> <p>Benutzerhandbuch (auf DVD)</p> <p>Sicherheitshinweise</p>

3.3.6 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale bintec WI1040n und bintec WI2040n

Eigenschaft	Wert
Varianten:	
bintec WI1040n	Ein internes Funkmodul, 3 externe Antennen (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 1 Ant.3)
bintec WI2040n	Zwei interne Funkmodule, 4 externe Antennen (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 2 Ant.1, WLAN 2 Ant.2)
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	220 mm x 185 mm x 42 mm ohne Füße
Gewicht	ca. 1200 g (mit WLAN-Modulen)
LEDs	bintec WI1040n 6 (1x Failure, 1x Status, 1x WLAN, 2x Ethernet, 1x SFP) bintec WI2040n 7 (1x Failure, 1x Status, 2x WLAN, 2x Ethernet, 1x SFP)
Leistungsaufnahme Gerät	je nach Ausbau 5-24 Watt
Spannungsversorgung	Schutzleiter/Erdanschluss 5-20 W. Die Geräte sind zu erden! 24 V ± 30 % DC 1,1 A polaritätsfrei, isoliert 3-polig PoE an Ethernet 1 Class 0 (isoliert) mit max. zwei WLAN-Modulen
Diebstahlsicherung	Diebstahlsicherung als Option erhältlich
Temperatur Sensor	Temperaturüberwachung und Software gesteuerte Aktionen möglich
Umweltanforderungen:	
Lagertemperatur	-40 °C bis +85 °C
Betriebstemperatur	-25 °C bis +70 °C
Relative Luftfeuchtigkeit	10 % bis 95 % (nichtkondensierend)
Raumklassifizierung	Nur in trockenen Räumen betreiben

Eigenschaft	Wert
Verfügbare Schnittstellen:	
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, auto-sensing, MDI/MDIX 2x 10/100 Base T/TX
Relais	Bei Übertemperatur oder bei Fehler ist ein Alarm mittels Relais möglich: potentialfreier Arbeitskontakt, 42 V AC 1 A / 30 V DC 2 A
Optisches Interface	Modulslot für Optisches Interface 100 Mbit/s LWL Single Mode LC oder LWL Multimode LC - 1x 100 Base FX/SX mit SFP Modul
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	9-polige SUB-D-Buchse
Relais-Schaltkontakt N/O	42 V AC 1 A / 30 V DC 2 A potentialfrei, software konfigurierbar, schaltbar
Ethernet-Schnittstelle	RJ45-Buchse
Antennen:	
Antennenanschluss	RTNC Buchse
Sendeleistung (WLAN)	max. 100 mW (20 dBm) EIRP
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371 (Medizinische Einrichtungen EN 60601-1; EN 60601-2; EN 55011) E1-mark (Kraftfahrzeugzulassung)
Taster	Reset und Reset auf Werkseinstellung mit zwei Tastern möglich (1x Config Reset, 1x HW-Reset)

Um einen sicheren Betrieb zu gewährleisten sind die Geräte der WI-Serie mit einem Erdanschluss versehen. Der Mindestquerschnitt des Erdleiters soll 1,5 mm² betragen. Der Abstand zwischen den Gerät und der Erdung soll möglichst kurz sein.



Abb. 16: Erdanschluss **bintec Wlx040n**

3.3.7 Reset

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

Dabei werden fast alle bestehenden Konfigurationsdaten ignoriert, nur die aktuellen Benutzer-Passwörter bleiben erhalten. Auf dem Gerät gespeicherte Konfigurationen werden nicht gelöscht und können nach dem Neustart des Geräts ggf. wieder geladen werden.

Bei **bintec WI1040n** und **bintec WI2040n** gehen Sie folgendermaßen vor:

- (1) Trennen Sie Ihr Gerät vom Strom.
- (2) Drücken Sie die **Cfg**-Taste Ihres Geräts.
- (3) Halten Sie die **Cfg**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.
- (4) Achten Sie auf die LEDs:
 - Zunächst blinkt die rote LED *Failure*.
 - Halten Sie die **Cfg**-Taste so lange gedrückt bis die rote LED erlischt und die grüne *Status*-LED anfängt zu blinken.

Sollen beim Zurücksetzen des Geräts auch sämtliche Benutzerpasswörter in den Auslieferungszustand zurückgesetzt und gespeicherte Konfigurationen gelöscht werden, gehen Sie wie folgt vor:

- (1) Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Starten Sie Ihr Gerät neu und verfolgen Sie die Boot-Sequenz. Starten Sie den BOOTmonitor und wählen Sie die Option **(4) Konfiguration löschen** und folgen Sie den Anweisungen.
oder
- (2) Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Führen Sie die zuerst beschriebene Reset-Prozedur aus und geben Sie auf der Kommandozeile beim darauf folgenden Anmeldeprompt *erase bootconfig* als **Login** ein. Lassen Sie das Passwort leer und drücken Sie die Eingabetaste. Das Gerät durchläuft erneut die Boot-Sequenz.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 48 beschrieben.



Hinweis

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

Auf den Geräten der **bintec Wlx040n**-Serie befindet sich ein weiterer Taster, der **HW-Reset**. Nach einmaligem kurzem Drücken führt das Gerät einen Neustart durch.



Abb. 17: Unterseite von **bintec Wlx040n** mit den HW und Cfg Reset-Knopf

3.4 bintec WI1065n und WI2065n

3.4.1 Aufstellen und Anschließen



Hinweis

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



Hinweis

Für die Geräte der **bintec Wlx065n**-Serie ist eine Schraubenklemmleiste für die Stromversorgung im Lieferumfang enthalten.

bintec WI1065n ist ein Outdoor Access Point mit einem Funkmodul und drei externen Antennen. **bintec WI 2065n** ist ein Outdoor Access Point mit zwei Funkmodulen und 4 externen Antennen.

Die Geräte der Industrial-WLAN-Serie mit 802.11n-Unterstützung verfügen über eine Vorrichtung, die die Radiomodule bei Temperaturen von unter 10 Grad Celsius zunächst auf Betriebstemperatur aufheizt. Erst wenn diese erreicht ist, fährt das Gerät mit dem eigentlichen Startvorgang fort. Während der Aufwärmphase blinkt die rote Failure-LED.

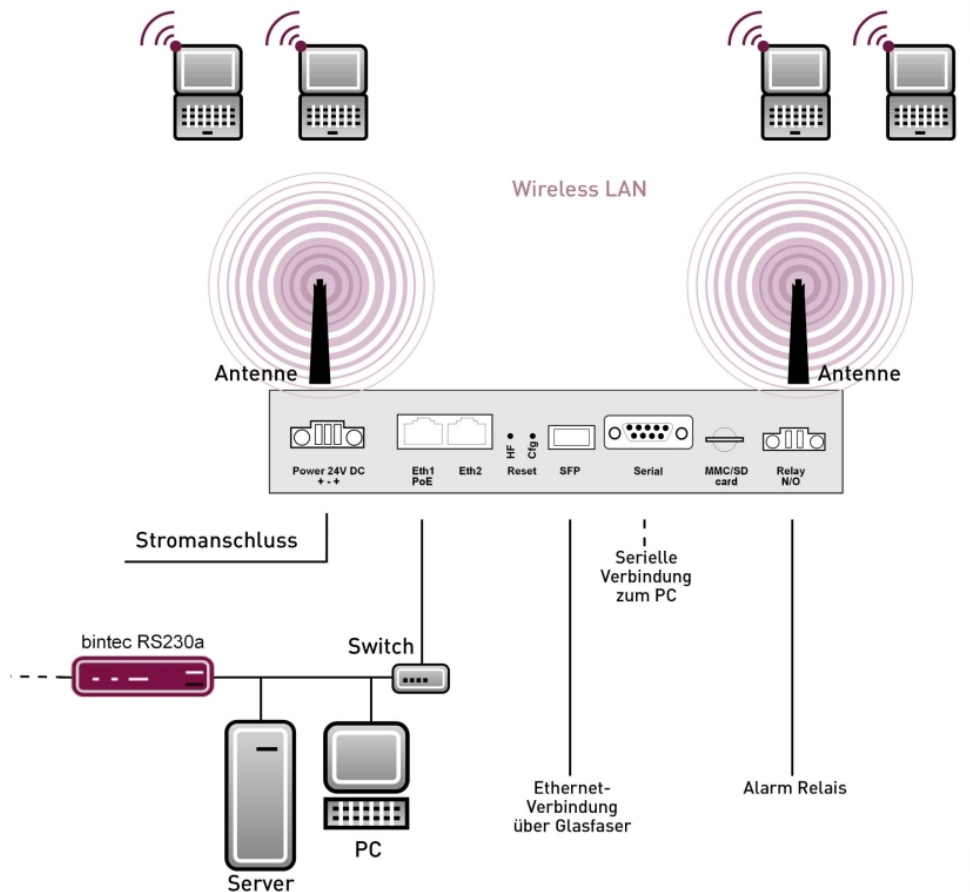


Abb. 18: Anschlussmöglichkeiten **bintec Wlx065n**

Gehen Sie beim Aufstellen und Anschließen folgendermaßen vor:

- (1) **Antennen**
Schrauben Sie die mitgelieferten Standardantennen auf die dafür vorgesehenen Anschlüsse.
- (2) **LAN**
Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den Anschluss **ETH1** oder **ETH2** Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.
Wählen Sie hier lediglich einen der Anschlüsse **ETH1** oder **ETH2**, der zweite Anschluss dient der Kaskadierung mehrerer Geräte. Bei Verwendung beider Ethernet-Anschlüsse am selben Switch können sich Loops bilden.
Das Standard-Patchkabel (RJ45-RJ45) ist symmetrisch aufgebaut. Ein Vertauschen der Kabelenden ist dadurch ausgeschlossen.

(3) Stromanschluss

Schließen Sie das Gerät an eine Steckdose an.

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



Hinweis

Die Produkte der **bintec Wlx065n**-Serie werden ohne Netzteil geliefert. Die Geräte sind zu erden!



Hinweis

Zur Leistungsbegrenzung im Fehlerfall ist der 24 V DC Versorgungsstromkreis installationseitig für **bintec Wlx065n** mit einer externen 2 A-Sicherung abzusichern. Ebenso ist der Relaiskontakt mit einer 1 A-Sicherung (AC) bzw. 2 A-Sicherung (DC) extern abzusichern.



Hinweis

Bei Outdoor Installation des **bintec Wlx065n** sind die außerhalb von Gebäuden verlegten Leitungen nach EN60950 als TNV1 Stromkreise einzustufen, da deren SELV-Pegel bei bestimmungsgemäßem Betrieb zusätzlich von transienten Überspannungen überlagert sein kann (z. B. bei Gewitter). Bei der Anschlussverkabelung ist deshalb darauf zu achten, dass im Bereich des Kabeleintritts im Gebäude Schutzmaßnahmen gegen Überspannung zu installieren sind, die es gewährleisten dass im Gebäude die Grenzwerte eines SELV-Stromkreises eingehalten werden.

Je nach Anforderung können Sie weitere Verbindungen einrichten:

- **Serielle Verbindung:** Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs (**COM1** oder **COM2**) mit der seriellen Schnittstelle des Geräts (**Console**). Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

Montage

Die Access Points sind wahlweise durch Laschen im Gehäuse an die Wand bzw. durch eine Haltevorrichtung an der Zimmerdecke oder am Mast montierbar.

Wand- / Deckenmontage

Um ein Gerät der Serie **bintec Wlx065n**-Serie an der Wand zu montieren, benutzen Sie die Laschen an der Gehäuserückseite. Optional ist eine Wandhalterung inkl. Diebstahlschutz (Artikelnummer 5020591600), und Masthalterung für die Acces Points (Artikelnummer 5020591700) als Zubehör erhältlich.



Warnung

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

- Schrauben Sie die Halterung mit den 2 Schrauben an der Wand bzw. Decke fest.
- Hängen Sie das Gerät, ohne es zu verschrauben mit der Nut in die Halterung ein. Achten Sie darauf das die Anschlüsse des Gerätes zugänglich sind.
- Sichern Sie das Gerät gegen Diebstahl mit dem mitgelieferten Schloss.



Abb. 19: Wandmontage **bintec Wlx065n** (Standardausführung und mit Diebstahlsicherung)

3.4.2 Anschlüsse

Alle Anschlüsse befinden sich auf der Unterseite des Geräts.

bintec W11065n und **bintec W12065n** verfügen über zwei Ethernet-Anschlüsse und über eine serielle Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

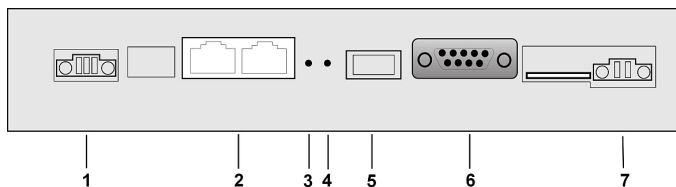


Abb. 20: Unterseite **bintec WI1065n** und **bintec WI2065n**

bintec WI1065n und bintec WI2065n Unterseite

1	Power 24 V DC	Buchse für die Stromversorgung
2	Eth1 PoE / Eth2	10/100 Base-T Ethernet-Schnittstellen
3	HW	Reset-Taste führt Neustart durch
4	Cfg	Löschen der Konfiguration
5	SFP	SFP slot für 100 Mbit/s Fiber-Modul (optional)
6	Serial	Serielle Schnittstelle RS232
7	Relay N/O	Alarm Relaiskontakt

3.4.3 Antennenanschlüsse



Hinweis

Die drei Antennen Ihrer Geräte **bintec WI1065n** haben in n-Betriebsart MIMO 2T3R, also 2 Transmit und 3 Receive Funktion. WLAN 1 Ant. 1 und WLAN 1 Ant. 2 senden und empfangen, Antenne 3 empfängt nur.

Bei den Geräten **bintec WI2065n** sind für jedes der zwei Radiomodule nur 2 Antennen verwendet. Das sind die beiden Sende- Empfangsantennen. Die jeweils dritte Empfangsantenne entfällt, hier also MIMO 2T2R Betrieb.

Die 300 Mbit/s Bruttorate sind jedoch möglich. Die Empfangsempfindlichkeit reduziert sich dabei geringfügig. Für den Betrieb von Bridgeline mit Dual-Polarisationsantenne werden nur 2 Antennenanschlüsse benötigt.

Antennen sollten $\lambda/2$ oder ein vielfaches davon auseinanderstehen. Bei **bintec Wix065n** stehen die Antennen 55 mm auseinander.

2,4 GHz $\lambda/2$ entspricht 6,15 cm 5 GHz $\lambda/2$ entspricht 2,72 cm.

Geräte mit 802.11n-Unterstützung können bis zu drei Antennen pro Radiomodul verwenden. Die Belegung der vorhandenen vier Antennenanschlüsse können Sie der folgenden Grafik entnehmen:

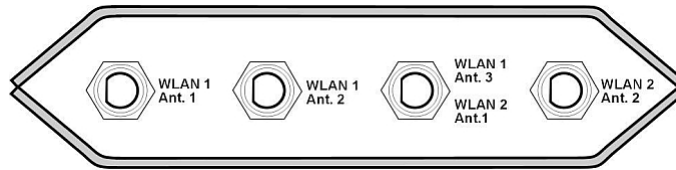


Abb. 21: Antennenbelegung der **bintec Wi065n**-Geräte

3.4.4 LEDs

Anhand der LEDs können Sie Funk-Status, Funk-Aktivität, Ethernet-Aktivität und LED-Zustände Ihres Geräts erkennen. Die LED-Zustände werden über Kombinationen der LEDs angezeigt.

Während der Aufwärmphase blinkt die rote Failure-LED. Danach gehen im Laufe des bootens die anderen LEDs an (bei Initialisierung der entsprechenden Baugruppen).

Beim Startvorgang sind alle LEDs an. Dies bedeutet, dass der Monitor gestartet ist und die Firmware geladen wird.



Hinweis

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

Die LEDs von **bintec WI1065n** und **bintec WI2065n** sind folgendermaßen angeordnet:

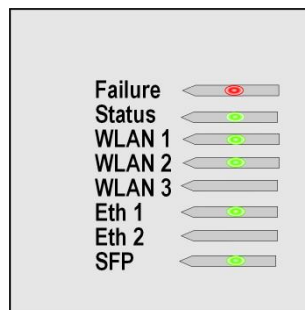


Abb. 22: LEDs von **bintec WI1065n** und **bintec WI2065n**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige bintec WI1065n und bintec WI2065n

LED	Status	Information
Failure (rot)	an	Nach Power-up und während des Bootens oder wenn ein Fehler auftritt.
	blinkt	Während der Aufwärmphase.
	aus	Wenn das Gerät am Login-Prompt steht.
Status (grün)	aus	Stromversorgung ist nicht angeschlossen. Wenn andere LEDs an sind auch Fehler.
	an (statisch)	Fehler
	an (blinkend)	Betriebsbereit
WLAN 1/2 (2x grün) WLAN 3 ohne Funktion	an (blinkend langsam)	Frei
	an (statisch)	Mindestens 1 Client ist angemeldet
	an (flackernd)	Mindestens 1 Client ist angemeldet und es besteht Datenverkehr
	an (blinkend schnell)	BLD (Broken Link Detection) aktiv
	an (blinkend schnell)	5 GHz Scan aktiv
	aus	Kein Kabel oder kein Ethernet Link
	an	Kabel eingesteckt und Link
ETH 1/2 (2x grün)	an (flackernd)	Kabel eingesteckt und Link und Datenverkehr
	aus	Kein Datenverkehr
	an	Datenverkehr über die SFP-Schnittstelle
SFP (grün)	an (flackernd)	Kabel eingesteckt und Datenverkehr

3.4.5 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
bintec WI1065n	Ethernet-Kabel (RJ-45, STP) Seriell Anschlusskabel (D-SUB9)	Companion DVD	Kurzanleitung (gedruckt) R&TTE Compliance Information (gedruckt)

	Kabelsätze/Netzteil/Sonstiges	Software	Dokumentation
	<p>3 externe Standardantennen</p> <p>Blindstopfen für SFP</p> <p>SD-Slot-Abdeckung mit Schraube</p> <p>3 polige Schraubenklemmleiste für die Stromversorgung</p> <p>2 polige Schraubenklemmleiste für Relais</p> <p>1 Schrauben-Dübelset</p> <p>Blindstopfen für Ethernet-Schnittstellen</p> <p>4 Abdeckgewindekappen für die Antennen</p>		<p>Benutzerhandbuch (auf DVD)</p> <p>Sicherheitshinweise</p>
bintec WI2065n	<p>Ethernet-Kabel (RJ-45, STP)</p> <p>Serielles Anschlusskabel (D-SUB9)</p> <p>4 externe Standardantennen</p> <p>Blindstopfen für SFP</p> <p>SD-Slot-Abdeckung mit Schraube</p> <p>3 polige Schraubenklemmleiste für die Stromversorgung</p> <p>2 polige Schraubenklemmleiste für Relais</p> <p>1 Schrauben-Dübelset</p> <p>Blindstopfen für Ethernet-Schnittstellen</p> <p>4 Abdeckgewindekappen für die Antennen</p> <p>Ein Satz Gummidichtungen für die Kabeldurchführungen</p>	Companion DVD	<p>Kurzanleitung (gedruckt)</p> <p>R&TTE Compliance Information (gedruckt)</p> <p>Benutzerhandbuch (auf DVD)</p> <p>Sicherheitshinweise</p>

3.4.6 Allgemeine Produktmerkmale

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

Die Merkmale sind in folgender Tabelle zusammengefasst:

Allgemeine Produktmerkmale bintec WI1065n und bintec WI2065n

Eigenschaft	Wert
Varianten:	
bintec WI1065n	Ein internes Funkmodul, 3 externe Antennen (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 1 Ant.3)
bintec WI2065n	Zwei interne Funkmodule, 4 externe Antennen (WLAN 1 Ant.1, WLAN 1 Ant.2, WLAN 2 Ant.1, WLAN 2 Ant.2)
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x L x H)	257 mm x 285 mm x 60 mm
Gewicht	ca. 1900 g (mit WLAN-Modulen)
LEDs	7 (1x Failure, 1x Status, 2x WLAN, 2x Ethernet, 1x SFP)
Leistungsaufnahme Gerät	je nach Ausbau 5-24 Watt
Spannungsversorgung	Schutzleiter/Erdanschluss 5-20 W. Die Geräte sind zu erden! 24 V ± 30 % DC 1,1 A polaritätsfrei isoliert, 3 polig PoE an Ethernet 1 Class 0 (isoliert) mit max. zwei WLAN-Modulen
Diebstahlsicherung	Diebstahlsicherung als Option erhältlich
Temperatur Sensor	Temperaturüberwachung und Software gesteuerte Aktionen möglich
Umweltanforderungen:	
Lagertemperatur	-40 °C bis +85 °C
Betriebstemperatur	-20 °C bis +65 °C
Relative Luftfeuchtigkeit	10 % bis 100 %
Verfügbare Schnittstellen:	
Serielle Schnittstelle V.24	Fest eingebaut, unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
Ethernet IEEE 802.3 LAN	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, auto-sensing, MDI/MDIX 2x 10/100 Base T/TX

Eigenschaft	Wert
Relais	Bei Übertemperatur oder bei Fehler ist ein Alarm mittels Relais möglich: potentialfreier Arbeitskontakt, 42 V AC 1 A / 30 V DC 2 A
Optisches Interface	Modulslot für Optisches Interface 100 Mbit/s LWL Single Mode LC oder LWL Multimode LC - 1x 100 Base FX/SX mit SFP Modul
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	9-polige SUB-D-Buchse
Relais-Schaltkontakt N/O	42 V AC 1 A / 30 V DC 2 A potentialfrei, software konfigurierbar, schaltbar
Ethernet-Schnittstelle	RJ45-Buchse
Antennen:	
Antennenanschluss	RTNC Buchse
Sendeleistung (WLAN)	max. 100 mW (20 dBm) EIRP
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG EN 60950-1 (IEC60950); EN 60950-22; EN 301489-1; EN301489-17; EN 55022; EN 300328-1; EN 301893; EN 302502; EN 50371
Taster	Reset und Reset auf Werkseinstellung mit zwei Tastern möglich (1x Config Reset, 1x HW-Reset)

Um einen sicheren Betrieb zu gewährleisten sind die Geräte der WI-Serie mit einem Erdanschluss versehen. Der Mindestquerschnitt des Erdleiters soll 1,5 mm² betragen. Der Abstand zwischen dem Gerät und der Erdung soll möglichst kurz sein. Bei den Geräten **bintec WIx065n** befindet sich der Erdanschluss unter der Abdeckung.

3.4.7 Reset

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

Dabei werden fast alle bestehenden Konfigurationsdaten ignoriert, nur die aktuellen Benutzer-Passwörter bleiben erhalten. Auf dem Gerät gespeicherte Konfigurationen werden nicht gelöscht und können nach dem Neustart des Geräts ggf. wieder geladen werden.

Bei **bintec WI1065n** und **bintec WI2065n** gehen Sie folgendermaßen vor:

- (1) Trennen Sie Ihr Gerät vom Strom.
- (2) Drücken Sie die **Cfg**-Taste Ihres Geräts.
- (3) Halten Sie die **Cfg**-Taste Ihres Geräts gedrückt und schließen Sie das Gerät wieder an den Strom an.

- (4) Achten Sie auf die LEDs:
 - Zunächst blinkt die rote LED *Failure*.
 - Halten Sie die **Cfg**-Taste so lange gedrückt bis die rote LED erlischt und die grüne *Status*-LED anfängt zu blinken.
- (1) Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Starten Sie Ihr Gerät neu und verfolgen Sie die Boot-Sequenz. Starten Sie den BOOTmonitor und wählen Sie die Option **(4) Konfiguration löschen** und folgen Sie den Anweisungen.
oder
- (2) Stellen Sie eine serielle Verbindung zu Ihrem Gerät her. Führen Sie die zuerst beschriebene Reset-Prozedur aus und geben Sie auf der Kommandozeile beim darauf folgenden Anmeldeprompt *erase bootconfig* als **Login** ein. Lassen Sie das Passwort leer und drücken Sie die Eingabetaste. Das Gerät durchläuft erneut die Boot-Sequenz.

Nun können Sie die Konfiguration Ihres Geräts erneut durchführen wie ab [Grundkonfiguration](#) auf Seite 48 beschrieben.



Hinweis

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

3.5 Reinigen

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

3.6 Pin-Belegung

3.6.1 Ethernet-Schnittstelle

Die Geräte **bintec W1002n**, **bintec W11040n**, **bintec W12040n**, **bintec W11065n** und **bintec W12065n** verfügen über zwei 10/100 Ethernet-Schnittstellen. Diese dienen zur Anbindung einzelner PCs oder weiterer Switches.

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt bei **bintec W1002n** keine Auto-MDI-X

Funktion.

Der Anschluss erfolgt über eine RJ45-Buchse.

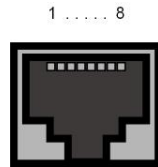


Abb. 23: 10/100 Base-T Ethernet-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für LAN-Anschluss

Pin	Funktion
1	Tx+ (eingang)
2	Tx- (eingang)
3	Rx+ (ausgang)
4	--
5	--
6	Rx- (ausgang)
7	--
8	--

Die Geräte **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** verfügen über zwei 10/100/1000 Ethernet-Schnittstellen, **bintec W1003n** hat eine 10/100/1000 Ethernet-Schnittstelle.

Der Anschluss erfolgt über eine RJ45-Buchse.

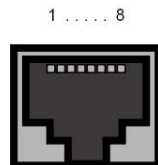


Abb. 24: 10/100/1000 Base-T Ethernet-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für LAN-Anschluss

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

3.6.2 Serielle Schnittstelle

Zum Anschluss einer Konsole verfügen die Geräte **bintec W1002n**, **bintec WI1040n**, **bintec WI2040n**, **bintec WI1065n** und **bintec WI2065n** über eine serielle Schnittstelle. Diese unterstützt Baudraten von 1200 bis 115200 Bit/s.

Die Schnittstelle ist als 9-polige SUB-D-Buchse ausgeführt.

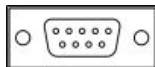


Abb. 25: 9-polige SUB-D-Buchse

Die Pin-Belegung ist wie folgt:

Pin-Belegung der SUB-D-Buchse

Pin	Funktion bintec W1002n
1	Nicht genutzt
2	RxD
3	TxD
4	Nicht genutzt
5	GND
6	DSR
7	RTS
8	CTS
9	Nicht genutzt

3.6.3 Buchse für die Stromversorgung

Die Geräte der WI-Serie (**bintec WI1040n**, **bintec WI2040n**, **bintec WI1065n** und **bintec WI2065n**) verfügen über einen 3-poligen Anschluss für die Stromversorgung. Eine einzelne Stromversorgung kann in beliebiger Polarität und an beliebigen Klemmen 2-polig angeschlossen werden. Wird eine redundante Stromversorgung gewählt (2 Netzteile) so sind die Minuspole gemeinsam an Klemme 2 und die Pluspole separat an die Klemmen 1 und 3 anzuschließen.

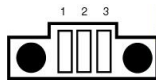


Abb. 26: 3-polige Buchse für die Stromversorgung

Die Pin-Belegung ist wie folgt:

Pin-Belegung der Buchse für die Stromversorgung

Pin	Belegung
1	+
2	-
3	+

3.7 Frequenzen und Kanäle

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

3.8 Support Information

Wenn Sie zu Ihrem neuen Produkt Fragen haben oder zusätzliche Informationen wünschen, erreichen Sie das Support Center von Teldat GmbH montags bis freitags von 8:00 bis 17:00 Uhr. Folgende Kontaktmöglichkeiten stehen Ihnen zur Verfügung:

Email hotline@teldat.de

Internationale Supportkoordinati-
on

Telefon: +49 911 9673 1550

Fax: +49 911 9673 1599

Endkunden-Hotline

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

Ausführliche Informationen zu unseren Support Leistungen erhalten Sie unter www.teldat.de.

3.9 WEEE-Information



The waste container symbol with the »X« through it on the device indicates that the device must be disposed of separately from normal domestic waste at an appropriate waste disposal facility at the end of its useful service life.



Das auf dem Gerät befindliche Symbol mit dem durchgekreuzten Müllcontainer bedeutet, dass das Gerät am Ende der Nutzungsdauer bei den hierfür vorgesehenen Entsorgungsstellen getrennt vom normalen Hausmüll zu entsorgen ist.



Le symbole se trouvant sur l'appareil et qui représente un conteneur à ordures barré signifie que l'appareil, une fois que sa durée d'utilisation a expiré, doit être éliminé dans des poubelles spéciales prévues à cet effet, de manière séparée des ordures ménagères courantes.



Il simbolo raffigurante il bidone della spazzatura barrato riportato sull'apparecchiatura significa che alla fine della durata in vita dell'apparecchiatura questa dovrà essere smaltita separatamente dai rifiuti domestici nei punti di raccolta previsti a tale scopo.



El símbolo del contenedor con la cruz, que se encuentra en el aparato, significa que cuando el equipo haya llegado al final de su vida útil, deberá ser llevado a los centros de recogida previstos, y que su tratamiento debe estar separado del de los residuos urbanos.



Symbolen som sitter på apparaten med den korsade avfallstunnan betyder att apparaten när den tjänat ut ska kasseras och lämnas till de förutsetta sortergårdarna och skiljas från normalt hushållsavfall.



Tegnet på apparatet som viser en avfallcontainer med et kryss over, betyr at apparatet må kastet på hertil egnet avfallssted og ikke sammen med vanlig avfall fra husholdningen.



Το σύμβολο που βρίσκεται στην συσκευή με το σταυρωμένο κοντέινερ απορριμμάτων σημαίνει, ότι η συσκευή στο τέλος της διάρκειας χρήσης της πρέπει να διατεθεί ξεχωριστά από τα κανονικά απορρίμματα στα γι' αυτό τον σκοπό προβλεπόμενα σημεία διάθεσης.



Symboliet med gennemkrydset affaldsbeholder på apparatet betyder, at apparatet, når det ikke kan bruges længere, skal bortskaffes adskilt fra normalt husholdningsaffald på et af de dertil regnede bortskaffelsessteder.



Znajdujący się na urządzeniu symbol przekreślonego pojemnika na śmieci oznacza, że po upływie żywotności urządzenia należy go oddać do odpowiedniej placówki utylizacyjnej i nie wyrzucać go do normalnych śmieci domowych.



Het doorgehaalde symbool van de afvalcontainer op het apparaat betekent dat het apparaat op het einde van zijn levensduur niet bij het normale huisvuil mag worden verwijderd. Het moet bij een erkend inzamelpunt worden ingeleverd.



O símbolo com um caixote de lixo riscado, que se encontra no aparelho, significa, que o aparelho no fim da sua vida útil deve ser eliminado separadamente do lixo doméstico nos centros de recolha adequados.

Kapitel 4 Grundkonfiguration

Zur Grundkonfiguration Ihres Geräts stehen der **Dime Manager** (IP-Adressvergabe) und das **GUI** (weitere Konfigurationsschritte) zur Verfügung.

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

Die Inhalte dieses Handbuches setzen die folgenden Basiskenntnisse voraus:

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

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

Weitere nützliche Applikationen finden Sie im Internet unter www.teldat.de.

4.1 Voreinstellungen

4.1.1 Vorkonfigurierte Daten

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

(a) Dynamische IP-Adresse

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

(b) Fallback-IP-Adresse

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

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

Achten Sie darauf, dass der PC, von dem aus die Konfiguration durchgeführt wird, über eine geeignete IP-Konfiguration verfügt (siehe dazu [PC einrichten](#) auf Seite 52).

(c) Feste IP-Adresse zuweisen

Mit dem **Dime Manager** können Sie Ihrem Gerät eine neue IP-Adresse und das gewünschte Passwort zuweisen.



Hinweis

Beachten Sie bitte:

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

Sollten sie dagegen bei der Erstkonfiguration eine Verbindung zum Gerät über die Fallback-IP-Adresse 192.168.0.252 aufgebaut 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.

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

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



Hinweis

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

Die Vorgehensweise bei der Änderung von Passwörtern finden Sie unter [Systempasswort ändern](#) auf Seite 56.

4.1.2 Software-Update

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

Eine Beschreibung des Update-Vorgangs finden Sie unter [Softwareaktualisierung](#) auf Seite 59

4.2 System-Voraussetzungen

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

- Internet Explorer oder Mozilla Firefox
- Installierte Netzwerkkarte (Ethernet)
- DVD-Laufwerk
- Installiertes TCP/IP-Protokoll (siehe [PC einrichten](#) auf Seite 52)

4.3 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

- die benötigten Daten für die Grundkonfiguration bereitlegen.
- überprüfen, ob der PC, von dem aus Sie die Konfiguration vornehmen wollen, die notwendigen Voraussetzungen erfüllt.
- die **Dime Manager**-Software installieren, die Ihnen weitere Werkzeuge zur Arbeit mit Ihrem Gerät zur Verfügung stellt.

4.3.1 Daten sammeln

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

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

- IP-Konfiguration (obligatorisch sofern sich Ihr Gerät im Auslieferungszustand befindet)



Hinweis

Die Geräte **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** unterstützen kein WDS, kein Bridgeling und kein Client-Modus.

- optional: Konfiguration einer drahtlosen Netzwerkverbindung im Access-Point-Modus
- optional: Konfiguration von Client Links im Client Links-Modus

- optional: Konfiguration von Bridge-Links im Bridge-Modus.

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

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

Grundkonfiguration

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

IP-Konfiguration des Access Points

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

Access-Point-Modus

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

Konfiguration eines Drahtlosnetzwerks

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

Access Client-Modus

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

IP-Konfiguration des Access Clients

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

Bridge-Modus

Wenn Sie Ihr Gerät im Bridge-Modus betreiben, können Sie entweder manuell Verbindungen zu anderen Bridges konfigurieren oder die Bridge-Link-Autokonfigurationsfunktion verwenden. Für die manuelle Konfiguration eines Bridge-Links benötigen Sie die folgenden Daten:

Konfiguration eines Bridge-Links

Zugangsdaten	Beispielwert	Ihre Werte
Preshared Key	<i>bridgesecret</i>	
MAC-Adresse der entfernten Bridge	<i>00:a0:f9:5a:42:53</i>	

Zur Verwendung der Bridge-Link-Autokonfigurationsfunktion gehen Sie bitte vor wie im **Workshop WLAN-Automatischer Aufbau eines Bridge-Links** beschrieben und lesen Sie für weiterführende Informationen auch im Handbuchkapitel **Wireless LAN** unter **WLAN->Bridge-Links->Neu**.

4.3.2 PC einrichten

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

- Stellen Sie sicher, dass das TCP/IP-Protokoll auf dem PC installiert ist.
- Wählen Sie die geeignete IP-Konfiguration für Ihren Konfigurations-PC.

Der PC, über den Sie die IP-Adresse für Ihr Gerät konfigurieren möchten, muss sich im gleichen Netzwerk wie das zu konfigurierende Gerät befinden.

Windows TCP/IP-Protokoll prüfen

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

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

Windows TCP/IP-Protokoll installieren

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

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

PC IP-Adresse zuweisen

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

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

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

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

4.4 IP-Konfiguration

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

Alternativ können Sie Ihrem Geräten die gewünschte feste IP-Adresse zuweisen, indem Sie den **Dime Manager** benutzen.

Installieren Sie dazu das Programm von der mitgelieferten DVD auf Ihren Konfigurations-PC.

Gehen Sie dazu vor wie folgt:

- (a) Legen Sie die mitgelieferte DVD in das DVD-Laufwerk Ihres Konfigurations-PCs. Der

Installationsassistent startet automatisch. Sollte das nicht der Fall sein, öffnen Sie auf der DVD über Ihren Dateibrowser die Datei `starter.exe`.

- (b) Folgen Sie den Anweisungen des Installations-Assistenten.

Führen Sie anschliessend folgende Schritte aus, um eine IP-Adresse für Ihr Gerät zu konfigurieren:

- (1) Starten Sie den **Dime Manager** aus dem Windows-Startmenü **Start -> Programme -> Teldat-> Dime Manager**.

Es erscheint folgendes Dialogfeld:

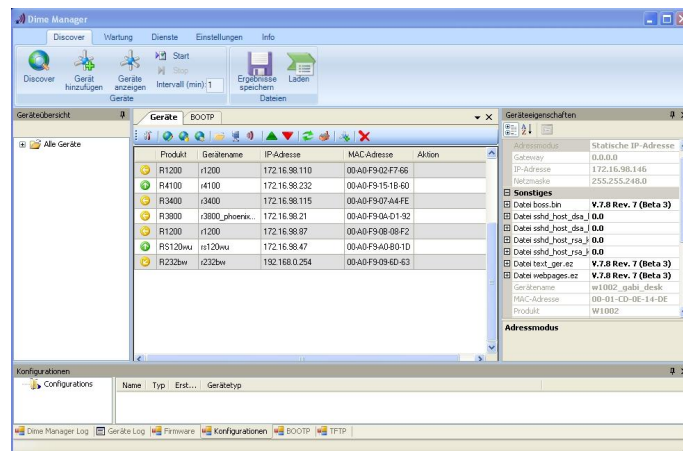


Abb. 28: **Dime Manager** Startseite

Der **Dime Manager** erkennt die im Netzwerk installierten Geräte.

- (2) Doppelklicken Sie in der Liste das Gerätes, das konfiguriert werden soll.
Es erscheint folgendes Dialogfeld:



Abb. 29: IP-Adressvergabe mit dem **Dimet Manager**

- (3) Geben Sie die Netzwerkparameter (**Gerätename**, **IP-Adresse**, **Netzmaske** und **Gateway**) ein und bestätigen Sie Ihre Angaben mit **OK**.



Hinweis

Der Parameter **Gerätename** darf maximal aus 32 Zeichen bestehen.

Der Parameter **Gerätename** darf nur aus Buchstaben „a“-“z“, „A“-“Z“, Ziffern „0“-“9“, Bindestrich „-“ und Punkt „.“ bestehen, um Fehler durch andere Systeme bei der Interpretation des Parameters **Gerätename** zu vermeiden. Das erste Zeichen muss ein Buchstabe sein, das letzte Zeichen darf kein Punkt „.“ und kein Minuszeichen „-“ sein, ein einzelnes Zeichen ist als Name nicht zulässig.

Ihr Gerät ist nun über das Ethernet mit seiner IP-Adresse über einen Web-Browser ansprechbar und kann jetzt konfiguriert werden.

GUI aufrufen

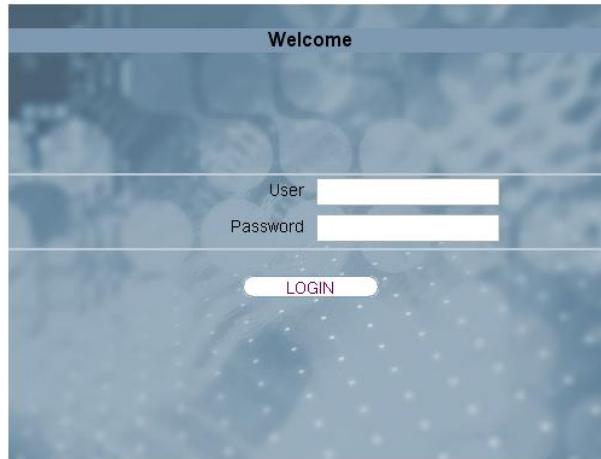


Abb. 30: GUI Login

Starten Sie die Konfigurationsoberfläche wie folgt:

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

Mit DHCP-Server:

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

Ohne DHCP-Server:

- Bei Direktanschluss an den Konfigurations-PC: die Fallback-IP-Adresse
192.168.0.252
- Die über den **Dime Manager** vergebene feste IP-Adresse

Drücken Sie die **Eingabetaste**.

- (b) Geben Sie in das Feld **User** *admin* und in das Feld **Password** *admin* ein.

4.5 Systempasswort ändern

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

Gehen Sie dazu vor wie folgt:

- Gehen Sie in das Menü **Systemverwaltung** -> **Globale Einstellungen** -> **Passwörter**.
- Geben Sie für **Systemadministrator-Passwort** ein neues Passwort ein.
- Geben Sie das neue Passwort noch einmal unter **Systemadministrator-Passwort**

bestätigen ein.

- (d) Klicken Sie auf **OK**.
- (e) Speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

Beachten Sie folgende Regeln zum Passwortgebrauch:

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

4.6 Drahtlosnetzwerk einrichten

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

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

WLAN-Adapter unter Windows XP konfigurieren

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

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

Fahren Sie folgendermaßen fort:

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

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



Hinweis

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

WLAN-Adapter unter Windows 7 konfigurieren

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


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

4.7 Bridge Link einrichten

Wenn Sie Ihr Gerät im Bridge-Modus betreiben, müssen Sie einen Bridge Link einrichten.

Für **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** nicht verfügbar.



Bridge-Link-Autokonfiguration

- (1) Gehen Sie zu **Wireless LAN->WLAN->Einstellungen Funkmodul->** .
- (2) Wählen Sie in **Betriebsmodus** *Bridge* aus.
- (3) Belassen Sie in allen anderen Feldern die Standardeinstellungen.
- (4) Klicken Sie auf **OK**.
- (5) Gehen Sie zu **Wireless LAN->WLAN->Bridge-Links->Neu**.
- (6) Geben Sie bei **Preshared Key** z. B. *bridgesecret* ein.
- (7) Belassen Sie in allen anderen Feldern die Standardeinstellungen.
- (8) Klicken Sie auf **OK**.
- (9) Konfigurieren Sie analog einen Bridge-Link auf dem entfernten Gerät.

- (10) Klicken Sie bei Ihrem lokalen Gerät in der Liste in **Wireless LAN->WLAN->Bridge-Links** auf das Symbol .
- (11) Klicken Sie im sich öffnenden Menü **Wireless LAN->WLAN->Bridge-Links->** unter **Aktion** auf die Verknüpfung *Scan*.
- (12) Nach dem Scan werden die Ergebnisse aufgelistet. Klicken Sie bei dem gewünschten Listeneintrag auf die Verknüpfung *Verbinden*.
- (13) Speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

Zur Verwendung der Bridge-Link-Autokonfigurationsfunktion lesen Sie bitte auch den **Workshop WLAN-Automatischer Aufbau eines Bridge-Links** und für weiterführende Informationen auch im Handbuchkapitel **Wireless LAN** unter **WLAN->Bridge-Links->Neu**.

Manuelle Konfiguration

- (1) Gehen Sie zu **Wireless LAN->WLAN->Einstellungen Funkmodul->**.
- (2) Wählen Sie in **Betriebsmodus** *Bridge* aus.
- (3) Belassen Sie in allen anderen Feldern die Standardeinstellungen.
- (4) Klicken Sie auf **OK**.
- (5) Gehen Sie zu **Wireless LAN->WLAN->Bridge-Links->**.
- (6) Geben Sie bei **Preshared Key** z. B. *bridgesecret* ein.
- (7) Geben Sie bei **Entfernte MAC-Adresse** die MAC-Adresse der Bridge ein, zu der Ihre Bridge eine Verbindung aufbauen soll, z. B. *00:a0:f9:5a:42:53*.
- (8) Belassen Sie in allen anderen Feldern die Standardeinstellungen.
- (9) Klicken Sie auf **OK**.
- (10) Konfigurieren Sie analog einen Bridge-Link auf dem entfernten Gerät.
- (11) Speichern Sie die Konfiguration mit der Schaltfläche **Konfiguration speichern** oberhalb der Menünavigation.

Nach Abschluss der Konfiguration ist Ihr Gerät einsatzbereit.

Die Konfiguration des Geräts und die Einbindung in Ihr Netzwerk sind damit abgeschlossen.

4.8 Softwareaktualisierung

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

Gehen Sie folgendermaßen vor:

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

Optionen

Aktuell installierte Software	
BOSS	V.9.1 Rev. 2 IPSec from 2011/06/10 00:00:00
Systemlogik	0.0
Optionen zu Software und Konfiguration	
Aktion	Systemsoftware aktualisieren
Quelle	Aktuelle Software vom Teldat-Server

Los

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



Achtung

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

Kapitel 5 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

5.1 Zugangsmöglichkeiten

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

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

- Über Ihr LAN
- Über die serielle Schnittstelle

5.1.1 Zugang über LAN

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



Achtung

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

5.1.1.1 HTTP/HTTPS

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

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

Mit DHCP-Server:

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

Ohne DHCP-Server:

- Bei Direktanschluss an den Konfigurations-PC: die Fallback-IP-Adresse
`192.168.0.252`
- Die über den **Dime Manager** vergebene feste IP-Adresse

Drücken Sie die **Eingabetaste**.

5.1.1.2 Telnet

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

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

Gehen Sie folgendermaßen vor:

Windows

- (1) Klicken Sie im Windows-Startmenü auf **Ausführen...**
- (2) Geben Sie `telnet <IP-Adresse Ihres Geräts>` ein.
- (3) Klicken Sie auf **OK**.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (4) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 67.

Unix

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

- (1) Geben Sie `telnet <IP-Adresse Ihres Geräts>` in ein Terminal ein.
Es öffnet sich ein Fenster mit dem Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.
- (2) Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 67.

5.1.1.3 SSH

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

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

- Auf dem Gerät müssen für den Vorgang benötigte Verschlüsselungsschlüssel vorhanden sein.

- Auf Ihrem PC muss ein SSH-Client installiert sein.

Schlüssel zur Verschlüsselung

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

- (1) Loggen Sie sich auf eine der bereits verfügbaren Arten auf Ihrem Gerät ein (z. B. über Telnet - zum Login siehe [Anmelden](#) auf Seite 66).
- (2) Am Eingabe-Prompt geben Sie `update -i` ein. Sie befinden sich auf der Flash Management Shell.
- (3) Rufen Sie eine Liste aller auf dem Gerät gespeicherten Dateien auf: `ls -al`.

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

```
Flash-Sh > ls -al

Flags Version Length Date Name...

Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860

Vrw-pl--f 0.0 350 2004/09/07 10:44:14 sshd_host_rsa_key.pub

Vrw-pl--f 0.0 1011 2004/09/07 10:44:12 sshd_host_rsa_key

Vrw-pl--f 0.0.01 730 2004/09/07 10:42:17 sshd_host_dsa_key.pub

Vrw-pl--f 0.0.01 796 2004/09/07 10:42:16 sshd_host_dsa_key

Flash-Sh >
```



Hinweis

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

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

- (1) Verlassen Sie die Flash Management Shell mit `exit`.
- (2) Rufen Sie das **GUI** auf und melden Sie sich an Ihrem Gerät an (siehe [Das GUI aufrufen](#) auf Seite 70).
- (3) Stellen Sie sicher, dass als Sprache *Deutsch* gewählt ist.
- (4) Kontrollieren Sie den Schlüsselstatus im Menü **Systemverwaltung** -> **Administrativer**

Zugriff->SSH. Wenn beide Schlüssel verfügbar sind, sehen Sie in den beiden Feldern **RSA-Schlüsselstatus** und **DSA-Schlüsselstatus** den Wert *Generiert*.

- (5) Wenn Sie in einem der beiden Felder oder in beiden Feldern den Wert *Nicht generiert* sehen, so müssen Sie den entsprechenden Schlüssel erzeugen lassen. Um die Schlüssel vom Gerät erzeugen zu lassen, klicken Sie auf **Generieren**.
Das Gerät erzeugt den entsprechenden Schlüssel und speichert ihn im FlashROM. *Generiert* zeigt die erfolgreiche Generierung an.
- (6) Stellen Sie sicher, dass beide Schlüssel erfolgreich erzeugt worden sind. Wiederholen Sie dazu gegebenenfalls die oben beschriebene Prozedur.

Login über SSH

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

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

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

UNIX

- (1) Geben Sie `ssh <IP-Adresse des Geräts>` in einem Terminal ein.
Das Login-Prompt-Fenster wird angezeigt, sie befinden sich auf der SNMP-Shell des Geräts.
- (2) Fahren Sie mit [Anmelden](#) auf Seite 66 fort.

Windows

- (1) Wie eine SSH-Verbindung aufgebaut wird, hängt stark von der verwendeten Software ab. Beachten Sie die Dokumentation des von Ihnen verwendeten Programms.
Sobald Sie sich mit dem Gerät verbunden haben, wird das Login-Prompt-Fenster angezeigt. Sie befinden sich auf der SNMP-Shell des Geräts.
- (2) Fahren Sie mit [Anmelden](#) auf Seite 66 fort.



Hinweis

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

5.1.2 Zugang über die serielle Schnittstelle

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

Der Zugang über die serielle Schnittstelle ist gut geeignet, wenn Sie bei Ihrem Gerät eine Erstkonfiguration durchführen und ein LAN-Zugang über die vorkonfigurierte IP-Adresse (192.168.0.252/255.255.255.0) nicht möglich ist.

Windows

Um Ihr Gerät über die serielle Schnittstelle an Ihren Rechner anzuschließen, gehen Sie vor wie in der *Inbetriebnahme* auf **Seite 6** beschrieben.

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

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

- (1) Klicken Sie im Windows-Startmenü auf **Programme** -> **Zubehör** -> **HyperTerminal**.
- (2) Drücken Sie die **Eingabetaste** (evtl. mehrmals), wenn sich das HyperTerminal-Fenster geöffnet hat.

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

Überprüfen

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

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

- (1) Klicken Sie auf **Datei** -> **Eigenschaften**.
- (2) Klicken Sie im Register **Verbinden mit** auf **Konfigurieren**
Folgende Einstellungen sind erforderlich:
 - Bits pro Sekunde: 9600
 - Datenbits: 8

- Parität: *Keiner*
- Stopbits: *1*
- Flusststeuerung: *Keiner*

- (3) Tragen Sie die Werte ein und klicken Sie auf **OK**.
- (4) Stellen Sie im Register **Einstellungen** ein:
 - Emulation: *VT100*
- (5) Klicken Sie auf **OK**.

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

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

Unix

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

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

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

5.2 Anmelden

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

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

5.2.1 Benutzernamen und Passwörter im Auslieferungszustand

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

Benutzernamen und Passwörter im Auslieferungszustand

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

Um Konfigurationsänderungen vorzunehmen und zu speichern, müssen Sie sich mit dem Benutzernamen `admin` einloggen. Auch die Zugangsdaten (Benutzernamen und Passwörter) können geändert werden, wenn sich der Benutzer mit dem Benutzernamen `admin` einloggt. Aus Sicherheitsgründen sind Passwörter im Setup Tool nicht im Klartext, sondern nur als Sternchen am Bildschirm sichtbar. Die Benutzernamen erscheinen hingegen im Klartext.

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



Achtung

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

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

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

5.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in [Zugangsmöglichkeiten](#) auf Seite 61 beschrieben.

GUI (Graphical User Interface)

So loggen Sie sich über die HTML-Oberfläche ein:

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

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

SNMP-Shell

So loggen Sie sich auf der SNMP-Shell ein:

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

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

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

5.3 Konfigurationsmöglichkeiten

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

Sie haben folgende Möglichkeiten, Ihr Gerät zu konfigurieren:

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

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

Verbindungs- und Konfigurationsarten

Verbindungsart	Mögliche Konfigurationsarten
LAN	Assistent, GUI , Shell-Kommandos
Serielle Verbindung	Shell-Kommandos

Es stehen also für jede Verbindungsart mehrere Konfigurationsarten zur Verfügung.



Hinweis

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

5.3.1 GUI (Graphical User Interface) für Fortgeschrittene

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

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

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

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

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

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen		
! Warnung: Systempasswort nicht geändert! ! [warning_boss_lang]		
Systeminformationen		
Uptime	0 Tag(e) 4 Stunde(n) 57 Minute(n)	
Systemdatum	Donnerstag, 25 Mär 2004, 15:42:45	
Seriennummer	WN2DJC010290024	
BOSS-Version	V.9.1 Rev. 2 IPSec from 2012/04/19 00:00:00	
Letzte gespeicherte Konfiguration	Donnerstag, 01 Jan 1970, 00:00:00	
Ressourceninformationen		
CPU-Nutzung	0%	
Arbeitsspeichernutzung	20.5/31.9 MByte (64%)	
Temperatur	Aktuell: 42°C / Min.: 38°C / Max.: 43°C	
Aktive Sitzungen (SIF, RTP, etc...)	0	
Aktive IPSec-Tunnel	0 / 0	
Physikalische Schnittstellen		
Schnittstelle	Verbindungsinformation	Link
en1-0	br0: 192.168.0.252 / 255.255.255.0	🟢
en1-1	br0: 192.168.0.252 / 255.255.255.0	🔴
WLAN1	Bridge / Verwendeter Kanal 1 / 1 BR Link / FW: 2.0.0.0	🟢
WLAN2	Aus	🔴
Relais	Modus: Inaktiv	🔴
WAN-Schnittstellen		
Beschreibung	Verbindungsinformation	Link

Abb. 31: GUI Startseite

5.3.1.1 Das GUI aufrufen

- (1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind.
- (2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe *PC einrichten* auf Seite 52).
- (3) Öffnen Sie einen Web-Browser.
- (4) Geben Sie `http://192.168.0.252` (oder die von Ihrem DHCP-Server dynamisch vergebene IP-Adresse oder die von Ihnen statisch mit dem **Dime Manager** vergebene IP-Adresse) in das Adressfeld des Web-Browsers ein.
- (5) Geben Sie in das Feld **User** `admin` und in das Feld **Password** `admin` ein und klicken Sie auf **LOGIN**.

Sie befinden sich nun im Statusmenü des **GUI** Ihres Geräts (siehe *Status* auf Seite 83).

5.3.1.2 Bedienelemente

GUI-Fenster

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

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

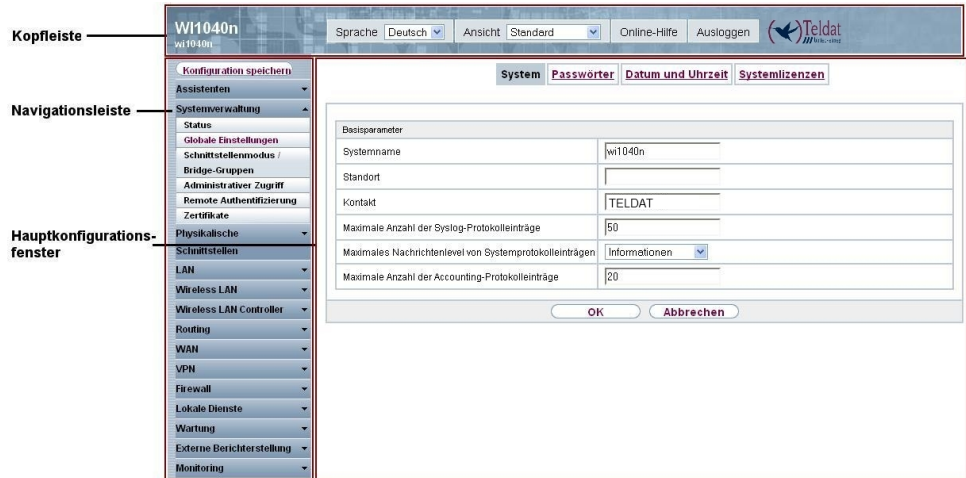


Abb. 32: Bereiche des **GUI**

Kopfleiste



Abb. 33: **GUI** Kopfleiste

GUI Kopfleiste

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

Menü	Funktion
Online-Hilfe	Online-Hilfe: Klicken Sie auf diese Schaltfläche, wenn Sie zu dem gerade aktiven Menü Hilfe benötigen. Die Beschreibung des Untermenüs, in dem Sie sich gerade befinden, wird angezeigt.
Ausloggen	<p>Ausloggen: Wenn Sie die Konfiguration beenden möchten, klicken Sie auf diese Schaltfläche, um sich von Ihrem Gerät abzumelden. Es wird ein Fenster geöffnet, in dem Ihnen folgende Optionen angeboten werden:</p> <ul style="list-style-type: none"> • Konfiguration speichern, vorherige Boot-Konfiguration sichern, dann verlassen. • Konfiguration speichern, dann verlassen. • Ohne zu speichern verlassen.

Navigationsleiste



Abb. 34: Konfiguration speichern Schaltfläche



Abb. 35: Menüs

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

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

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

Sie haben folgende zwei Wahlmöglichkeiten:

- *Konfiguration speichern*, d.h. aktuelle Konfiguration als Boot-Konfiguration speichern
- *Konfiguration speichern und vorhergehende Boot-Konfiguration sichern*, d.h. aktuelle Konfiguration als Boot-Konfiguration speichern und zusätzlich vor-

hergehende Boot-Konfiguration als Backup archivieren.

Wenn Sie die archivierte Boot-Konfiguration in Ihr Gerät laden wollen, gehen Sie in das Menü **Wartung->Software & Konfiguration**, wählen Sie **Aktion = Konfiguration importieren** und klicken Sie auf **Los**. Das archivierte Backup wird als aktuelle Boot-Konfiguration verwendet.

Die Navigationsleiste enthält weiterhin die Hauptkonfigurationsmenüs und deren Untermenüs.

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

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

Statusseite

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






Hauptkonfigurationsfenster


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

Konfigurationselemente



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

GUI Schaltflächen

Schaltfläche	Funktion
	Aktualisiert die Ansicht.
	Wenn Sie einen neu konfigurierten Listeneintrag nicht sichern wollen, machen Sie diesen und die evtl. getätigten Einstellungen durch Abbrechen rückgängig.
	Bestätigt die Einstellungen eines neuen Eintrags und die Parameteränderungen in einer Liste.
	Startet die konfigurierte Aktion sofort.
	Ruft das Untermenü zum Anlegen eines neuen Eintrags auf.








Schaltfläche	Funktion
	Fügt einen Eintrag zu einer internen Liste hinzu.






GUI Schaltflächen für spezielle Funktionen

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

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

GUI Symbole

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

Symbol	Funktion
	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.

In der Listenansicht haben Sie folgende Bedienfunktionen zur Auswahl:

GUI Listenoptionen

Menü	Funktion
Aktualisierungsintervall	<p>Hier können Sie das Intervall einstellen, in dem die Ansicht aktualisiert werden soll.</p> <p>Geben Sie dazu einen Zeitraum in Sekunden in das Eingabefeld ein und bestätigen Sie mit Übernehmen.</p>
Filter	<p>Sie haben die Möglichkeit, die Einträge einer Liste nach bestimmten Kriterien filtern und entsprechend anzeigen zu lassen.</p> <p>Sie können die Anzahl der pro Seite angezeigten Einträge bestimmen, indem Sie in Ansicht x pro Seite die gewünschte Zahl eingeben.</p> <p>Mit den Tasten  und  blättern Sie eine Seite vor bzw. eine Seite zurück.</p> <p>Sie können nach bestimmten Stichwörtern innerhalb der Konfigurationsparameter filtern, indem Sie bei Filtern in x <Option> y die gewünschte Filterregel auswählen und das Suchwort in das Eingabefeld eingeben. Los startet den Filtervorgang.</p>
Konfigurationselemente	<p>Einige Listen enthalten Konfigurationselemente.</p> <p>So können Sie direkt in der Liste die Konfiguration des entsprechenden Listeneintrags ändern.</p>

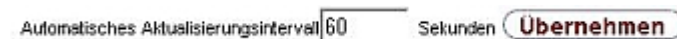


Abb. 36: Konfiguration des Aktualisierungsintervalls






Abb. 37: Liste filtern

Struktur der GUI Konfigurationsmenüs



Die Menüs des **GUI** enthalten folgende Grundstrukturen:





GUI Menüstruktur

Menü	Funktion
Basis-Konfigurationsmenü/Liste	Bei Auswahl eines Menüs der Navigationsleiste wird zunächst das Menü mit den Basisparametern angezeigt. Bei einem Untermenü mit mehreren Seiten wird jeweils das Menü mit den Basisparametern der ersten Seite angezeigt. Das Menü enthält entweder eine Liste aller konfigurierten Einträge oder die Grundeinstellungen für die jeweilige Funktion.
Untermenü 	Die Schaltfläche Neu ist in jedem Menü vorhanden, in dem eine Liste aller konfigurierten Einträgen angezeigt wird. Klicken Sie diese Schaltfläche, um das Konfigurationsmenü für das Anlegen eines neuen Listeneintrags aufzurufen.
Untermenü 	Klicken Sie auf diese Schaltfläche, um den bestehenden Listeneintrag zu bearbeiten. Sie gelangen in das Konfigurationsmenü.
Menü 	Klicken Sie auf diesen Reiter, um erweiterte Konfigurationsoptionen anzuzeigen.

Für die Konfiguration stehen folgende Optionen zur Verfügung:

GUI Konfigurationselemente

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

Menü	Funktion									
	<table border="1"> <tr> <td>IP-Adressmodus</td> <td><input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse abrufen</td> </tr> </table> <p>Wählen Sie die entsprechende Option aus.</p>	IP-Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse abrufen							
IP-Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse abrufen									
Checkboxen	<p>z. B. Aktivieren durch Auswahl der Checkbox</p> <p><input checked="" type="checkbox"/> Aktiviert</p> <p>Auswahl verschiedener möglicher Optionen</p> <table border="1"> <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"/> RipeMD160</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"/> RipeMD160					
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"/> RipeMD160									
Dropdown-Menüs	<p>z. B.</p> <table border="1"> <tr><td>Vollständige automatische Aushandlung</td></tr> <tr><td>Vollständige automatische Aushandlung</td></tr> <tr><td>Vollständige automatische Aushandlung</td></tr> <tr><td>Vollständige automatische Aushandlung</td></tr> </table> <p>Klicken Sie auf den Pfeil, um die Liste zu öffnen. Wählen Sie die gewünschte Option mit der Maus.</p>	Vollständige automatische Aushandlung	Vollständige automatische Aushandlung	Vollständige automatische Aushandlung	Vollständige automatische Aushandlung					
Vollständige automatische Aushandlung										
Vollständige automatische Aushandlung										
Vollständige automatische Aushandlung										
Vollständige automatische Aushandlung										
Interne Listen	<p>z. B.</p> <table border="1"> <tr> <td>IP-Adresse</td> <td>Netzmaske</td> <td></td> </tr> <tr> <td></td> <td>255.255.255.0</td> <td></td> </tr> <tr> <td colspan="3"><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>	IP-Adresse	Netzmaske			255.255.255.0		<input type="button" value="Hinzufügen"/>		
IP-Adresse	Netzmaske									
	255.255.255.0									
<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 stattdessen grau dargestellt und sind nicht auswählbar.



Wichtig

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

Warnsymbole

Symbol	Bedeutung
	Dieses Symbol erscheint in Meldungen, die Sie auf Einstellungen hinweisen, die mit dem Setup Tool vorgenommen wurden.
	Dieses Symbol erscheint in Meldungen, die Sie darauf hinweisen, dass Werte falsch eingegeben bzw. ausgewählt wurden.
Achten Sie besonders auf folgenden Hinweis:	
"Warnung: Nicht unterstützte Änderungen durch das Setup-Tool!". Falls Sie sie mit dem GUI verändern, kann dies Inkonsistenzen oder Fehlfunktionen verursachen. Daher wird empfohlen, die Konfiguration mit dem Setup Tool fortzuführen.	

5.3.1.3 GUI Menüs

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



Hinweis

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

5.3.2 SNMP-Shell

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

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

5.4 BOOTmonitor

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

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

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

Beim Hochfahren durchläuft das Gerät verschiedene Funktionszustände:

- Start-Modus
- BOOTmonitor-Modus
- Normaler Betriebsmodus

Nachdem im Start-Modus einige Selbsttests erfolgreich ausgeführt wurden, erreicht Ihr Gerät den BOOTmonitor-Modus. Der BOOTmonitor-Prompt wird angezeigt, falls Sie seriell mit Ihrem Gerät verbunden sind.

```
Press <sp> for boot monitor or any other key to boot system
```

```
W1002 Bootmonitor V.7.9.1 Rev. 1 from 2009/10/19 00:00:00  
Copyright (c) 1996-2005 by Teldat GmbH
```

- (1) Boot System
- (2) Software Update via TFTP
- (3) Software Update via XMODEM
- (4) Delete Configuration
- (5) Default Bootmonitor Parameters
- (6) Show System Information

```
Your Choice> _
```

Abb. 38: BOOTmonitor

Betätigen Sie nach Anzeige des BOOTmonitor-Prompts innerhalb von vier Sekunden die Leertaste, um die Funktionen des BOOTmonitors zu nutzen. Wenn Sie keine Eingabe machen, wechselt das Gerät nach Ablauf der vier Sekunden in den normalen Betriebs-Modus.



Hinweis

Wenn Sie die Baudrate verändern (voreingestellt ist 9600 Baud), achten Sie darauf, dass das verwendete Terminalprogramm diese Baudrate verwendet. Wenn dies nicht der Fall ist, können Sie keine serielle Verbindung zum Gerät herstellen!

Kapitel 6 Assistenten

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

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

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

Kapitel 7 Systemverwaltung

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

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

7.1 Status

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

Sie erhalten einen Überblick über folgende Daten:

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

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



Achtung

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

Automatisches Aktualisierungsintervall	60	Sekunden	Übernehmen
! Warnung: Systempasswort nicht geändert! ! [warning_boss_lang]			
Systeminformationen			
Uptime	0 Tag(e) 4 Stunde(n) 57 Minute(n)		
Systemdatum	Donnerstag, 25 Mär 2004, 15:42:45		
Seriennummer	WN2DJC010290024		
BOSS-Version	V.9.1 Rev. 2 IPSec from 2012/04/19 00:00:00		
Letzte gespeicherte Konfiguration	Donnerstag, 01 Jan 1970, 00:00:00		
Ressourceninformationen			
CPU-Nutzung	0%		
Arbeitsspeichernutzung	20.5/31.9 MByte (64%)		
Temperatur	Aktuell: 42°C / Min.: 38°C / Max.: 43°C		
Aktive Sitzungen (SIF, RTP, etc...)	0		
Aktive IPSec-Tunnel	0 / 0		
Physikalische Schnittstellen			
Schnittstelle	Verbindungsinformation	Link	
en1-0	br0: 192.168.0.252 / 255.255.255.0		
en1-1	br0: 192.168.0.252 / 255.255.255.0		
WLAN1	Bridge / Verwendeter Kanal 1 / 1 BR Link / FW: 2.0.0.0		
WLAN2	Aus		
Relais	Modus: Inaktiv		
WAN-Schnittstellen			
Beschreibung	Verbindungsinformation	Link	

Abb. 39: 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 (Boot-Konfiguration im Flash) an.

Felder im Menü Ressourceninformationen

Feld	Wert
CPU-Nutzung	Zeigt die CPU-Auslastung in Prozent an.
Arbeitsspeichernutzung	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtarbeitsspeicher in MByte an. Die Auslastung

Feld	Wert
	tung wird außerdem in Klammern in Prozent angezeigt.
Temperatur	Die Geräte der bintec WI -Serie sind mit einem Temperatur-Sensor ausgestattet. Hier wird die aktuelle Temperatur, sowie die erreichte Minimal- und Maximaltemperatur angezeigt.
Aktive Sitzungen (SIF, RTP, etc...)	Zeigt die Summe aller SIF-, TDRC- und IP-Lastverteilung Sessions an.
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Felder im Menü **Physikalische Schnittstellen**

Feld	Wert
Schnittstelle - Verbindungsinformation - Link	<p>Hier sind alle physikalischen Schnittstellen aufgelistet und deren wichtigste Einstellungen genannt. Außerdem wird angezeigt, ob die jeweilige Schnittstelle angeschlossen bzw. aktiv ist.</p> <p>Schnittstellendetails für Ethernet-Schnittstellen:</p> <ul style="list-style-type: none"> • IP-Adresse • Netzmaske <p>Schnittstellendetails für serielle Schnittstellen / ISDN-Schnittstellen:</p> <ul style="list-style-type: none"> • Konfiguriert • Nicht konfiguriert <p>Schnittstellendetails für xDSL-Schnittstellen:</p> <ul style="list-style-type: none"> • Leitungsgeschwindigkeit Downstream/Upstream <p>Schnittstellendetails für WLAN-Schnittstellen:</p> <p>Access-Point-Modus:</p> <ul style="list-style-type: none"> • Betriebsmodus: Access Point oder Aus • Der auf diesem Funkmodul verwendete Kanal • Anzahl der verbundenen Clients • Anzahl der WDS-Links <p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p>

Feld	Wert
	<ul style="list-style-type: none"> • Softwareversion der Funkkarte <p>Access Client-Modus:</p> <p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <ul style="list-style-type: none"> • Betriebsmodus: Access Client oder Aus • Der auf diesem Funkmodul verwendete Kanal • Softwareversion der Funkkarte <p>Bridge-Modus:</p> <p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <ul style="list-style-type: none"> • Betriebsmodus: Bridge oder Aus • Der auf diesem Funkmodul verwendete Kanal • Anzahl der konfigurierten Bridge-Links • Softwareversion der Funkkarte <p>Schnittstellendetails für Relais:</p> <ul style="list-style-type: none"> • Konfigurierter Modus

Felder im Menü WAN-Schnittstellen

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

7.2 Globale Einstellungen

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

7.2.1 System

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

System
Passwörter
Datum und Uhrzeit
Systemlizenzen

Grundeinstellungen	
Systemname	<input type="text" value="Produktname"/>
Standort	<input type="text"/>
Kontakt	<input type="text" value="TEL DAT"/>
Maximale Anzahl der Syslog-Protokolleinträge	<input type="text" value="50"/>
Maximales Nachrichtenlevel von Systemprotokolleinträgen	<input type="text" value="Informationen"/>
Maximale Anzahl der Accounting-Protokolleinträge	<input type="text" value="20"/>
Manuelle IP-Adresse des WLAN-Controller	<input type="text"/>
LED-Modus	<input type="text" value="Status"/>

OK
Abbrechen

Abb. 40: 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. Dieser wird auch als PPP-Host-Name benutzt.</p> <p>Möglich ist eine Zeichenkette mit maximal 255 Zeichen.</p> <p>Als Standardwert ist der Gerätetyp voreingestellt.</p>
Standort	<p>Geben Sie an, wo sich Ihr Gerät befindet.</p>
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 maximal 255 Zeichen.</p> <p>Standardwert ist <i>TEL DAT</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>Standardwert ist <i>50</i>.</p>

Feld	Wert
	<p>Sie können die gespeicherten Meldungen in Monitoring->Internes Protokoll anzeigen lassen.</p>
<p>Maximales Nachrichtenlevel von Systemprotokolleinträgen</p>	<p>Wählen Sie die Priorität der Systemmeldungen aus, ab der protokolliert werden soll.</p> <p>Nur Systemmeldungen mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass bei der Priorität <i>Debug</i> sämtliche erzeugten Meldungen aufgezeichnet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i>: Es werden nur Meldungen mit der Priorität Notfall aufgezeichnet. • <i>Alarm</i>: Es werden Meldungen mit der Priorität Notfall und Alarm aufgezeichnet. • <i>Kritisch</i>: Es werden Meldungen mit der Priorität Notfall, Alarm und Kritisch aufgezeichnet. • <i>Fehler</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch und Fehler aufgezeichnet. • <i>Warnung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler und Warnung aufgezeichnet. • <i>Benachrichtigung</i>: Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung und Benachrichtigung aufgezeichnet. • <i>Informationen</i> (Standardwert): Es werden Meldungen mit der Priorität Notfall, Alarm, Kritisch, Fehler, Warnung, Benachrichtigung und Informationen aufgezeichnet. • <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.
<p>Maximale Anzahl der Accounting-Protokolleinträge</p>	<p>Geben Sie die maximale Anzahl an Einträgen an, die für Login-Vorgänge auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000</i>.</p> <p>Standardwert ist <i>20</i>.</p>
<p>Manuelle IP-Adresse des WLAN-Controller</p>	<p>Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar.</p>

Feld	Wert
	<p>Geben Sie die IP-Adresse des WLAN-Controllers an.</p> <p>Der Wert kann nur verändert werden, wenn die WLAN-Controller-Funktion aktiviert ist.</p>
LED-Modus	<p>Diese Funktion ist nur für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n verfügbar.</p> <p>Wählen Sie das Leuchtverhalten der LEDs.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Status</i> (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde. • <i>Blinkend</i>: Die LEDs zeigen ihr Standardverhalten. • <i>Aus</i>: Alle LEDs sind deaktiviert.

7.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

System **Passwörter** Datum und Uhrzeit Systemlizenzen

Systempasswort	
Systemadministrator-Passwort	<input type="password" value="....."/>
Systemadministrator-Passwort bestätigen	<input type="password" value="....."/>
SNMP-Communities	
SNMP Read Community	<input type="password" value="....."/>
SNMP Write Community	<input type="password" value="....."/>
Globale Passwortoptionen	
Passwörter und Schlüssel als Klartext anzeigen	<input type="button" value="Anzeigen"/>

Abb. 41: Systemverwaltung ->Globale Einstellungen->Passwörter



Hinweis

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

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

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

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

Felder im Menü Systempasswort

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

Felder im Menü SNMP-Communities

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

Feld im Menü Globale Passwortoptionen

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

7.2.3 Datum und Uhrzeit

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

System		Passwörter		Datum und Uhrzeit		Systemlizenzen	
Grundeinstellungen							
Zeitzone	Europe/Berlin						
Aktuelle Ortszeit	Samstag, 29 Apr 2000, 05:21:06						
Manuelle Zeiteinstellung							
Datum einstellen	Tag	Monat	Jahr				
Zeit einstellen	Stunde	Minute					
Automatische Zeiteinstellung (Zeitprotokoll)							
ISDN-Zeitserver	<input type="checkbox"/> Aktiviert						
Erster Zeitserver		SNTP					
Zweiter Zeitserver		SNTP					
Dritter Zeitserver		SNTP					
Zeitaktualisierungsintervall	1440	Minute(n)					
Zeitaktualisierungsrichtlinie	Normal						
System als Zeitserver	<input type="checkbox"/> Aktiviert						
				OK		Abbrechen	

Abb. 42: Systemverwaltung ->Globale Einstellungen->Datum und Uhrzeit

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

ISDN/Manuell

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

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

den anschließend durchgeführt.

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

Zeitserver

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



Hinweis

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

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

Felder im Menü Grundeinstellungen

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

Felder im Menü Manuelle Zeiteinstellung

Feld	Beschreibung
Datum einstellen	Geben Sie ein neues Datum ein. Format: <ul style="list-style-type: none"> • Tag: dd • Monat: mm

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

Felder im Menü Automatische Zeiteinstellung (Zeitprotokoll)

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

Feld	Beschreibung
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>

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

7.2.4 Systemlizenzen

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

Es sind generell folgende Lizenztypen zu unterscheiden:

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

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

Lizenzdaten eintragen

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

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

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

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

Mögliche Werte für Status

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

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



Hinweis

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

7.2.4.1 Bearbeiten oder Neu


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

Abb. 43: **Systemverwaltung -> Globale Einstellungen -> Systemlizenzen -> Neu**

Freischalten von Zusatzlizenzen

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

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

Felder im Menü Grundeinstellungen

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



Hinweis

Wenn als Status *Nicht OK* angezeigt wird:

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

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

Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

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

- (3) Bestätigen Sie mit **OK**.

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

7.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

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

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

Konventionen für die Port-/Schnittstellennamen

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

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

Beispiel: *WLAN1*

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

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

Beispiel: *ETH1*

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

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

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

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

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

Beispiel: *br0* (erste Bridge-Gruppe)

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

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

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

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

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

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

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

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

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

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

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

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

7.3.1 Schnittstellen

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

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

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

Schnittstellen

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

Konfigurationsschnittstelle

Abb. 44: 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 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:

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Eine auswählen</i> (Standardwert): Einstellung im Auslieferungszustand. Die richtige Konfigurationsschnittstelle muss aus den anderen Optionen ausgewählt werden. • <i>Nicht beachten</i>: Keine Schnittstelle wird als Konfigurationsschnittstelle definiert. • <i><Schnittstellename></i>: Legen Sie die Schnittstelle fest, die zur Konfiguration benutzt wird. Wenn diese Schnittstelle Mitglied einer Bridge-Gruppe ist, übernimmt sie deren IP-Adresse, wenn sie aus der Bridge-Gruppe herausgenommen wird.

7.3.1.1 Hinzufügen

Hinzufügen

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

Schnittstellen

Schnittstelle	Eine auswählen ▾
OK Abbrechen	


Abb. 45: **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.

Bearbeiten für Geräte der Wlxxxxn und RS-Serie

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

Schnittstellen

Layer 2.5-Optionen	
Schnittstelle	sta1-0
Wildcard-Modus	letzte


Abb. 46: **Systemverwaltung ->Schnittstellenmodus / Bridge-Gruppen->Schnittstellen->**



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

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

Das Menü **Systemverwaltung ->Schnittstellenmodus /**

Bridge-Gruppen->Schnittstellen->  besteht aus folgenden Feldern:

Felder im Menü Layer 2.5-Optionen

Feld	Wert
Schnittstelle	Zeigt die Schnittstelle an, die gerade bearbeitet wird.
Wildcard-Modus	<p>Wählen Sie aus, welchen Wildcard-Modus Sie auf der Schnittstelle nutzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird kein Wildcard-Modus verwendet. • <i>statisch</i>: Mit dieser Einstellung müssen Sie bei Wildcard-

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

7.4 Administrativer Zugriff

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

7.4.1 Zugriff

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

Zugriff SSH SNMP

! Der administrative Zugang ist zur Zeit nicht eingeschränkt. Die angezeigte Konfiguration wurde noch nicht aktiviert.

Schnittstelle	Telnet	SSH	HTTP	HTTPS	Ping	SNMP	ISDN-Login
en1-0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
en1-4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
bri-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Erweiterte Einstellungen

Standardeinstellungen wiederherstellen

Hinzufügen OK Abbrechen

Abb. 47: **Systemverwaltung** -> **Administrativer Zugriff** -> **Zugriff**

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

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

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

Felder im Menü **Erweiterte Einstellungen**

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

7.4.1.1 Hinzufügen

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



Abb. 48: Systemverwaltung ->Administrativer Zugriff ->Zugriff ->Hinzufügen

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

Felder im Menü Zugriff

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

7.4.2 SSH

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

Zugriff SSH SNMP

SSH-Parameter (Secure Shell)	
SSH-Dienst aktiv	<input checked="" type="checkbox"/> Aktiviert
SSH-Port	<input type="text" value="22"/>
Maximale Anzahl gleichzeitiger Verbindungen	<input type="text" value="1"/>
Authentifizierungs- und Verschlüsselungsparameter	
Verschlüsselungsalgorithmen	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256
Hashing-Algorithmen	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD 160
Schlüsselstatus	
RSA-Schlüsselstatus	Generiert
DSA-Schlüsselstatus	Nicht generiert [Generieren]
Erweiterte Einstellungen	
Toleranzzeit beim Login	<input type="text" value="600"/> Sekunden
Komprimierung	<input type="checkbox"/> Aktiviert
TCP-Keepalives	<input checked="" type="checkbox"/> Aktiviert
Protokollierungslevel	<input type="text" value="Informationen"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 49: Systemverwaltung ->Administrativer Zugriff ->SSH

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

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

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



Hinweis

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

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

Felder im Menü SSH-Parameter (Secure Shell)

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

Felder im Menü Authentifizierungs- und Verschlüsselungsparameter

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

Felder im Menü Schlüsselstatus

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

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Wert
	Standardwert ist <i>600</i> Sekunden.
Komprimierung	Wählen Sie aus, ob Datenkompression verwendet werden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-Keepalives	Wählen Sie aus, ob das Gerät Keepalive-Pakete senden soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Protokollierungslevel	Wählen Sie den Syslog-Level für die vom SSH Daemon generierten Syslog-Messages aus. Zur Verfügung stehen: <ul style="list-style-type: none"> • <i>Informationen</i> (Standardwert): Es werden schwerwiegende Fehler, einfache Fehler des SSH Daemon und Infomeldungen aufgezeichnet. • <i>Fatal</i>: Es werden nur schwerwiegende Fehler des SSH Daemon aufgezeichnet. • <i>Fehler</i>: Es werden schwerwiegende Fehler und einfache Fehler des SSH Daemon aufgezeichnet. • <i>Debug</i>: Es werden alle Meldungen aufgezeichnet.

7.4.3 SNMP

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

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

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

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

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

Zugriff SSH SNMP

Grundeinstellungen	
SNMP-Version	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> v3
SNMP-Listen-UDP-Port	<input type="text" value="161"/>

OK Abbrechen

Abb. 50: **Systemverwaltung ->Administrativer Zugriff->SNMP**

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

Felder im Menü Grundeinstellungen

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



Tipp

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

7.5 Remote Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

7.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete

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


Pakettypen

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

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

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

7.5.1.1 Bearbeiten oder Neu

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

RADIUS TACACS+ Optionen

Basisparameter	
Authentifizierungstyp	PPP-Authentifizierung ▾
Server-IP-Adresse	<input type="text"/>
RADIUS-Passwort	••••••••
Standard-Benutzerpasswort	••••••••
Priorität	0 ▾
Eintrag aktiv	<input checked="" type="checkbox"/> Aktiviert
Gruppenbeschreibung	Default Group 0 ▾

Erweiterte Einstellungen

Richtlinie	Verbindlich ▾
UDP-Port	<input type="text" value="1812"/>
Server Timeout	<input type="text" value="1000"/> Millisekunden
Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
Wiederholungen	<input type="text" value="1"/>
RADIUS-Dialout:	<input type="checkbox"/> Aktiviert Neulade-Intervall <input type="text" value="0"/> Sekunden

OK Abbrechen

Abb. 51: Systemverwaltung ->Remote Authentifizierung ->RADIUS->Neu

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

Felder im Menü Basisparameter

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

Feld	Wert
	<p>trollieren.</p> <ul style="list-style-type: none"> • <i>IPSec-Authentifizierung</i>: Der RADIUS-Server wird verwendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln. • <i>WLAN (802.1x)</i>: Der RADIUS-Server wird verwendet, um den Zugang zu einem Drahtlosnetzwerk zu regeln. • <i>XAUTH</i>: Der RADIUS-Server wird verwendet, um IPSec-Peers über XAuth zu authentisieren.
Betreibermodus	<p>Nur für Authentifizierungstyp = <i>Accounting</i></p> <p>Wählen Sie in Hotspot-Anwendungen den Modus aus, der vom Anbieter definiert ist.</p> <p>In Standardanwendungen belassen Sie den Wert bei <i>Standard</i>.</p> <p>Mögliche Werte für Hotspot-Anwendungen:</p> <ul style="list-style-type: none"> • <i>France Telecom</i>: Für Hotspot-Anwendungen der France Telecom. • <i>bintec HotSpot Server</i>: Für Teldat Hotspot-Anwendungen.
Server-IP-Adresse	Geben Sie die IP-Adresse des RADIUS-Servers ein.
RADIUS-Passwort	Geben Sie das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort ein.
Standard-Benutzerpasswort	Einige RADIUS-Server benötigen für jede RADIUS-Anfrage ein Benutzerpasswort. Geben Sie daher das Passwort hier ein, das Ihr Gerät als Standard-Benutzerpasswort in der Anfrage für die Dialout-Routen an den RADIUS-Server mitsendet.
Priorität	<p>Wenn mehrere RADIUS-Server-Einträge angelegt wurden, wird der Server mit der obersten Priorität als erstes verwendet. Wenn dieser Server nicht antwortet, wird der Server mit der nächstniedrigeren Priorität verwendet usw.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 7 (niedrigste Priorität).</p> <p>Standardwert ist 0.</p>

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

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Wert
Richtlinie	<p>Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Verbindlich</i> (Standardwert): Eine negative Antwort auf eine Anfrage wird akzeptiert. • <i>Nicht verbindlich</i>: Eine negative Antwort auf eine Anfrage wird nicht akzeptiert. Der nächste RADIUS-Server wird angefragt, bis Ihr Gerät eine Antwort von einem als autoritativ konfigurierten Server erhält.
UDP-Port	Geben Sie den zu verwendenden UDP-Port für RADIUS-Daten ein.

Feld	Wert
	<p>Gemäß RFC 2138 sind die Standard-Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Gebührenerfassung (1646 in älteren RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist.</p> <p>Standardwert ist <i>1812</i>.</p>
Server Timeout	<p>Geben Sie die maximale Wartezeit zwischen ACCESS_REQUEST und Antwort in Millisekunden ein.</p> <p>Nach Ablauf dieser Zeit wird die Anfrage gemäß Wiederholungen wiederholt bzw. der nächste konfigurierte RADIUS-Server angefragt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>50</i> und <i>50000</i>.</p> <p>Standardwert ist <i>1000</i> (1 Sekunde).</p>
Erreichbarkeitsprüfung	<p>Wählen Sie eine Überprüfung der Erreichbarkeit eines RADIUS-Servers im Status <i>Inaktiv</i>.</p> <p>Es wird regelmäßig (alle 20 Sekunden) ein Alive-Check durchgeführt, in dem ein ACCESS_REQUEST an die IP-Adresse des RADIUS-Servers gesendet wird. Bei erneuter Erreichbarkeit wird der Status wieder auf <i>aktiv</i> gesetzt. Wenn der RADIUS-Server nur über eine Wählverbindung erreichbar ist, können ungewollte Kosten entstehen, wenn dieser Server längere Zeit <i>inaktiv</i> ist.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Wiederholungen	<p>Geben Sie die Anzahl der Wiederholungen für den Fall ein, dass eine Anfrage nicht beantwortet wird. Falls nach diesen Versuchen dennoch keine Antwort erhalten wurde, wird der Status auf <i>inaktiv</i> gesetzt. bei Erreichbarkeitsprüfung = <i>Aktiviert</i> versucht Ihr Gerät alle 20 Sekunden, den Server zu erreichen. Wenn der Server antwortet, wird Status wieder auf <i>aktiv</i> zurückgesetzt.</p> <p>Mögliche Werte sind ganze Zahlen zwischen <i>0</i> und <i>10</i>.</p> <p>Standardwert ist <i>1</i>. Um zu verhindern, dass Status auf <i>inaktiv</i></p>

Feld	Wert
	<i>tiv</i> gesetzt wird, setzen Sie diesen Wert auf <i>0</i> .
RADIUS-Dialout	<p>Nur für Authentifizierungstyp = <i>PPP-Authentifizierung</i> und <i>IPSec-Authentifizierung</i>.</p> <p>Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiv ist, können Sie folgende Optionen eingeben:</p> <ul style="list-style-type: none"> • <i>Neulade-Intervall</i>: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. <p>Standardmäßig ist hier <i>0</i> eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p>

7.5.2 TACACS+

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

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


Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:

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

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

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

7.5.2.1 Bearbeiten oder Neu

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

RADIUS TACACS+ Optionen

Basisparameter	
Authentifizierungstyp	Login-Authentifizierung
Server-IP-Adresse	
TACACS+-Passwort	••••••••
Priorität	0
Eintrag aktiv	<input checked="" type="checkbox"/> Aktiviert

Erweiterte Einstellungen	
Richtlinie	Nicht verbindlich
TCP-Port	49
Timeout	3 Sekunden
Blockzeit	60 Sekunden
Verschlüsselung	<input checked="" type="checkbox"/> Aktiviert

OK Abbrechen

Abb. 52: Systemverwaltung ->Remote Authentifizierung ->TACACS+ ->Neu

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

Felder im Menü Basisparameter

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

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

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

Felder im Menü Erweiterte Einstellungen

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

Feld	Beschreibung
	TCP-Port (49) an. Der Wert kann nicht verändert werden.
Timeout	<p>Geben Sie die Zeit in Sekunden ein, die der NAS auf eine Antwort von TACACS+ warten soll.</p> <p>Falls während der Wartezeit keine Antwort empfangen wird, wird der als nächster konfigurierte TACACS+-Server abgefragt (nur für Richtlinie = <i>Nicht verbindlich</i>) und der aktuelle Server in einen <i>blockiert</i>-Status versetzt.</p> <p>Mögliche Werte sind 1 bis 60, der Standardwert ist 3.</p>
Blockzeit	<p>Geben Sie die Zeit in Sekunden ein, die der aktuelle Server in einem blockierten Status verbleiben soll.</p> <p>Nach Ende der Blockierung wird der Server in den Status versetzt, der im Feld Eintrag aktiv angegeben ist.</p> <p>Mögliche Werte sind 0 bis 3600, der Standardwert ist 60. Der Wert 0 bedeutet, dass der Server nie in einen <i>blockiert</i>-Status versetzt wird und somit keine weiteren Server angefragt werden.</p>
Verschlüsselung	<p>Wählen Sie aus, ob der Datenaustausch zwischen dem TACACS+-Server und dem NAS mit MD5 verschlüsselt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Ist die Funktion nicht aktiv, werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung sondern nur für Debug-Zwecke empfohlen.</p>

7.5.3 Optionen

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

Abb. 53: Systemverwaltung ->Remote Authentifizierung ->Optionen

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

Felder im Menü Globale RADIUS-Optionen

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

7.6 Zertifikate

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

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

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

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

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


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

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

7.6.1 Zertifikatsliste

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

7.6.1.1 Bearbeiten

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

Zertifikatsliste CRLs Zertifikatsserver

Parameter bearbeiten	
Beschreibung	<input type="text" value="xp.ptx"/>
Zertifikat ist ein CA-Zertifikat	<input checked="" type="checkbox"/> Wahr
Überprüfung anhand einer Zertifikatsperlliste (CRL)	<input type="radio"/> Deaktiviert <input type="radio"/> Immer <input checked="" type="radio"/> Nur wenn ein Zertifikatsperllisten-Verteilungspunkt vorhanden ist <input type="radio"/> Einstellungen des übergeordneten Zertifikates benutzen
Vertrauenswürdigkeit des Zertifikats erzwingen	<input checked="" type="checkbox"/> Wahr
Details anzeigen	
<pre> Certificate = SerialNumber = 11 SubjectName = &lt;CN=r1200_aw, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE&gt; IssuerName = &lt;CN=linuxCA, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE&gt; Validity = NotBefore = 2006 Sep 15th, 07:07:49 GMT NotAfter = 2008 Sep 14th, 07:07:49 GMT PublicKeyInfo = Algorithm name (X.509) : rsaEncryption Modulus n (1024 bits) : 1657430007353061929971175628985365836058592284552111716307381855989730994 4241959750497426343375890536490502929548450998243448632595011570952551767 70116166569068963216398179133323977323187771274664312501085550617414306630 0411834850766905090689578661769721208181141085359073369329733126120426693 320106097890434357773 Exponent e (17 bits) : 65537 Extensions = Available = key usage, basic constraints KeyUsage = DigitalSignature NonRepudiation KeyEncipherment BasicConstraints = cA = FALSE </pre>	
MD5-Fingerabdruck	F0:41:44:3F:6A:62:DD:12:97:2C:67:21:F7:59:80:3E
SHA1-Fingerabdruck	98:5B:D6:3E:4A:9B:95:8B:FE:FF:C2:27:CF:24:42:A7:17:6F:8C:54
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 54: 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 vorhanden ist</i> (Standardwert): Überprüfung nur dann, wenn ein CRL-Distribution-Point-Eintrag im Zertifikat enthalten ist, Dies kann im Inhalt des Zertifikats unter "Details anzeigen" nachgesehen werden. • <i>Einstellungen des übergeordneten Zertifikates benutzen</i>: Es werden die Einstellungen des übergeordneten Zertifikates verwendet, falls eines vorhanden ist. Falls nicht, wird genauso verfahren, wie unter "Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist" beschrieben.
Vertrauenswürdigkeit des Zertifikats erzwingen	<p>Legen Sie fest, dass dieses Zertifikat ohne weitere Überprüfung bei der Authentifizierung als Benutzerzertifikat akzeptiert werden soll.</p> <p>Mit <i>Wahr</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>



Achtung

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

7.6.1.2 Zertifikatsanforderung

Registration-Authority-Zertifikate im SCEP

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

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

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

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

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

Zertifikatsliste CRLs Zertifikatsserver


Zertifikatsanforderung	
Zertifikatsanforderungsbeschreibung	<input type="text"/>
Modus	<input checked="" type="radio"/> Manuell <input type="radio"/> SCEP
Privaten Schlüssel generieren	RSA <input type="text" value="1024"/> Bits
Subjektname	
Benutzerdefiniert	<input type="checkbox"/> Aktiviert
Allgemeiner Name	<input type="text"/>
E-Mail	<input type="text"/>
Organisationseinheit	<input type="text"/>
Organisation	<input type="text"/>
Ort	<input type="text"/>
Staat/Provinz	<input type="text"/>
Land	<input type="text"/>
Erweiterte Einstellungen	
Subjekt-Alternativnamen	
#1	Keiner <input type="text"/>
#2	Keiner <input type="text"/>
#3	Keiner <input type="text"/>
Optionen	
Autospeichermodus	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 55: Systemverwaltung ->Zertifikate->Zertifikatsliste->Zertifikatsanforderung

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

Felder im Menü Zertifikatsanforderung

Feld	Beschreibung
Zertifikatsanforderungsbeschreibung	Geben Sie eine eindeutige Bezeichnung für das Zertifikat ein.
Modus	<p>Wählen Sie aus, auf welche Art Sie das Zertifikat beantragen wollen.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Manuell</i> (Standardwert): Ihr Gerät erzeugt für den Schlüssel eine PKCS#10-Datei, die direkt im Browser hochgeladen oder

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

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

Felder im Menü Subjektname

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

Feld	Beschreibung
Land	Nur für Benutzerdefiniert = deaktiviert. Geben Sie das Land laut CA ein.

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

Felder im Menü **Subjekt-Alternativnamen**

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

Feld im Menü **Optionen**

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

7.6.1.3 Importieren

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

The screenshot shows a dialog box titled 'Importieren' with the following fields and controls:

- Externer Dateiname:** A text input field with a 'Durchsuchen...' button to its right.
- Lokale Zertifikatsbeschreibung:** A text input field.
- Dateikodierung:** A dropdown menu currently showing 'Auto'.
- Passwort:** A text input field.
- Buttons:** 'OK' and 'Abbrechen' buttons at the bottom.

Abb. 56: Systemverwaltung ->Zertifikate->Zertifikatsliste->Importieren

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

Felder im Menü Importieren

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

Feld	Beschreibung
	Tragen Sie das Passwort hier ein.

7.6.2 CRLs

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

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

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

7.6.2.1 Importieren

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

Abb. 57: **Systemverwaltung** -> **Zertifikate** -> **CRLs** -> **Importieren**

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

Felder im Menü CRL-Import

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

Feld	Beschreibung
Lokale Zertifikatsbeschreibung	Geben Sie eine eindeutige Bezeichnung für die CRL ein.
Dateikodierung	Wählen Sie die Art der Kodierung, so dass Ihr Gerät die CRL decodieren kann. Mögliche Werte: <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Aktiviert die automatische Kodierererkennung. Falls der CRL-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung. • <i>Base64</i> • <i>Binär</i>
Passwort	Geben Sie das zum Importieren zu verwendende Passwort ein.

7.6.3 Zertifikatsserver

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

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

7.6.3.1 Neu

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

Zertifikatsliste CRLs **Zertifikatsserver**

Basisparameter	
Beschreibung	<input style="width: 80%;" type="text"/>
LDAP-URL-Pfad	<input style="width: 80%;" type="text" value="ldap://"/>
OK Abbrechen	

Abb. 58: **Systemverwaltung** -> **Zertifikate** -> **Zertifikatsserver** -> **Neu**

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

Felder im Menü Basisparameter

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

Kapitel 8 Physikalische Schnittstellen

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

8.1 Ethernet-Ports

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



Hinweis

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

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

8.1.1 Portkonfiguration

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

Portkonfiguration

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

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

OK Abbrechen

Abb. 59: Physikalische Schnittstellen->Ethernet-Ports->Portkonfiguration

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

Felder im Menü Portkonfiguration

Feld	Beschreibung
Switch-Port	Zeigt den jeweiligen Port an. Die Nummerierung entspricht der Nummerierung der Ethernet-Ports auf der Rückseite des Geräts.
Schnittstelle	Zeigt die logische Schnittstelle an, die dem jeweiligen Ethernet-Port zugeordnet ist.
Konfigurierte Geschwindigkeit/konfigurierter Modus	<p>Wählen Sie den Modus aus, in dem die Schnittstelle betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Vollständige automatische Aushandlung (Standardwert)</i> • <i>Auto 100 Mbit/s only</i> • <i>Auto 10 Mbit/s only</i> • <i>Auto 100 Mbit/s / Full Duplex</i> • <i>Auto 100 Mbit/s / Half Duplex</i> • <i>Auto 10 Mbit/s / Full Duplex</i> • <i>Auto 10 Mbit/s / Half Duplex</i> • <i>Fest 1000 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Full Duplex</i> • <i>Fest 100 Mbit/s / Half Duplex</i> • <i>Fest 10 Mbit/s / Full Duplex</i> • <i>Fest 10 Mbit/s / Half Duplex</i> • <i>Keiner</i>: Die Schnittstelle wird angelegt, bleibt aber inaktiv.
Aktuelle Geschwindigkeit / Aktueller Modus	<p>Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>100 Mbit/s / Full Duplex</i> • <i>100 Mbit/s / Half Duplex</i> • <i>10 Mbit/s / Full Duplex</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>10 Mbit/s / Half Duplex</i> • <i>Inaktiv</i>

8.2 Serieller Port

Die serielle Schnittstelle kann wahlweise als Konsole oder als Datenschnittstelle betrieben werden. Im Modus Datenschnittstelle können die Daten der seriellen Schnittstelle über eine IP-Infrastruktur transportiert werden (Serial over IP).

8.2.1 Serieller Port

Im Menü **Physikalische Schnittstellen->Serieller Port->Serieller Port** können Sie Einstellungen für die serielle Schnittstelle vornehmen.



Abb. 60: **Physikalische Schnittstellen->Serieller Port->Serieller Port**

Das Menü **Physikalische Schnittstellen->Serieller Port->Serieller Port** besteht aus folgenden Feldern:

Felder im Menü Allgemein

Feld	Beschreibung
Port-Modus	<p>Wählen Sie aus, in welchem Modus die serielle Schnittstelle verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Konfiguration</i> (Standardwert): Die serielle Schnittstelle wird als Konsole verwendet. • <i>Datenport</i>: Die serielle Schnittstelle wird als Datenschnittstelle betrieben, Serial over IP wird verwendet.

Wird die Option *Datenport* für den **Port-Modus** ausgewählt, öffnet sich ein weiterer Konfigurationsabschnitt.

Serieller Port

Allgemein	
Port-Modus	<input type="radio"/> Konfiguration <input checked="" type="radio"/> Datenport
Einstellungen Seriell	
Baudrate	9600 ▾
Datenbits	8 ▾
Parität	Keiner ▾
Stoppbits	1 ▾
Handshake:	Keiner ▾
IP	
Modus	<input checked="" type="radio"/> Server <input type="radio"/> Client <input type="radio"/> UDP
Lokale IP-Adresse	0.0.0.0
Lokaler Port	0
Entfernte IP	0.0.0.0
Portnummer	0
Trigger	
Bytezahl	128
Timeout	<input type="checkbox"/> Aktiviert
Inter-Byte Gap	100 ms <input checked="" type="checkbox"/> Aktiviert
Zwischenspeicher	
Seriellen RX-Zwischenspeicher löschen	Löschen
Seriellen TX-Zwischenspeicher löschen	Löschen
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 61: Physikalische Schnittstellen->Serieller Port->Serieller Port mit Port-Modus = Datenport

Felder im Menü Einstellungen Seriell

Feld	Beschreibung
Baudrate	<p>Wählen Sie, welche Baud Rate verwendet werden soll. Achten Sie darauf, dass die Gegenstelle die gewählte Baud Rate beherrscht. Wenn dies nicht der Fall ist, können Sie keine serielle Verbindung zum Gerät herstellen!</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • 300 • 600 • 1200 • 2400

Feld	Beschreibung
	<ul style="list-style-type: none"> • 4800 • 9600 (Standardwert) • 19200 • 57600 • 115200
Datenbits	<p>Wählen Sie, wieviel Datenbits jeweils hintereinander für Nutzdaten gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • 8 (Standardwert): Acht Datenbits werden hintereinander gesendet. • 7: Sieben Datenbits werden hintereinander gesendet.
Parität	<p>Wählen Sie, ob ein Parity Bit zur Erkennung von Übertragungsfehlern verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird kein Parity Bit verwendet. • <i>Gerade</i>: Es wird eine gerade Anzahl von "1"-Bits zur Erkennung von Übertragungsfehlern verwendet. • <i>Ungerade</i>: Es wird eine ungerade Anzahl von "1"-Bits zur Erkennung von Übertragungsfehlern verwendet.
Stoppbits	<p>Stopp Bits schließen die Datenübertragung einer Übertragungseinheit ab.</p> <p>Wählen Sie, ob ein Stopp Bit verwendet werden soll oder ob zwei Stopp Bits verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • 1 (Standardwert) • 2
Handshake	<p>Wählen Sie, wie der Empfänger die Datenübertragung anhalten kann, damit keine Datenverluste auftreten, wenn aktuell keine weiteren Daten verarbeitet werden können.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Der Empfänger kann die Datenübertragung nicht anhalten. • <i>RTS/CTS</i>: Der verwendeten Hardware-Handshake steuert den Datenfluss über die Leitungen RTS und CTS. • <i>XON/XOFF</i>: Beim verwendeten Software-Handshake sendet der Empfänger zur Steuerung des Datenflusses spezielle Zeichen an den Sender.

Felder im Menü IP

Feld	Beschreibung
Modus	<p>Wählen Sie den Modus, in welchem das Gateway IP-Datenpakete verarbeiten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Server</i> (Standardwert): Das Gateway wartet auf eingehende TCP-Verbindungen. • <i>Client</i>: Das Gateway baut aktiv eine TCP-Verbindung auf. • <i>UDP</i>: Das Gateway sendet und empfängt UDP-Pakete.
Lokale IP-Adresse	Geben Sie die IP-Adresse des Clients an, der sich anmelden will. Wenn Lokale IP-Adresse = 0.0.0.0, kann sich jeder beliebige Client anmelden.
Lokaler Port	Geben Sie den Port zur Lokale IP-Adresse ein.
Entfernte IP	Geben Sie die IP-Adresse des Servers an, an dem sich Ihr Gateway anmelden soll.
Portnummer	Geben Sie den Port zur Entfernte IP ein.

Felder im Menü Trigger

Feld	Beschreibung
Bytezahl	<p>Geben Sie die empfangenen Zeichen in Byte an, die als Trigger für die Datenübertragung benutzt werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Mögliche Werte: 1.. 1460. Standardwert: 128.</p>

Feld	Beschreibung
Timeout	<p>Geben Sie die Zeit in ms seit dem Empfang des letzten Zeichens an, die als Trigger für die Datenübertragung benutzt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Mögliche Werte: 0.. 65535. Standardwert: 0.</p>
Inter-Byte Gap	<p>Geben Sie die Zeit in ms seit dem Empfang des ersten Zeichens an, die als Trigger für die Datenübertragung benutzt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Mögliche Werte: 0.. 65535. Standardwert: 100.</p>

Felder im Menü **Zwischenspeicher**

Feld	Beschreibung
Seriellen RX-Zwischenspeicher löschen	Wählen Sie die Schaltfläche Löschen , um den Empfangspuffer zu leeren.
Seriellen TX-Zwischenspeicher löschen	Wählen Sie die Schaltfläche Löschen , um den Sendepuffer zu leeren.

8.3 Relais

Die Geräten der **WI-Serie** sind mit einem steuerbaren Relais ausgestattet. Das Relais ist im Ruhezustand (d.h. stromlos bzw. im Fehlerfall) offen. Das Relais kann wahlweise manuell gesteuert werden, oder als Alarm-Relais mit der roten Error-LED gekoppelt werden. Bei manueller Steuerung wird der Relaiszustand während des Bootens bei der Übernahme der Konfiguration gesetzt.

8.3.1 Relaiskonfiguration

In diesem Menü können Sie den **Port-Modus** konfigurieren.

Relaiskonfiguration

Basisparameter	
Port-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv <input type="radio"/> Alarm-Relais
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 62: Physikalische Schnittstellen->Relais->Relaiskonfiguration

Das Menü **Physikalische Schnittstellen->Relais->Relaiskonfiguration** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Port-Modus	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Relais ist manuell permanent offen. • <i>Aktiv</i>: Relais ist manuell permanent geschlossen. • <i>Alarm-Relais</i>: Relais ist automatisch mit der roten Error-LED gekoppelt.

Kapitel 9 LAN


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

9.1 IP-Konfiguration

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

9.1.1 Schnittstellen

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

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

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

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



Hinweis

Beachten Sie bitte:

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


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

Beispiel Teilnetze

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

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

9.1.1.1 Bearbeiten oder Neu

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

Schnittstellen

Basisparameter					
Basierend auf Ethernet-Schnittstelle	<input type="text" value="Eine auswählen"/>				
Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> DHCP				
IP-Adresse / Netzmaske	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;"><input type="text" value="IP-Adresse"/></td> <td><input type="text" value="Netzmaske"/></td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	<input type="text" value="IP-Adresse"/>	<input type="text" value="Netzmaske"/>	<input type="button" value="Hinzufügen"/>	
<input type="text" value="IP-Adresse"/>	<input type="text" value="Netzmaske"/>				
<input type="button" value="Hinzufügen"/>					
Schnittstellenmodus	<input type="radio"/> Untagged <input checked="" type="radio"/> Tagged (VLAN)				
MAC-Adresse	<input type="text" value="00:a0:f9"/> <input checked="" type="checkbox"/> Voreingestellte verwenden				
VLAN-ID	<input type="text" value="1"/>				
Erweiterte Einstellungen					
Proxy ARP	<input type="checkbox"/> Aktiviert				
TCP-MSS-Clamping	<input type="checkbox"/> Aktiviert				
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

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

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.
Adressmodus	<p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse / Netzmaske zugewiesen. • <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse / Netzmaske	<p>Nur für Adressmodus = <i>Statisch</i></p> <p>Fügen Sie mit Hinzufügen einen neuen Adresseintrag hinzu und geben Sie die IP-Adresse und die entsprechende Netzmaske der virtuellen Schnittstelle ein.</p>
Schnittstellenmodus	<p>Nur bei physikalischen Schnittstellen im Routing-Modus.</p> <p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Untagged</i> (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet. • <i>Tagged (VLAN)</i>: Diese Option gilt nur für Routing-Schnittstellen. <p>Mit dieser Option weisen Sie die Schnittstelle einem VLAN zu. Dies geschieht über die VLAN-ID, die in diesem Modus angezeigt wird und konfiguriert werden kann. Die Definition einer MAC-Adresse in MAC-Adresse ist in diesem Modus optional.</p>
MAC-Adresse	<p>Nur bei virtuellen Schnittstellen und nur für Schnittstellenmodus = <i>Untagged</i></p> <p>Geben Sie die mit der Schnittstelle verbundene MAC-Adresse ein. Sie können für virtuelle Schnittstellen die MAC-Adresse der physikalischen Schnittstelle verwenden, unter der die virtuelle Schnittstelle erstellt wurde. Das ist allerdings nicht notwendig. Das Zuweisen einer virtuellen MAC-Adresse ist ebenfalls möglich. Die ersten 6 Zeichen der MAC-Adresse sind voreingestellt</p>

Feld	Beschreibung
	(sie können jedoch geändert werden).
VLAN-ID	<p>Nur für Schnittstellenmodus = <i>Tagged</i> (VLAN)</p> <p>Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben.</p> <p>Mögliche Werte sind 1 (Standardwert) bis 4094.</p>

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

Felder im Menü **Erweiterte Einstellungen**

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

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

9.2 VLAN

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

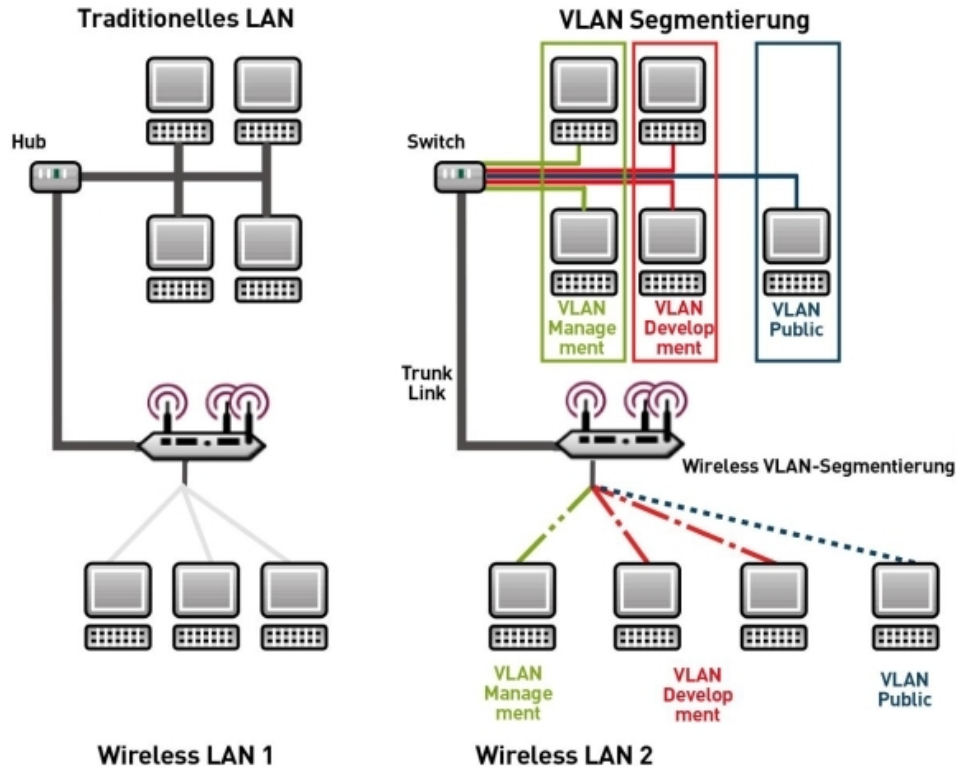


Abb. 64: VLAN-Segmentierung

VLAN für Bridging und VLAN für Routing

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



Achtung

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

9.2.1 VLANs

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

9.2.1.1 Bearbeiten oder Neu



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



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

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

Felder im Menü VLAN konfigurieren

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

Feld	Beschreibung
	übertragen werden sollen.

9.2.2 Portkonfiguration

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

The screenshot shows the 'Portkonfiguration' menu. At the top, there are three tabs: 'VLANs', 'Portkonfiguration', and 'Verwaltung'. Below the tabs is a search and filter area with 'Ansicht: 20 pro Seite', 'Filtern in: Keiner', and a dropdown set to 'gleich'. A 'Los' button is to the right. The main table has four columns: 'Schnittstelle', 'PVID', 'Frames ohne Tag verwerfen', and 'Nicht-Mitglieder verwerfen'. The first row shows 'en1-0' in the 'Schnittstelle' column, '1 - Management' in the 'PVID' column, and two unchecked checkboxes in the other two columns. Below the table, it says 'Seite: 1, Objekte: 1 - 1'. At the bottom, there are 'OK' and 'Abbrechen' buttons.

Abb. 66: LAN->VLANs->Portkonfiguration

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

Felder im Menü Portkonfiguration

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

9.2.3 Verwaltung

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

Abb. 67: LAN->VLANs->Verwaltung

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

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

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

Kapitel 10 Wireless LAN

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

Netzwerkfunktionen

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

Derzeit gültiger Standard: IEEE 802.11

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

IEEE 802.11g ist der derzeit am weitesten verbreitete Standard für Funk-LANs und bietet eine maximale Datenübertragungsrate von 54 Mbit/s. Dieses Verfahren arbeitet im 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.

10.1 WLAN

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

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

10.1.1 Einstellungen Funkmodul

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

Einstellungen Funkmodul

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

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

10.1.1.1 Einstellungen Funkmodul->

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie das Symbol um die Konfiguration zu bearbeiten.

Einstellungen Funkmodul

WLAN-Einstellungen	
Betriebsmodus	Access-Point ▼
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
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

Einstellungen Funkmodul

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

Erweiterte Einstellungen

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

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

Felder im Menü WLAN-Einstellungen

Feld	Beschreibung
Betriebsmodus	<p>Legen Sie fest, in welchem Modus das Funkmodul Ihres Geräts betrieben werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Das Funkmodul ist nicht aktiv. • <i>Access-Point</i>: Ihr Gerät dient als Access Point in Ihrem Netzwerk. • <i>Access Client</i>: Ihr Gerät dient als Access Client in Ihrem Netzwerk. Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar. • <i>Bridge</i>: Ihr Gerät dient als Wireless Bridge in Ihrem Netzwerk. Für bintec W1003n, bintec W2003n, bintec W2003n-ext, bintec W2004n und Geräte der RS-Serie nicht

Feld	Beschreibung
	verfügbar.
Client-Modus	<p>Nur für Betriebsmodus = <i>Access Client</i></p> <p>Wählen Sie den Modus der Verbindung des Clients zum Access Point aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Infrastruktur</i> (Standardwert): In einem Netz im Infrastruktur Modus kommunizieren alle Clients ausschließlich über Access Points miteinander. Es läuft keine Kommunikation zwischen den einzelnen Clients direkt ab. • <i>Ad-Hoc</i>: Ein Access Client kann im Ad-Hoc-Modus als zentrale Schnittstelle zwischen mehreren Endgeräten verwendet werden. Auf diese Weise können Geräte wie Computer und Drucker kabellos miteinander verbunden werden. <p>Wählen Sie den Kanal aus, der verwendet werden soll.</p>
Frequenzband	<p>Wählen Sie das Frequenzband und ggf. den Einsatzbereich des Funkmoduls aus.</p> <p>Für Betriebsmodus = <i>Access-Point, Bridge</i> oder Betriebsmodus = <i>Access Client</i> und Client-Modus = <i>Ad-Hoc</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2,4 GHz In/Outdoor</i> (Standardwert): Ihr Gerät wird mit 2.4 GHz (Mode 802.11b und Mode 802.11g) innerhalb oder außerhalb von Gebäuden betrieben. • <i>5 GHz Indoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb von Gebäuden betrieben. • <i>5 GHz Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) außerhalb von Gebäuden betrieben. • <i>5 GHz In/Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) innerhalb oder außerhalb von Gebäuden betrieben. • <i>5,8 GHz Outdoor</i>: Nur für so genannte Broadband Fixed Wireless Access (BFWA) Anwendungen. Die Frequenzen im Frequenzbereich von 5 755 MHz bis 5 875 MHz dürfen nur in Verbindung mit gewerblichen Angeboten für öffentliche Netzzugänge genutzt werden und bedürfen einer Anmeldung bei

Feld	Beschreibung
	<p>der Bundesnetzagentur.</p> <p>Für Betriebsmodus = <i>Access Client</i> und Client-Modus = <i>Infrastruktur</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2,4 und 5 GHz</i>: Ihr Gerät wird mit 2,4 (Mode 802.11b und Mode 802.11g) oder 5 GHz (Mode 802.11a/h) betrieben. • <i>5 GHz</i> (Standardwert): Ihr Gerät wird mit 5 GHz (Mode 802.11a/h) betrieben. • <i>2,4 GHz</i>: Ihr Gerät wird mit 2.4 GHz (Mode 802.11b und Mode 802.11g) betrieben.
Nutzungsbereich	<p>Nur für Betriebsmodus = <i>Access Client</i>, Client-Modus = <i>Infrastruktur</i> und Frequenzband = <i>2,4 und 5 GHz</i> oder <i>5 GHz</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Indoor-Outdoor</i> (Standardwert) • <i>Indoor</i> • <i>Outdoor</i>
IEEE 802.11d-Konformität	<p>Nur für Betriebsmodus = <i>Access Client</i></p> <p>Wählen Sie aus, wie die Länderinformation ermittelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Flexibel</i> (Standardwert): Es wird versucht, die Länderinformation des Access Points zu ermitteln, ansonsten wird die eigene Länderinformation verwendet. • <i>Keine</i>: Die eigene Länderinformation wird verwendet. • <i>Strikt</i>: Die Länderinformation des Access Points wird verwendet.
Kanal	<p>Die Anzahl der wählbaren Kanäle ist von der Ländereinstellung abhängig. Bitte ziehen Sie hier das aktuelle Datenblatt Ihres Geräts zu Rate.</p> <p>Access-Point-Modus / Bridge-Modus:</p>

Feld	Beschreibung
	<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). Im Bridge-Modus ist <i>Auto</i> nicht möglich.</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz Indoor</i> <p>Mögliche Werte sind <i>36, 40, 44, 48</i> und <i>Auto</i> (Standardwert)</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Outdoor</i> und <i>5,8 GHz Outdoor</i> <p>Hier ist nur die Option <i>Auto</i> möglich.</p> <p>Access Client Modus:</p> <p>Im Access Client Modus können Sie nur im Client-Modus = <i>Ad-Hoc</i> den erforderlichen Kanal auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>2,4 GHz In/Outdoor</i> <p>Mögliche Werte sind <i>1</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, 40, 44, 48</i> und <i>Auto</i> (Standardwert)</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Outdoor</i> und <i>5,8 GHz Outdoor</i>

Feld	Beschreibung
	Hier ist nur die Option <i>Auto</i> möglich.
Ausgewählter Kanal	Zeigt den verwendeten Kanal an.
Zweiter Verwendeter Kanal	Nicht für Betriebsmodus = <i>Access-Point</i> und Frequenzband = <i>2,4 GHz In/Outdoor</i> Zeigt den zweiten verwendeten Kanal an.
Bandbreite	Nur für Drahtloser Modus = <i>802.11b/g/n, 802.11g/n, 802.11n, 802.11a/n</i> Wählen Sie aus, wie viele Kanäle verwendet werden sollen. Mögliche Werte: <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	Nur für Drahtloser Modus = <i>802.11b/g/n, 802.11g/n, 802.11n, 802.11a/n</i> Wählen Sie aus, wie viele Datenströme parallel verwendet werden sollen. Mögliche Werte: <ul style="list-style-type: none">• <i>3</i>: Drei Datenströme werden verwendet.• <i>2</i>: Zwei Datenströme werden verwendet.• <i>1</i>: Ein Datenstrom wird verwendet.
Max. Link-Entfernung	Nur für Betriebsmodus = <i>Bridge</i> Geben Sie die maximale Link-Entfernung ein. Ist die Option <i>Benutze Standard</i> aktiviert, wird die automatisch generierte Entfernung übernommen. Ist die Option nicht aktiviert, geben Sie den gewünschten Maximalwert in das Eingabefeld in m ein.

Feld	Beschreibung
	Standardmäßig ist die Option <i>Benutze Standard</i> aktiviert.
Sendeleistung	<p>Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die tatsächlich abgestrahlte Antennenleistung kann abhängig von der übertragenen Datenrate auch niedriger liegen als der eingestellte Maximalwert. Der Maximalwert der verfügbaren Sendeleistung ist länderabhängig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet. • <i>5 dBm</i> • <i>8 dBm</i> • <i>11 dBm</i> • <i>14 dBm</i> • <i>16 dBm</i>

Felder im Menü Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	<p>Wählen Sie die Wireless-Technologie aus, die der Access Point anwenden soll.</p> <p>Nur für Frequenzband = 2,4 GHz In/Outdoor</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>802.11g</i>: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • <i>802.11b</i>: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • <i>802.11 mixed (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. • <i>802.11 mixed long (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Nur die Datenrate von 1 und 2 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). Dieser Modus wird auch für Centrino Clients benötigt, falls

Feld	Beschreibung
	<p>Verbindungsprobleme aufgetreten sind.</p> <ul style="list-style-type: none"> • <i>802.11 mixed short (b/g)</i>: Ihr Gerät passt sich der Technologie der Clients an und arbeitet entweder nach 802.11b oder 802.11g. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • <i>802.11b/g/n</i>: Ihr Gerät arbeitet entweder nach 802.11b, 802.11g oder 802.11n. • <i>802.11g/n</i>: Ihr Gerät arbeitet entweder nach 802.11g oder 802.11n. • <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. <p>Im Betriebsmodus <i>Access Client</i> mit Client-Modus <i>Ad-Hoc</i> stehen zusätzliche Optionen für Frequenzband = 5 GHz <i>Indoor</i>, 5 GHz <i>Outdoor</i>, 5 GHz <i>In/Outdoor</i>, 5,8 GHz <i>Outdoor</i> zur Verfügung</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>802.11a</i>: Ihr Gerät arbeitet ausschließlich nach 802.11a. • <i>802.11n</i>: Ihr Gerät arbeitet ausschließlich nach 802.11n. • <i>802.11a/n</i>: Ihr Gerät arbeitet entweder nach 802.11a oder 802.11n. • <i>802.11a/b/g/n</i> (nur Anzeige): Nur im Betriebsmodus <i>Access Client</i> mit Client-Modus <i>Infrastruktur</i>.
Max. Übertragungsrate	<p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <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>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p>

Feld	Beschreibung
	<p>Aktivieren Sie diese Funktion, um die Übertragungsgeschwindigkeit für 802.11g durch Frame Bursting zu erhöhen. Dabei werden mehrere Pakete nacheinander ohne Wartezeiten verschickt. Dies ist besonders effektiv im 11b/g Mischbetrieb.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiviert.</p> <p>Falls Probleme mit älterer WLAN-Hardware auftreten, sollte diese Funktion deaktiviert werden.</p>
Airtime Fairness	<p>Diese Funktion ist nicht für alle Geräte verfügbar.</p> <p>Mit der Airtime Fairness -Funktion wird gewährleistet, dass Senderressourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.</p>

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

Felder im Menü **Erweiterte Einstellungen für Betriebsmodus = Access-Point**

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Alle</i>: Alle Kanäle können bei der Kanalwahl gewählt werden. • <i>Auto</i>: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • <i>Benutzerdefiniert</i>: Wählen Sie die gewünschten Kanäle selbst aus.
Ausgewählte Kanäle	<p>Nur für Kanalplan = <i>Benutzerdefiniert</i></p> <p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <p>Mit Hinzufügen können Sie Kanäle hinzufügen. Wenn alle verfügbaren Kanäle angezeigt werden, können Sie keine Einträge hinzufügen.</p> <p>Mithilfe von -Symbol können Sie Einträge löschen.</p>
Beacon Period	<p>Nur für Betriebsmodus = <i>Access-Point</i> oder <i>Access Client</i> mit Client-Modus <i>Ad-Hoc</i>.</p> <p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <p>Geben Sie die Zeit in Millisekunden zwischen dem Senden zweier Beacons an.</p> <p>Dieser Wert wird in Beacon und Probe Response Frames übermittelt.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 100 ms.</p>
DTIM Period	<p>Nur für Betriebsmodus = <i>Access-Point</i> oder <i>Access Client</i> mit Client-Modus <i>Ad-Hoc</i>.</p> <p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <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-</p>

Feld	Beschreibung
	<p>oder Multicast-Übertragung informiert. Wenn Clients im Stromsparmodus arbeiten, wachen sie zum richtigen Zeitpunkt auf und empfangen die Daten.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 2.</p>
RTS Threshold	<p>Hier wählen Sie aus, wie der RTS/CTS-Mechanismus ein- bzw. ausgeschaltet werden soll.</p> <p>Wählen Sie <i>Benutzerdefiniert</i> aus, können Sie in das Eingabefeld den Schwellwert in Bytes (1 - 2346) angeben, ab welcher Datenpaketlänge der RTS/CTS-Mechanismus verwendet werden soll. Dies ist sinnvoll, wenn an einem Access Point mehrere Clients betrieben werden, die sich gegenseitig nicht in Funkreichweite befinden. Der Mechanismus kann auch unabhängig von der Datenpaketlänge ein- bzw. ausgeschaltet werden, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.</p>
Short Guard Interval	<p>Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.</p>
Short Retry Limit	<p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <p>Geben Sie die maximale Anzahl an Sendeversuchen für ein Frames ein. Dieser Wert muss kürzer oder gleich dem in RTS Threshold definierten Wert sein. Nach dieser Anzahl an Fehlversuchen wird das Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 7.</p>
Long Retry Limit	<p>Für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n nicht verfügbar.</p> <p>Geben Sie die maximale Anzahl an Sendeversuchen eines Datenpakets ein. Dieser Wert muss länger sein, als der in RTS Threshold definierte Wert. Nach dieser Anzahl an Fehlversuchen wird das Paket verworfen.</p>

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

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

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

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

Felder im Menü Erweiterte Einstellungen für Access Client Modus



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

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

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

Feld	Beschreibung
	den, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.
Short Guard Interval	Aktivieren Sie diese Funktion, um das Guard Interval (= Zeit zwischen der Übertragung von zwei Datensymbolen) von 800 ns auf 400 ns zu verkürzen.
Short Retry Limit	<p>Geben Sie die maximale Anzahl an Sendeversuchen für einen Frame ein. Dieser Wert muss kleiner oder gleich dem in RTS Threshold definierten Wert sein. Nach dieser Anzahl an Fehlversuchen wird das Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 7.</p>
Long Retry Limit	<p>Geben Sie die maximale Anzahl an Sendeversuchen für ein Datenpaket ein. Dieser Wert muss größer als der in RTS Threshold definierte Wert sein. Nach dieser Anzahl an Fehlversuchen wird das Paket verworfen.</p> <p>Mögliche Werte sind 1 bis 255.</p> <p>Der Standardwert ist 4.</p>
Fragmentation Threshold	<p>Geben Sie maximale Größe an, ab der Datenpakete fragmentiert (d. h. in kleinere Einheiten aufgeteilt) werden. Niedrige Werte in diesem Feld sind in Bereichen mit schlechtem Empfang und bei Funkstörungen empfehlenswert.</p> <p>Möglich Werte sind 256 bis 2346.</p> <p>Der Standardwert ist 2346 Bytes.</p>

10.1.2 Drahtlosnetzwerke (VSS)

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



Hinweis

Das voreingestellte Drahtlosnetzwerk default verfügt im Auslieferungszustand über folgende Sicherheitseinstellungen:

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

Einstellen von Netzwerknamen

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

Absicherung von Funknetzwerken

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

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

WEP

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

IEEE 802.11i

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

WPA

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

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

WPA 2

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

Zugangskontrolle

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

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


Sicherheitsmaßnahmen

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

- Ändern Sie die Zugangspasswörter Ihres Geräts.
- Ändern Sie die Standard-SSID, **Netzwerkname (SSID)** = *default*, Ihres Access Points. Setzen Sie **Sichtbar** = *Aktiviert*. Damit werden alle WLAN-Clients ausgeschlossen, die mit dem allgemeinen Wert für **Netzwerkname (SSID)** *Beliebig* einen Verbindungsaufbau versuchen und welche die eingestellten SSIDs nicht kennen.
- Nutzen Sie die zur Verfügung stehenden Verschlüsselungsmethoden. Wählen Sie dazu **Sicherheitsmodus** = *WEP 40, WEP 104, WPA-PSK* oder *WPA-Enterprise* und tragen Sie den entsprechenden Schlüssel im Access Point unter **WEP-Schlüssel 1 - 4** bzw. **Preshared Key** sowie in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmäßig geändert werden. Wechseln Sie dazu den **Übertragungsschlüssel**. Wählen Sie den längeren 104-Bit-WEP-Schlüssel.
- Für die Übertragung von extrem sicherheitsrelevanten Informationen sollte der **Sicherheitsmodus** = *WPA-Enterprise* mit **WPA-Modus** = *WPA 2* konfiguriert werden. Diese Methode beinhaltet eine hardwarebasierte Verschlüsselung und RADIUS-Authentifizierung des Clients. In Sonderfällen ist auch eine Kombination mit IPSec möglich.
- Beschränken Sie den Zugriff im WLAN auf zugelassene Clients. Tragen Sie die MAC-Adressen der Funknetzwerkkarten dieser Clients in die **Erlaubte Adressen**-Liste im Menü **MAC-Filter** ein (siehe *Felder im Menü MAC-Filter* auf Seite 177).

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

10.1.2.1 Bearbeiten oder Neu

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

Einstellungen Funkmodul Drahtlosnetzwerke (VSS)

Service Set Parameter	
Netzwerkname (SSID)	default <input checked="" type="checkbox"/> Sichtbar
Intra-cell Repeating	<input checked="" type="checkbox"/> Aktiviert
U-APSD	<input checked="" type="checkbox"/> Aktiviert
Sicherheitseinstellungen	
Sicherheitsmodus	Inaktiv <input type="button" value="v"/>
Client-Lastverteilung	
Max. Anzahl Clients - Hard Limit	32
Max. Anzahl Clients - Soft Limit	24
Auswahl des Client-Bands	Deaktiviert, optimiert für Fast Roaming <input type="button" value="v"/>
MAC-Filter	
Zugriffskontrolle	<input type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Beacon Period	100 ms
DTIM Period	2
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

Felder im Menü Service Set Parameter


Feld	Beschreibung
Netzwerkname (SSID)	<p>Geben Sie den Namen des Wireless Netzwerks (SSID) ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit max. 32 Zeichen ein.</p> <p>Wählen Sie außerdem aus, ob der Netzwerkname (SSID) übertragen werden soll.</p> <p>Mit Auswahl von <i>Sichtbar</i> wird der Netzwerkname sichtbar übertragen.</p> <p>Standardmäßig ist er sichtbar.</p>
Intra-cell Repeating	<p>Wählen Sie aus, ob die Kommunikation zwischen den WLAN-Clients innerhalb einer Funkzelle erlaubt sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
ARP Processing	<p>Wählen Sie aus, ob die Funktion ARP Processing aktiv sein soll. Dabei wird das ARP-Datenaufkommen im Netzwerk reduziert, indem in ARP-Unicasts umgewandelte ARP-Broadcasts an die intern bekannten IP-Adressen weitergeleitet werden. Unicasts sind zudem schneller, und Clients mit aktivierter Power-Save-Funktion werden nicht angesprochen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Beachten Sie, dass ARP Processing nicht in Zusammenhang mit der Funktion MAC-Bridge angewendet werden kann.</p>
WMM	<p>Wählen Sie aus, ob für das Drahtlosnetzwerk Sprach- oder Videodaten- Priorisierung mittels WMM (Wireless Multimedia) aktiviert sein soll, um stets eine optimale Übertragungsqualität bei zeitkritischen Anwendungen zu erreichen. Es wird Datenpriorisierung nach DSCP (Differentiated Services Code Point) oder IEEE802.1d unterstützt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
U-APSD	<p>Nur für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n</p> <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>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Key • <i>WPA-Enterprise</i>: 802.11i/TKIP
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Standardwert ist <i>Schlüssel 1</i>.</p>
WEP-Schlüssel 1-4	<p>Nur für Sicherheitsmodus = <i>WEP 40</i>, <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein.</p> <p>Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen, z. B. <i>hallo</i> für <i>WEP 40</i>, <i>teldat-wep1</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> und <i>WPA 2</i> (Standardwert): WPA und WPA 2 können angewendet werden. • <i>WPA</i>: Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA 2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA</i> und <i>WPA und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA anwenden wollen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): AES wird angewendet. • <i>AES und TKIP</i>: AES oder TKIP werden angewendet.
<p>WPA2 Cipher</p>	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA 2</i> und <i>WPA und WPA 2</i></p> <p>Wählen Sie aus, mit welcher Verschlüsselung Sie WPA 2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): AES wird angewendet. • <i>AES und TKIP</i>: AES oder TKIP werden angewendet.
<p>Preshared Key</p>	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.</p> <div data-bbox="542 935 1320 1140" style="border: 1px solid black; padding: 5px;"> <p> Hinweis</p> <p>Ändern Sie unbedingt den Standard Preshared Key! Solange der Schlüssel nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!</p> </div>
<p>EAP-Vorabauthentifizierung</p>	<p>Nur für Sicherheitsmodus = <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob EAP-Vorabauthentifizierung aktiviert werden soll. Mit dieser Funktion gibt ihr Gerät bekannt, dass WLAN-Clients, die schon mit einem anderen Access Point verbunden sind, vorab eine 802.1x-Authentifizierung mit Ihrem Gerät durchführen können, sobald sie in Reichweite sind. Solche WLAN-Clients können sich anschließend auf vereinfachte Weise über die bestehende Netzwerkverbindung mit Ihrem Gerät verbinden.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Client-Lastverteilung für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n

Feld	Beschreibung
<p>Max. Anzahl Clients - Hard Limit</p>	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p> <p>Mögliche Werte sind ganze Zahlen von 1 bis 254.</p> <p>Der Standardwert ist 32.</p>
<p>Max. Anzahl Clients - Soft Limit</p>	<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>
<p>Auswahl des Client-Bands</p>	<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</p>

Feld	Beschreibung
	<p>tes 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>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 Erweiterte Einstellungen für bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n

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 1 bis 65535.</p> <p>Der Standardwert ist 100 ms.</p>

Feld	Beschreibung
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 Stromsparmmodus 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>

10.1.3 WDS-Links

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

Für **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** nicht verfügbar.



Wichtig

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

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

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




Wichtig

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

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

10.1.3.1 Bearbeiten oder Neu

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

Einstellungen Funkmodul Drahtlosnetzwerke (VSS) **WDS-Links**

Basisparameter	
WDS-Beschreibung	<input checked="" type="checkbox"/> <i>Benutze Standard</i>
WDS-Sicherheitseinstellungen	
Schutz	Keiner ▼
Entfernter Partner	
Entfernte MAC-Adresse	00:00:00:00:00:00
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

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

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
	Standardmäßig ist die Option <i>Benutze Standard</i> aktiviert.

Felder im Menü WDS-Sicherheitseinstellungen



Feld	Beschreibung
Schutz	<p>Wählen Sie aus, ob und wenn ja welche Verschlüsselungsmethode auf diesem WDS Link angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Der Datenverkehr auf diesem WDS Link wird nicht verschlüsselt. • <i>WEP 40</i>: Der Datenverkehr auf diesem WDS Link wird mit WEP 40 verschlüsselt. Geben Sie in WEP-Schlüssel 1 bis WEP-Schlüssel 4 die Schlüssel für diesen WDS-Link ein und wählen Sie in Übertragungsschlüssel den Standard-Schlüssel aus. • <i>WEP 104</i>: Der Datenverkehr auf diesem WDS Link wird mit WEP104 verschlüsselt. Geben Sie in WEP-Schlüssel 1 bis WEP-Schlüssel 4 die Schlüssel für diesen WDS-Link ein und wählen Sie in Übertragungsschlüssel den Standard-Schlüssel aus. • <i>WPA</i>: Der Datenverkehr auf diesem WDS Link wird mit WPA verschlüsselt. Geben Sie in Preshared Key den Schlüssel für diesen WDS-Link ein. • <i>WPA 2</i>: Der Datenverkehr auf diesem WDS Link wird mit WPA verschlüsselt. Geben Sie in Preshared Key den Schlüssel für diesen WDS-Link ein.
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> oder <i>WEP 104</i></p> <p>Wählen Sie einen der in WEP-Schlüssel 1 bis WEP-Schlüssel 4 konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Standardwert ist <i>Schlüssel 1</i>.</p>
WEP-Schlüssel 1 bis WEP-Schlüssel 4	<p>Nur für Schutz = <i>WEP 40</i>, <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein. Es gibt zwei Möglichkeiten, einen WEP-Schlüssel einzugeben:</p> <ul style="list-style-type: none"> • Direkte Eingabe in hexadezimaler Form

Feld	Beschreibung
	<p>Beginnt die Eingabe mit <i>0x</i>, wird der Generator deaktiviert. Geben Sie eine hexadezimale Zeichenfolge mit exakt der für den gewählten WEP-Modus passenden Zeichenanzahl ein. 10 Zeichen für <i>WEP 40</i> oder 26 Zeichen für <i>WEP 104</i> z. B. <i>WEP 40: 0xA0B23574C5</i>, <i>WEP 104: 0x81DC9BDB52D04DC20036DBD831</i></p> <ul style="list-style-type: none"> • Direkte Eingabe von ASCII Zeichen <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>teldat-wep1</i> für <i>WEP 104</i>.</p>
Preshared Key	<p>Nur für Schutz = <i>WPA</i>, <i>WPA 2</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII Zeichenfolge mit 8 - 63 Zeichen ein.</p>

Felder im Menü Entfernter Partner

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

10.1.4 Client Link

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

Für **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** nicht verfügbar.


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

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

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


cker kabellos miteinander verbunden werden.

10.1.4.1 Bearbeiten

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.

Einstellungen Funkmodul Client Link

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

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

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

Felder im Menü Basisparameter

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


Felder im Menü Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA None</i>: Nur für Client-Modus = Ad-Hoc. WPA None • <i>WPA-PSK</i>: Nur für Client-Modus = Infrastruktur. WPA Preshared Keys
Übertragungsschlüs-	Nur für Sicherheitsmodus = WEP 104

Feld	Beschreibung
sel	<p>Wählen Sie einen der in WEP-Schlüssel <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus.</p> <p>Standardwert ist <i>Schlüssel 1</i>.</p>
WEP-Schlüssel 1 - 4	<p>Nur für Sicherheitsmodus = <i>WEP 40</i>, <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein.</p> <p>Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen z. B. <i>hallo</i> für <i>WEP 40</i>, <i>teldat-wep1</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Wählen Sie aus, ob Sie WPA oder WPA 2 anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> (Standardwert): Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 wird angewendet.
Preshared Key	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>Geben Sie das WPA-Passwort ein.</p> <p>Geben Sie eine ASCII-Zeichenfolge mit 8 - 63 Zeichen ein.</p>
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA</i></p> <p>Wählen Sie aus welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): Temporal Key Integrity Protocol • <i>AES</i>: Advanced Encryption Standard. <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.</p>
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA 2</i></p>

Feld	Beschreibung
	<p>Wählen Sie aus, welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AES</i> (Standardwert): Advanced Encryption Standard. • <i>TKIP</i>: Temporal Key Integrity Protocol <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als leistungsfähiger gilt.</p>

10.1.4.2 Client Link Scan

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



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

Einstellungen Funkmodul Client Link

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

Zurück

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

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



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

Felder im Menü Scan

Feld	Beschreibung
Beschreibung des Cli-	Zeigt den Namen des von Ihnen konfigurierten Client-Links an.

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

10.1.5 Bridge-Links

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

Für **bintec W1003n**, **bintec W2003n**, **bintec W2003n-ext** und **bintec W2004n** nicht verfügbar.

Mit der Bridge-Funktionalität können Sie ein Teldat WLAN-Gerät mit einem oder mehreren anderen drahtlos verbinden. Die Entfernung, über die Sie diese drahtlose Verbindung herstellen können, kann dabei je nach den verwendeten Antennen mehrere Kilometer betragen.

**Hinweis**

Verwenden Sie stets die mitgelieferten Antennen und Antennenkabel, um unbeabsichtigte Verstöße gegen geltendes Recht zu vermeiden. Sollten Sie spezielle Anforderungen, z. B. bezüglich der Kabellängen haben, wenden Sie sich bitte an Ihren Händler oder an die Teldat GmbH.

Generell dienen Bridges dazu, verschiedene LAN-Segmente auf Layer 2 des OSI-7-Schichten-Modells miteinander zu verbinden. Die Besonderheit von Teldat Bridges ist, dass zwischen diesen Segmenten Distanzen von mehreren Kilometern liegen können, ohne ein Kabel für diese Entfernungen zu benötigen.

Wenn Sie einen Wireless-Port im Bridge-Modus betreiben, kann dieser ausschließlich für einen Bridge-Link verwendet werden. Das bedeutet:

- Der Port verfügt über keinen Netzwerknamen.
- An diesem Port können sich keine Wireless Clients assoziieren (anmelden).
- Es existiert keine Node Table für den Port (da es keine Clients gibt).
- Es existiert keine Access Control List (ACL) für diesen Port.

Dieser Port wird ausschließlich zu dem von Ihnen konfigurierten Port der Partner-Bridge Verbindung aufnehmen, und auch nur von diesem Port Verbindungen akzeptieren.

Dabei bieten die Teldat Bridges Übertragungsraten, die weit über die Möglichkeiten von ISDN S0, ISDN S2M und ADSL hinausgehen. Die Highspeed-Bridge übertrifft dabei sogar Standard Ethernet (10BaseT, 10Base2, 10Base5).

**Achtung**

Schließen Sie nie zwei Bridges, die im Funk eine Verbindung aufgebaut haben, an dasselbe LAN Segment an. Das führt unweigerlich zu einer Überlastung Ihres Netzwerkes, so dass jeglicher Netzwerkverkehr zum Erliegen kommt.

Um Ihnen einen Überblick darüber zu geben, welche Möglichkeiten Ihnen durch den Einsatz von Teldat Bridges offen stehen, werden hier einige realisierbare Netzwerk-Topologien dargestellt.

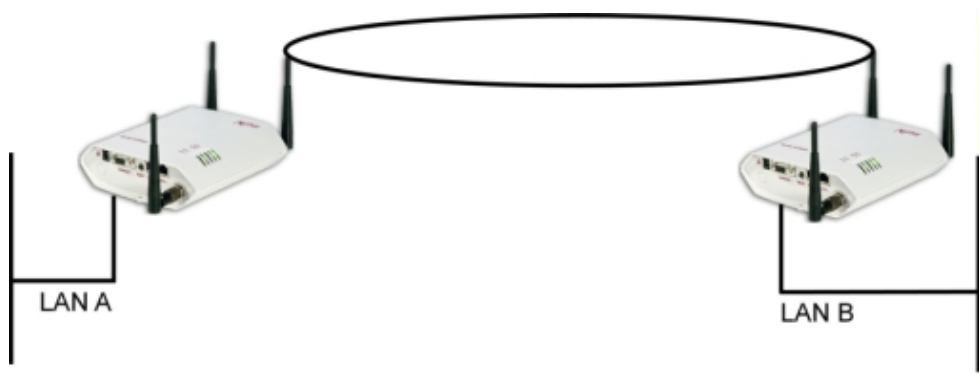


Abb. 76: Point-to-Point-Topologie

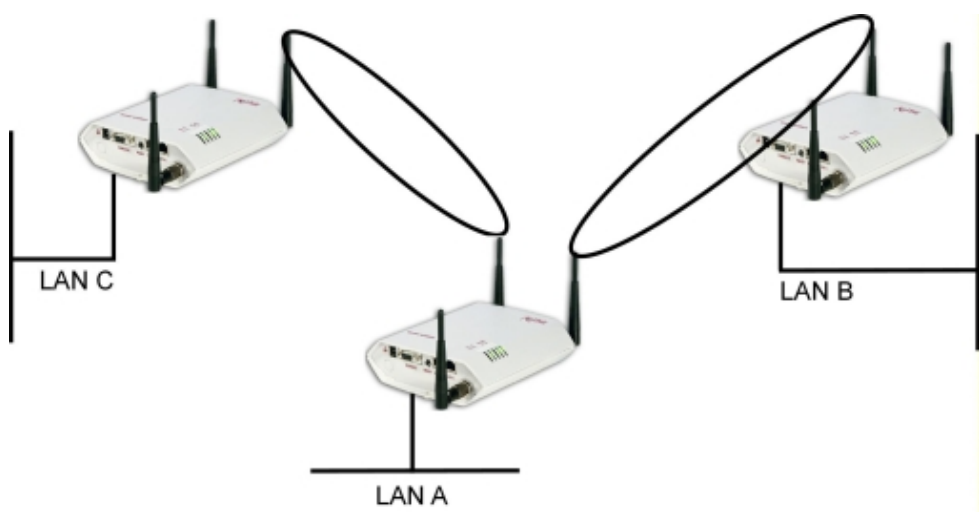


Abb. 77: Point-to-Multipoint-Topologie

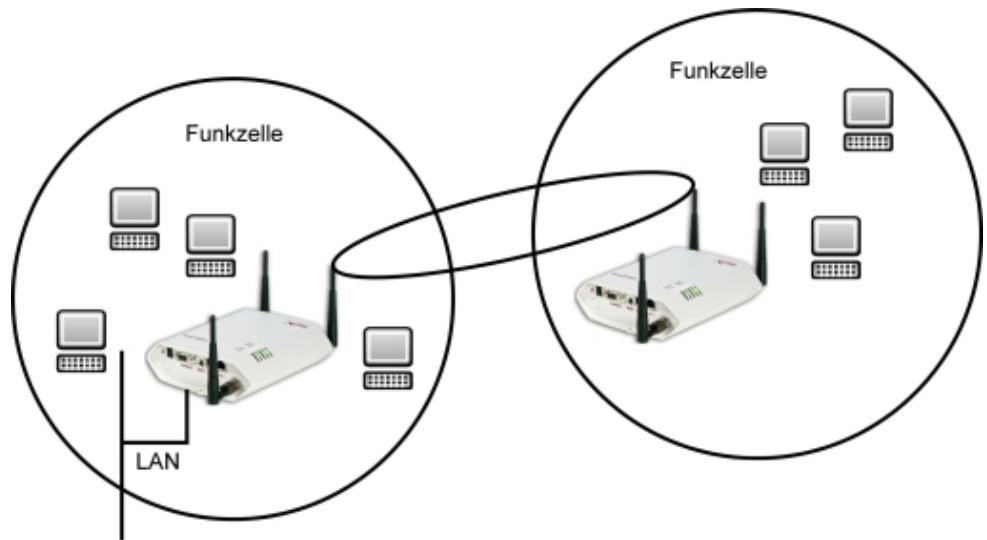


Abb. 78: Wireless Backbone

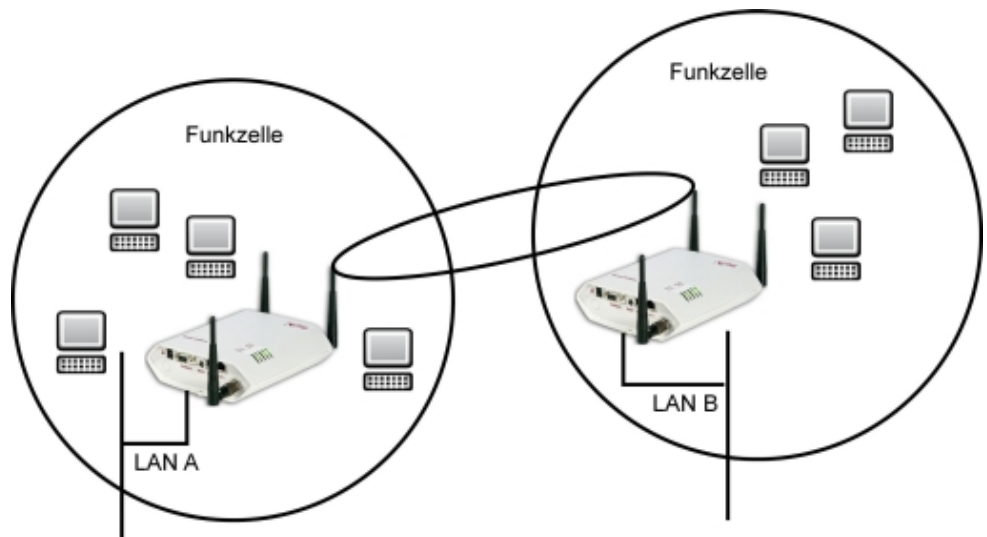


Abb. 79: Wireless Bridge mit Anbindung von Wireless Clients

Um einen Wireless Link mit Teldat Bridges herstellen zu können, muss zwischen den Antennen beider Seiten freie Sicht bestehen. In Fachkreisen redet man hier von Line-of-Sight, kurz LOS.

Der Begriff "Line-of-Sight" bezeichnet dabei nicht nur eine geradlinige Sichtverbindung, sondern eine Art "Tunnel", der nicht durch Hindernisse beeinträchtigt werden darf. Bei diesem "Tunnel" handelt es sich um die sogenannte 1. Fresnel-Zone. Die Fresnel-Zone hat

die Form einer um ihre Längsachse rotierten Ellipse. Mindestens 60 % der 1. Fresnel-Zone müssen freibleiben. Der Radius (bzw. die kleine Halbachse) hängt von der verwendeten Frequenz und der Distanz zwischen den Antennen ab.

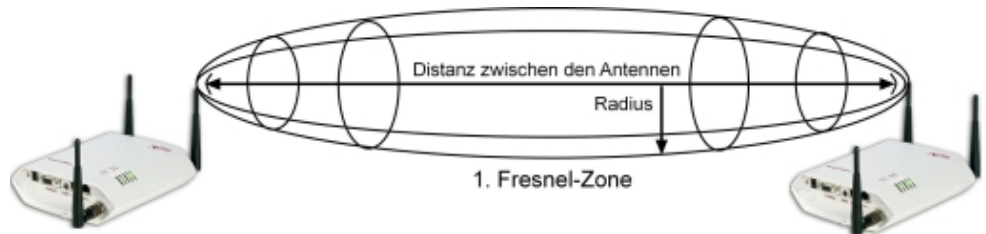


Abb. 80: 1. Fresnel-Zone

Beispiel: Radius der 1. Fresnel-Zone in Abhängigkeit von der Entfernung zur Sendeantenne für einen Antennenabstand von 5 km bei 2,45 GHz.

Beispiel 1

Abstand zur Sendeantenne [km]	Radius der 1. Fresnel-Zone [m]	Radius bei 60 % 1. Fresnel-Zone [m]
0,250	5,4	4,2
0,500	7,4	5,7
0,750	8,8	6,8
1,000	9,9	7,7
1,250	10,7	8,3
1,500	11,3	8,8
1,750	11,8	9,1
2,000	12,1	9,4
2,250	12,3	9,5
2,500	12,4	9,6
2,750	12,3	9,5
3,000	12,1	9,4
3,250	11,8	9,1
3,500	11,3	8,8
3,750	10,7	8,3
4,000	9,9	7,7
4,250	8,8	6,8
4,500	7,4	5,7

Abstand zur Sendeantenne [km]	Radius der 1. Fresnel-Zone [m]	Radius bei 60 % 1. Fresnel-Zone [m]
4,750	5,4	4,2

Beispiel: Radius der Fresnel-Zone in Abhängigkeit von der Entfernung zur Sendeantenne für eine Distanz von 700 m bei 2,45 GHz.

Beispiel 2

Abstand zur Sendeantenne [km]	Radius der 1. Fresnel-Zone [m]	Radius bei 60 % 1. Fresnel-Zone [m]
100	1,6	1,25
200	2,1	1,6
300	2,3	1,75
400	2,3	1,75
500	2,	1,6
600	1,6	1,25



Hinweis

Bitte achten Sie beim Aufbau eines Bridge-Links darauf, dass keine Hindernisse (auch keine Bäume) in die Fresnel-Zone ragen. Sollte das der Fall sein, geht die Übertragungsrate zurück, bis hin zum Ausfall der Strecke.

Bei kurzen Distanzen innerhalb von Gebäuden ist die Berücksichtigung der LOS nicht unbedingt nötig, da der Radius der Fresnel- Zone hier sehr klein wird.

Wurden diese Voraussetzungen beachtet, kann der Link ohne weitere Einschränkungen aufgebaut und aufrechterhalten werden. Insbesondere sind die Links mit Teldat Bridges völlig unbeeinflusst von den jeweiligen Witterungsverhältnissen.



Hinweis

Verwenden Sie bei einer Bridge-Strecke grundsätzlich den markierten Antennenanschluss. Hierbei handelt es sich um den primären Anschluss des Gerätes.

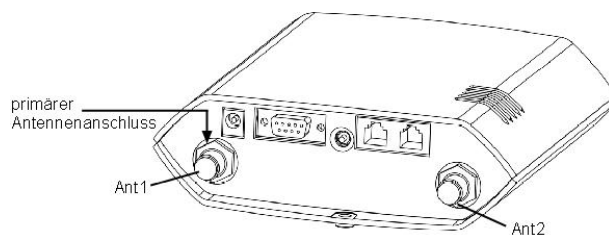



Abb. 81: Antennenanschluss

Auf der Geräterückseite findet Sie ein Aufkleber auf dem die beiden Antennen beschriftet sind. Die primäre Antenne trägt die Bezeichnung **Ant 1**.

10.1.5.1 Bearbeiten oder Neu

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

Einstellungen Funkmodul Bridge-Links

Basisparameter	
Bridge-Link-Beschreibung	<input checked="" type="checkbox"/> Benutze Standard
Fernkonfiguration	<input type="radio"/> Nicht erlaubt <input checked="" type="radio"/> Erlaubt
Bridge-Sicherheitseinstellungen	
Schutz	TKIP
Preshared Key	<input checked="" type="checkbox"/> Automatisch
Entfernter Partner	
Entfernte MAC-Adresse	00:00:00:00:00:00

OK Abbrechen

Abb. 82: Wireless LAN->WLAN->Bridge-Links->->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Bridge-Link-Beschreibung	<p>Geben Sie einen Namen für den Bridge Link ein.</p> <p>Ist die Option <i>Benutze Standard</i> aktiviert, wird der automatisch generierte Name der Schnittstelle übernommen.</p> <p>Ist die Option nicht aktiviert, können Sie einen geeigneten Na-</p>

Feld	Beschreibung
	<p>men in das Eingabefeld eintragen.</p> <p>Standardmäßig ist die Option <i>Benutze Standard</i> aktiviert.</p>
Fernkonfiguration	<p>Wählen Sie aus, ob der Aufbau eines Bridge-Links von einer entfernten Bridge erlaubt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erlaubt</i> (Standardwert): Es ist möglich, von einer entfernten Bridge einen Bridge Link herzustellen. • <i>Nicht erlaubt</i>: Es ist nicht möglich, von einer entfernten Bridge einen Bridge Link herzustellen.

Felder im Menü Bridge-Sicherheitseinstellungen

Feld	Beschreibung
Schutz	<p>Wählen Sie aus, ob und wenn ja welche Verschlüsselungsmethode auf diesem Bridge Link angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): Temporal Key Integrity Protocol. • <i>AES</i>: Advanced Encryption Standard. <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als "performanter" gilt.</p>
Preshared Key	Geben Sie das Passwort für diesen Bridge-Link ein. Sie können den Preshared Key auch automatisch beziehen.

Felder im Menü Entfernter Partner

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

10.1.5.2 Bridge-Links Scan

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



Über dieses Symbol öffnen Sie das Menü **Automatische Bridge-Link-Konfiguration**.

Einstellungen Funkmodul Bridge-Links

Automatische Bridge-Link-Konfiguration	
Bridge-Link-Beschreibung	wds1-0
Max. Scan-Dauer	<input type="text" value="120"/> Sekunden
Aktion	[Scan]
Beschreibung	Entfernter Link
Name	Entferntes Gerät
Signal	dBm
Entfernte	MAC-Adresse
Entfernter	Link aktiviert
Verbunden	Aktion

OK
Abbrechen
Zurück

Abb. 83: Wireless LAN->WLAN->Bridge-Links->Automatische Bridge-Link-Konfiguration

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

Das Menü **Wireless LAN->WLAN->Bridge-Links->Automatische Bridge-Link-Konfiguration** besteht aus den folgenden Feldern:

Felder im Menü Automatische Bridge-Link-Konfiguration

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des von Ihnen konfigurierten Bridge-Links an.
Max. Scan-Dauer	<p>Geben Sie die maximale Zeit in Sekunden an, die der Scan durchgeführt werden soll.</p> <p>Mögliche Werte sind <i>10</i> bis <i>600</i>.</p> <p>Standardwert ist <i>120</i>.</p>
Aktion	<p>Lösen Sie den Scan durch Klicken von Scan aus.</p> <p>Bei sachgerechter Installation der Antennen auf beiden Seiten und freier LOS wird die Bridge verfügbare Bridges finden und in der folgenden Liste anzeigen.</p> <p>Sollte die Partner-Bridge nicht gefunden werden, überprüfen Sie die Line-of-Sight und die Antenneninstallation. Führen Sie dann erneut Scan aus. Der Partner sollte daraufhin gefunden werden.</p>

Feld	Beschreibung
Beschreibung Entfernter Link	Zeigt den Namen des auf der entfernten Bridge konfigurierten Bridge-Links an.
Name Entferntes Gerät	Zeigt den Namen der entfernten Bridge an.
Signal dBm	Zeigt die Signalstärke des erkannten Bridge-Links an.
Entfernte MAC-Adresse	Zeigt die MAC-Adresse der entfernten Bridge an.
Entfernter Link aktiviert	Zeigt den Status des Links auf der entfernten Bridge an.
Verbunden	Zeigt den Status des Links auf Ihrer Bridge an.
Aktion	Sie können den Status des Bridge-Links verändern. In diesem Feld werden die zur Verfügung stehenden Aktionen angezeigt.

10.2 Verwaltung

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

10.2.1 Grundeinstellungen

The screenshot shows a dialog box titled "Grundeinstellungen". Inside, there is a section for "WLAN Administration" with a "Region" dropdown menu currently set to "Germany". At the bottom of the dialog, there are two buttons: "OK" and "Abbrechen".

Abb. 84: **Wireless LAN->Verwaltung->Grundeinstellungen**

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

Felder im Menü WLAN Administration

Feld	Beschreibung
Region	Wählen Sie das Land, in welchem der Access Point betrieben werden soll. Mögliche Werte sind alle auf dem Wireless-Modul des Geräts vorkonfigurierten Länder.

Feld	Beschreibung
	<p>Der Bereich der auswählbaren Kanäle (Kanal im Menü Wireless LAN->WLAN->Einstellungen Funkmodul) variiert je nach Ländereinstellung.</p> <p>Standardwert ist <i>Germany</i>.</p>

Kapitel 11 Wireless LAN Controller

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

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

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

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

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

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

11.1 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.

11.1.1 Grundeinstellungen

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

Der Wireless LAN Controller verwendet folgende Einstellungen:

Region

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

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

Schnittstelle

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

DHCP-Server

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

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

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

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

IP-Adressbereich

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

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

11.1.2 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.

11.1.3 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.

11.1.3.1 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.

11.1.4 Automatische Installation starten

Sie sehen eine Liste der gefundenen Access Points.

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

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

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

Standort

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

Zugewiesene Drahtlosnetzwerke (VSS)

Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.

Folgende Parameter stehen im Menü Funkmodul 1 zur Verfügung:

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

Betriebsmodus

Wählen Sie den Betriebsmodus des Funkmoduls.

Mögliche Werte:

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

- *Aus*: Das Funkmodul ist nicht aktiv.

Aktives Funkmodulprofil

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

Kanal

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

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



Hinweis

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

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

Sendeleistung

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

Mit **OK** übernehmen Sie die Einstellungen.

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

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



Hinweis

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

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

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

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

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

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

11.2 Controller-Konfiguration

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

11.2.1 Allgemein

Allgemein

Grundeinstellungen	
Region	Germany ▼
Schnittstelle	LAN_EN1-0 ▼
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 ▼

OK
Abbrechen

Abb. 85: 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> <p>Der Bereich der verwendbaren Kanäle variiert je nach Länder-einstellung.</p> <p>Standardwert ist <i>Germany</i>.</p>
Schnittstelle	<p>Wählen Sie die Schnittstelle, die für den Wireless Controller verwendet werden soll.</p>
DHCP-Server	<p>Wählen Sie aus, ob ein externer DHCP-Server die IP-Adressen an die APs vergeben soll bzw. ob Sie selbst feste IP-Adressen vergeben wollen. Alternativ können Sie Ihr Gerät als DHCP-Server verwenden. Bei diesem internen DHCP-Server ist die CAPWAP Option 138 aktiv, um die Kommunikation zwischen Master und Slaves zu ermöglichen.</p>

Feld	Beschreibung
	<p>Hinweis: Stellen Sie bei Nutzung eines externen DHCP-Servers sicher, dass CAPWAP Option 138 aktiv ist.</p> <p>Wenn Sie z. B. ein Teldat Gateway als DHCP-Server verwenden wollen, klicken Sie im GUI Menü dieses Geräts unter Lokale Dienste->DHCP-Server->DHCP Pool->Neu->Erweiterte Einstellungen im Feld DHCP-Optionen auf die Schaltfläche Hinzufügen. Wählen Sie als Option <i>CAPWAP Controller</i> und tragen Sie im Feld Wert die IP-Adresse des WLAN Controllers ein.</p> <p>Wenn Sie in Ihrem Netzwerk statische IP-Adressen verwenden, müssen Sie diese IP-Adressen auf allen APs von Hand eingeben. Die IP-Adresse des Wireless LAN Controllers müssen Sie bei jedem AP im Menü Systemverwaltung->Globale Einstellungen->System im Feld Manuelle IP-Adresse des WLAN-Controller eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Extern oder statisch</i> (Standardwert): Ein externer DHCP-Server mit aktiver CAPWAP Option 138 vergibt die IP-Adressen an die APs oder Sie vergeben statische IP-Adressen an die APs. • <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</p>

Feld	Beschreibung
	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.
Slave-AP-LED-Modus	<p>Diese Funktion ist nur für die Access-Points bintec W1003n, bintec W2003n, bintec W2003n-ext und bintec W2004n verfügbar.</p> <p>Wählen Sie das Leuchtverhalten der Slave-AP-LEDs.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Status</i> (Standardwert): Nur die Status-LED blinkt einmal in der Sekunde. • <i>Blinkend</i>: Die LEDs zeigen ihr Standardverhalten. • <i>Aus</i>: Alle LEDs sind deaktiviert.

11.3 Slave-AP-Konfiguration

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

11.3.1 Slave Access Points

Slave Access Points Funkmodulprofile Drahtlosnetzwerke (VSS)

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

Ansicht pro Seite Filtern in **Los**

Standort	Name	IP-Adresse	LAN-MAC-Adresse	Kanal	Kanalsuche	Status	Aktion
1:	WI2040n	10.0.0.232	00:01:cd:06:76:fa	auto (Ch.100)		● Managed	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="🗑️"/> <input type="button" value="📄"/>


Seite: 1, Objekte: 1 - 1

Abb. 86: 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 Kli-

cken 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.

11.3.1.1 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	WI2040n				
Standort	<input type="text"/>				
Name	WI2040n				
Beschreibung	<input type="text"/>				
CAPWAP-Verschlüsselung	<input checked="" type="checkbox"/> Aktiviert				
Funkmodul1					
Betriebsmodus	<input checked="" type="radio"/> Ein <input 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;"> <tr> <td style="width: 50%;">Profil</td> <td style="width: 50%;">MAC-Adresse</td> </tr> <tr> <td colspan="2" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </table>	Profil	MAC-Adresse	<input type="button" value="Hinzufügen"/>	
Profil	MAC-Adresse				
<input type="button" value="Hinzufügen"/>					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>					

Abb. 87: 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 unter-</p>

Feld	Beschreibung
	<p>stützen.</p> <p>Mögliche Werte (entsprechend dem gewählten Funkmodulprofil):</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>2,4 GHz In/Outdoor</i> <p>Mögliche Werte sind <i>1 bis 13</i> und <i>Auto</i> (Standardwert).</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz Indoor</i> <p>Mögliche Werte sind <i>36, 40, 44, 48</i> und <i>Auto</i> (Standardwert)</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Outdoor</i> <p>Hier ist nur die Option <i>Auto</i> möglich.</p>
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> • <i>11 dBm</i> • <i>14 dBm</i> • <i>16 dBm</i>
Zugewiesene Drahtlosnetzwerke (VSS)	<p>Zeigt die aktuell zugewiesenen Drahtlosnetzwerke.</p>

11.3.2 Funkmodulprofile


Slave Access Points Funkmodulprofile Drahtlosnetzwerke (VSS)				
Funkmodulprofil	Konfigurierte Funkmodule	Frequenzband	Drahtloser Modus	
2.4 GHz Radio Profile	0	2,4 GHz In/Outdoor	802.11 b/g/n	
5 GHz Radio Profile	0	5 GHz Indoor	802.11 a/n	 
<input type="button" value="Neu"/>				

Abb. 88: 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**).

11.3.2.1 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 type="text"/>
Betriebsmodus	Access-Point ▼
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 <input type="text"/> ms
DTIM Period	2 <input type="text"/>
RTS Threshold	2347 <input type="text"/>
Short Guard Interval	<input type="checkbox"/> Aktiviert
Short Retry Limit	7 <input type="text"/>
Long Retry Limit	4 <input type="text"/>
Fragmentation Threshold	2346 <input type="text"/> Bytes
Wiederkehrender Hintergrund-Scan	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 89: **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	Legen Sie fest, in welchem Modus das Funkmodulprofil betrieben werden soll. Mögliche Werte:

Feld	Beschreibung
	<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 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 = <i>2,4 GHz In/Outdoor</i></p> <p>Wählen Sie aus, wieviele Kanäle verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>20 MHz</i> (Standardwert): Ein Kanal mit 20 MHz Bandbreite wird verwendet. • <i>40 MHz</i>: Zwei Kanäle mit je 20 MHz Bandbreite werden verwendet. Dabei dient ein Kanal als Kontrollkanal und der andere als Erweiterungskanal.
Anzahl der Spatial Streams	<p>Wählen Sie aus, wieviele Datenströme parallel verwendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>3</i>: Drei Datenströme werden verwendet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • 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 = <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 Frequenzband = <i>5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor</i> oder <i>5,8 GHz Outdoor</i></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 Senderressourcen des Access Points intelligent auf die verbundenen Clients verteilt werden. Dadurch lässt sich verhindern, dass ein leistungsfähiger Client (z. B. ein 802.11n-Client) nur geringen Durchsatz erzielt, da ein weniger leistungsfähiger Client (z. B. ein 802.11a-Client) bei der Zuteilung gleich behandelt wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Diese Funktion wirkt sich lediglich auf nicht priorisierte Frames der WMM-Klasse "Background" aus.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Kanalplan	<p>Wählen Sie den gewünschten Kanalplan aus.</p> <p>Der Kanalplan trifft bei der Kanalwahl eine Vorauswahl. Dadurch wird sichergestellt, dass sich keine Kanäle überlappen, d.h. dass zwischen den verwendeten Kanälen ein Abstand von vier Kanälen eingehalten wird. Dies ist nützlich, wenn mehrere Access Points eingesetzt werden, deren Funkzellen sich überlappen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i>: Alle Kanäle können bei der Kanalwahl gewählt werden. • <i>Auto</i>: Abhängig von der Region, vom Frequenzband, vom drahtlosen Modus und von der Bandbreite werden diejenigen Kanäle zur Verfügung gestellt, die vier Kanäle Abstand haben. • <i>Benutzerdefiniert</i>: Sie können die gewünschten Kanäle selbst auswählen.
Benutzerdefinierter Kanalplan	<p>Nur für Kanalplan = <i>Benutzerdefiniert</i></p> <p>Hier werden die aktuell gewählten Kanäle angezeigt.</p> <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>Standardwert ist 100.</p>
DTIM Period	<p>Geben Sie das Intervall für die Delivery Traffic Indication Message (DTIM) an.</p>

Feld	Beschreibung
	<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>

Feld	Beschreibung
	Der Standardwert ist <i>2346</i> .
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>

11.3.3 Drahtlosnetzwerke (VSS)

Slave Access Points		Funkmodulprofile		Drahtlosnetzwerke (VSS)	
VSS-Beschreibung	Netzwerkname (SSID)	Anzahl der zugeordneten Funkmodule	Sicherheit	Status	Aktion
vss-1	default	0	WPA-PSK		
Nicht zugewiesenes VSS allen Funkmodulen zuweisen		<input type="button" value="START"/>			
<input type="button" value="Neu"/>					


Abb. 90: 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.

11.3.3.1 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 <input type="button" value="v"/>
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 <input type="button" value="v"/>
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

Abb. 91: 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)	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) übertragen werden soll.

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Key • <i>WPA-Enterprise</i>: 802.11x
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>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>teldat-wep104</i> für <i>WEP 104</i>.</p>
WPA-Modus	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i></p> <p>Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>WPA</i> und <i>WPA 2</i> (Standardwert): WPA und WPA 2 können angewendet werden. • <i>WPA</i>: Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> und für WPA-Modus = <i>WPA</i> und <i>WPA 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.
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.
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>

Feld	Beschreibung
	<p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Client-Lastverteilung

Feld	Beschreibung
<p>Max. Anzahl Clients - Hard Limit</p>	<p>Geben Sie die maximale Anzahl an Clients ein, die sich mit diesem Drahtlosnetzwerk (SSID) verbinden dürfen.</p> <p>Die Anzahl der Clients, die sich maximal an einem Funkmodul anmelden können, ist abhängig von der Spezifikation des jeweiligen WLAN-Moduls. Diese Anzahl verteilt sich auf alle auf diesem Radiomodul Drahtlosnetzwerke. Ist die maximale Anzahl an Clients erreicht, können keine neuen Drahtlosnetzwerke mehr angelegt werden und es erscheint ein Warnhinweis.</p> <p>Mögliche Werte sind ganze Zahlen von 1 bis 254.</p> <p>Der Standardwert ist 32.</p>
<p>Max. Anzahl Clients - Soft Limit</p>	<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>
<p>Auswahl des Client-Bands</p>	<p>Diese Funktion wird nicht von allen Geräten unterstützt.</p> <p>Diese Funktion erfordert eine Konfiguration mit zwei Radiomo-</p>

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

Felder im Menü MAC-Filter

Feld	Beschreibung
Zugriffskontrolle	<p>Wählen Sie aus, ob für dieses Drahtlosnetzwerk nur bestimmte Clients zugelassen werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erlaubte Adressen	<p>Legen Sie Einträge mit Hinzufügen an und geben Sie die MAC-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.</p>
Dynamische Black List	<p>Mithilfe der Funktion Dynamische Black List ist es möglich, Clients, die sich möglicherweise unbefugter Zugriff auf das Netzwerk verschaffen wollen, zu erkennen und für einen bestimmten Zeitraum zu sperren. Ein Client wird dann gesperrt, wenn die Anzahl erfolgloser Anmeldeversuche innerhalb einer definierten Zeit eine bestimmte Anzahl überschreitet. Diese Grenzwerte ebenso wie die Dauer der Sperrung können konfiguriert werden.</p>

Feld	Beschreibung
	<p>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>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>

11.4 Monitoring

Dieses Menü dient zur Überwachung Ihrer WLAN-Infrastruktur.

11.4.1 Aktive Clients

[Aktive Clients](#)
[Drahtlosnetzwerke \(VSS\)](#)
[Client-Verwaltung](#)
[Benachbarte APs](#)
[Rogue APs](#)
[Rogue Clients](#)

Automatisches Aktualisierungsintervall Sekunden [Übernehmen](#)

Ansicht pro Seite Filtern in gleich [Los](#)

Standort	Name des Slave-APs	VSS	Client MAC	Client-IP-Adresse	Signal : Noise (dBm)	Status	Uptime
Seite: 1							

Abb. 92: 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, VSS, Client MAC, Client-IP-Adresse, Signal : Noise (dBm), Status, Uptime**.

Mögliche Werte für Status

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

11.4.2 Drahtlosnetzwerke (VSS)


[Aktive Clients](#)
[Drahtlosnetzwerke \(VSS\)](#)
[Client-Verwaltung](#)
[Benachbarte APs](#)
[Rogue APs](#)
[Rogue Clients](#)

Ansicht pro Seite Filtern in gleich [Los](#)

Standort	Name des Slave-APs	VSS	MAC-Adresse (VSS)	Kanal	Status
Seite: 1					

Abb. 93: Wireless LAN Controller->Monitoring->Drahtlosnetzwerke (VSS)

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

Zusätzlich werden Ihnen die **Load Balancing Statistics** angezeigt (**2,4/5-GHz-Übergang**, **Abgewiesene Clients soft/hard**, **Moved clients**, **Delete statistics**). Sie sehen 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. Mithilfe des -Symbols können Sie die Werte für den gewünschten Eintrag löschen.

11.4.3 Lastverteilung



Abb. 94: Wireless LAN Controller->Monitoring+Lastverteilung

Im Menü **Wireless LAN Controller->Monitoring+Lastverteilung** wird eine Übersicht des **Lastverteilung** 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.

11.4.4 Benachbarte APs



Abb. 95: Wireless LAN Controller->Monitoring->Benachbarte APs

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



Hinweis

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

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

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

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

11.4.5 Rogue APs

Abb. 96: Wireless LAN Controller->Monitoring->Rogue APs

Im Menü **Wireless LAN Controller->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.


11.4.6 Rogue Clients

Abb. 97: Wireless LAN Controller->Monitoring+Rogue Clients

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

Mögliche Werte für Rogue Clients

Status	Bedeutung
MAC-Adresse des Rogue Clients	Zeigt die MAC-Adresse des Clients an, der sich auf der Blacklist befindet.
SSID	Zeigt die beteiligten SSID an.
Angegriffener Access Point	Zeigt den betroffenen AP an.

Status	Bedeutung
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 der 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.

11.4.6.1 Neu

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

[Aktive Clients](#)
[Drahtlosnetzwerke \(VSS\)](#)
[Client-Verwaltung](#)
[Benachbarte APs](#)
[Rogue APs](#)
[Rogue Clients](#)

Neuer Eintrag in die Blacklist

MAC-Adresse des Rogue Clients	<input type="text"/>
Netzwerkname (SSID)	Eine auswählen ▾

Abb. 98: **Wireless LAN Controller->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.

11.5 Wartung

Dieses Menü dient zur Wartung Ihrer managed APs.

11.5.1 Firmware-Wartung

Firmware-Wartung

Managed Access Points						
Firmware aktualisieren Alle auswählen / Alle deaktivieren	Standort ^	Gerät	IP-Adresse	LAN-MAC-Adresse	Firmware-Version	Status
Aktion	Systemssoftware aktualisieren ▼					
Quelle	HTTP-Server ▼					
URL	<input style="width: 100%;" type="text"/>					
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>						

Abb. 99: **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. • <i>Aktuelle Software vom Teldat-Server</i>: Die Datei liegt auf dem offiziellen Teldat-Update-Server. (Nur für Aktion = <i>Systemsoftware aktualisieren</i>) • <i>TFTP-Server</i>: Die Datei ist bzw. wird auf dem TFTP-Server gespeichert, der in der URL angegeben wird.
URL	<p>Nur für Quelle = <i>HTTP-Server</i> oder <i>TFTP-Server</i></p> <p>Geben Sie die URL des Servers ein, von dem die Systemsoftware-Datei geladen werden soll bzw. auf dem die Konfigurationsdatei gespeichert werden soll.</p>

Kapitel 12 Netzwerk

12.1 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.

12.1.1 Konfiguration von IPv4-Routen

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

12.1.1.1 Bearbeiten oder Neu

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

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

Abb. 100: Netzwerk->Routen+Konfiguration von IPv4-Routen->Neu mit Erweiterte Route = Standard.

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


Konfiguration von IPv4-Routen		IPv4-Routing-Tabelle	Optionen
Basisparameter			
Routentyp	Netzwerkroute via Schnittstelle ▾		
Schnittstelle	Keine ▾		
Routenklasse	<input type="radio"/> Standard <input checked="" type="radio"/> Erweitert		
Routenparameter			
Ziel-IP-Adresse/Netzmaske	/		
Lokale IP-Adresse	0.0.0.0		
Metrik	1 ▾		
Erweiterte Routenparameter			
Beschreibung			
Quellschnittstelle	Beliebig ▾		
Quell-IP-Adresse/Netzmaske	0.0.0.0 255.255.255.0		
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. 101: Netzwerk->Routen+Konfiguration von IPv4-Routen->Neu mit Erweitert = Aktiviert

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

Feld im Menü Grundeinstellungen

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

Feld	Beschreibung
	<p>Informationen werden vollständig vom DHCP-Server übernommen. Lediglich erweiterte Parameter können zusätzlich konfiguriert werden. Diese Route bleibt von weiteren für diese Schnittstelle angelegten Routen unverändert und wird parallel mit diesen in die Routing-Tabelle übernommen.</p> <ul style="list-style-type: none"> • <i>Vorlage für Host-Route per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Host ergänzt. • <i>Vorlage für Netzwerkroute per DHCP</i>: Die per DHCP empfangenen Einstellungen werden um Routing-Informationen zu einem bestimmten Netzwerk ergänzt. <div data-bbox="539 635 1316 925" style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> Hinweis</p> <p>Durch dem Ablauf des DHCP Leases oder durch einen Neustart des Geräts werden die Routen, die aus der Kombination von DHCP- und hier vorgenommenen Einstellungen entstehen, zunächst wieder aus dem aktiven Routing gelöscht. Mit einer erneuten DHCP-Konfiguration werden sie dann neu generiert und wieder aktiviert.</p> </div>
Routenklasse	<p>Wählen Sie die Art der Routenklasse aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i>: Definiert eine Route mit den Standardparametern. • <i>Erweitert</i>: Wählen Sie aus, ob die Route mit erweiterten Parametern definiert werden soll. Ist die Funktion aktiv, wird eine Route mit erweiterten Routing-Parametern wie Quell-Schnittstelle und Quell-IP-Adresse sowie Protokoll, Quell- und Ziel-Port, Art des Dienstes (Type of Service, TOS) und der Status der Geräte-Schnittstelle angelegt.

Felder im Menü Routenparameter

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

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

Felder im Menü Erweiterte Routenparameter

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

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Privilegiert</i>: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • <i>Server</i>: Eingabe von Server Port-Nummern: 5000 ... 32767. • <i>Clients 1</i>: Eingabe von Client Port-Nummern: 1024 ... 4999. • <i>Clients 2</i>: Eingabe von Client Port-Nummern: 32768 ... 65535. • <i>Nicht privilegiert</i>: Eingabe von unprivilegierten Port-Nummern: 1024 ... 65535. <p>Geben Sie entsprechend der Auswahl des Port-Nummern-Bereichs in Port (einzelner bzw. Anfangsport) und ggf. in bis Port (Endport) die entsprechenden Werte ein.</p>
DSCP-/TOS-Wert	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F. <p>Geben Sie für <i>DSCP-Binärwert</i>, <i>DSCP-Dezimalwert</i>, <i>DSCP-Hexadezimalwert</i>, <i>TOS-Binärwert</i>, <i>TOS-Dezimalwert</i> und <i>TOS-Hexadezimalwert</i> den entsprechenden Wert ein.</p>

Feld	Beschreibung
Modus	<p>Wählen Sie aus, wann die in Routenparameter->Schnittstelle definierte Schnittstelle benutzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Wählen und warten</i> (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. • <i>Verbindlich</i>: Die Route ist immer benutzbar. • <i>Wählen und fortfahren</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist. • <i>Nie einwählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. • <i>Immer wählen</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. In diesem Fall wird über eine alternative Schnittstelle mit schlechterer Metrik geroutet, bis die Schnittstelle "aktiv" ist.

12.1.2 IPv4-Routing-Tabelle

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


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

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

Seite: 1, Objekte: 1 - 2

Abb. 102: **Netzwerk->Routen+IPv4-Routing-Tabelle**

Felder im Menü IPv4-Routing-Tabelle

Feld	Beschreibung
Ziel-IP-Adresse	Zeigt die IP-Adresse des Ziel-Hosts bzw. Zielnetzes an.
Netzmaske	Zeigt die Netzmaske des Ziel-Hosts bzw. Zielnetzes an.
Gateway	Zeigt die Gateway IP-Adresse an. Im Falle von per DHCP erhaltenen Routen wird hier nichts angezeigt.
Schnittstelle	Zeigt die Schnittstelle an, welche für diese Route verwendet wird.
Metrik	Zeigt die Priorität der Route an. Je niedriger der Wert, desto höhere Priorität besitzt die Route.
Routentyp	Zeigt den Routentyp an.
Erweiterte Route	Zeigt an, ob eine Route mit erweiterten Parametern konfiguriert worden ist.
Löschen	Mithilfe des  -Symbols können Sie Einträge löschen.

12.1.3 Optionen

Überprüfung der Rückroute

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

Konfiguration von IPv4-Routen | IPv4-Routing-Tabelle | Optionen

Überprüfung der Rückroute

Modus

Für alle Schnittstellen aktivieren
 Für bestimmte Schnittstellen aktivieren
 Für alle Schnittstellen deaktivieren

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

Nr.	Schnittstelle	Überprüfung der Rückroute
1	br0	<input type="checkbox"/> Aktiviert

Seite: 1, Objekte: 1 - 1

Abb. 103: Netzwerk->Routen->Optionen

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

Felder im Menü Überprüfung der Rückroute

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

12.2 NAT

Network Address Translation (NAT) ist eine Funktion Ihres Geräts, um Quell- und Zieladressen von IP-Paketen definiert umzusetzen. Mit aktiviertem NAT werden weiterhin IP-Verbindungen standardmäßig nur noch in einer Richtung, ausgehend (forward) zugelassen (=Schutzfunktion). Ausnahmeregeln können konfiguriert werden (in *NAT-Konfiguration* auf Seite 243).

12.2.1 NAT-Schnittstellen

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

Schnittstelle	NAT aktiv	Loopback aktiv	Verwerfen ohne Rückmeldung	PPTP-Passthrough	Portweiterleitungen
LAN_EN1-0	<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

Abb. 104: **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

Feld	Beschreibung
	<p>Server Services testen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Verwerfen ohne Rückmeldung	<p>Wählen Sie aus, ob IP-Pakete stillschweigend durch NAT abgelehnt werden sollen. Ist diese Funktion deaktiviert, wird der Absender der abgelehnten IP-Pakete mit einer entsprechenden ICMP- oder TCP-RST-Nachricht informiert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
PPTP-Passthrough	<p>Wählen Sie aus, ob auch bei aktiviertem NAT der Aufbau und Betrieb mehrerer gleichzeitiger ausgehender PPTP-Verbindungen von Hosts im Netzwerk erlaubt sein soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn PPTP-Passthrough aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpunkt konfiguriert werden.</p>
Portweiterleitungen	<p>Zeigt die Anzahl der in Netzwerk->NAT->NAT-Konfiguration konfigurierten Portweiterleitungsregeln an.</p>

12.2.2 NAT-Konfiguration

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

12.2.2.1 Neu

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

NAT-Schnittstellen
NAT-Konfiguration

Basisparameter	
Beschreibung	<input type="text"/>
Schnittstelle	Beliebig ▼
Art des Datenverkehrs	eingehend (Ziel-NAT) ▼
Ursprünglichen Datenverkehr angeben	
Dienst	Benutzerdefiniert ▼
Protokoll	Beliebig ▼
Quell-IP-Adresse/Netzmaske	Beliebig ▼
Original Ziel-IP-Adresse/Netzmaske	Beliebig ▼
Substitutionswerte	
Neue Ziel-IP-Adresse/Netzmaske	Host ▼ <input style="width: 100px;" type="text" value="0.0.0.0"/>
OK Abbrechen	

Abb. 105: Netzwerk->NAT->NAT-Konfiguration ->Neu

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

Feld im Menü Basisparameter

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

Feld	Beschreibung
	ausgenommen ist.
NAT-Methode	<p>Nur für Art des Datenverkehrs = <i>ausgehend</i> (<i>Quell-NAT</i>)</p> <p>Wählen Sie die NAT-Methode für ausgehenden Datenverkehr. Ausgangspunkt für die Wahl der NAT-Methode ist ein NAT-Szenario, bei dem ein "interner" Quell-Host über die NAT-Schnittstelle eine IP-Verbindung zu einem "externen" Ziel-Host initiiert hat und bei der eine intern gültige Quelladresse und ein intern gültiger Quellport auf eine extern gültige Quelladresse und einen extern gültigen Quellport umgesetzt werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>full-cone</i> (nur UDP): Jeder beliebige externe Host darf IP-Pakete über die externe Adresse und den externen Port an die initiiierende Quelladresse und den initialen Quellport senden. • <i>restricted-cone</i> (nur UDP): Wie full-cone NAT; als externer Host ist jedoch ausschließlich der initiale "externe" Ziel-Host zugelassen. • <i>port-restricted-cone</i> (nur UDP): Wie restricted-cone NAT; es sind jedoch ausschließlich Daten vom initialen Ziel-Port zugelassen. • <i>symmetrisch</i> (Standardwert) Für beliebige Protokolle: In ausgehender Richtung werden eine extern gültige Quelladresse und ein extern gültiger Quell-Port administrativ festgelegt. In eingehender Richtung sind nur Antwortpakete innerhalb der bestehenden Verbindung zugelassen.

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

Felder im Menü **Ursprünglichen Datenverkehr angeben**

Feld	Beschreibung
Dienst	<p>Nicht für Art des Datenverkehrs = <i>ausgehend</i> (<i>Quell-NAT</i>) und NAT-Methode = <i>full-cone</i>, <i>restricted-cone</i> oder <i>port-restricted-cone</i>.</p> <p>Wählen Sie einen der vorkonfigurierten Dienste aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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> • <i>IGMP</i>

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

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


12.3 Lastverteilung

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

12.3.1 Lastverteilungsgruppen

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

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

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

12.3.1.1 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. 106: 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>

Feld	Beschreibung
	<p>Optionen:</p> <ul style="list-style-type: none"> • <i>Download</i>: Nur die Datenrate in Empfangsrichtung wird berücksichtigt. • <i>Upload</i>: Nur die Datenrate in Senderichtung wird berücksichtigt. <p>Standardmäßig sind die Optionen <i>Download</i> und <i>Upload</i> deaktiviert.</p>
Verteilungsmodus	<p>Wählen Sie aus, welchen Zustand die Schnittstellen der Gruppe haben dürfen, damit sie in die Lastverteilung einbezogen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Immer</i> (Standardwert): Auch Schnittstellen im Zustand ruhend werden einbezogen. • <i>Nur aktive Schnittstellen verwenden</i>: Es werden nur Schnittstellen im Zustand aktiv berücksichtigt.

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

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

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

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

Abb. 107: Netzwerk->Lastverteilung->Lastverteilungsgruppen->Hinzufügen

Felder im Menü Basisparameter

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

Felder im Menü Schnittstellenauswahl für Verteilung

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

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
<p>Routenselektor</p>	<p>Der Parameter Routenselektor ist ein zusätzliches Kriterium zur genaueren Definition einer Lastverteilungsgruppen. Der Schnittstelleneintrag innerhalb einer Lastverteilungsgruppen wird hierbei um eine Routinginformation erweitert. Der Routenselektor ist in bestimmten Anwendungsfällen notwendig, um die vom Router verwalteten IP Sessions eindeutig je Loadbalancing-Gruppe bilanzieren zu können. Für die Anwendung des Parameters gelten folgende Regeln:</p> <ul style="list-style-type: none"> • Ist eine Schnittstelle nur einer Lastverteilungsgruppe zugewiesen, so ist die Konfiguration des Routenselektors nicht notwendig. • Ist eine Schnittstelle mehreren Lastverteilungsgruppen zugewiesen, so ist die Konfiguration des Routenselektors zwingend erforderlich. • Innerhalb einer Lastverteilungsgruppe muss der Routenselektor aller Schnittstelleneinträge identisch konfiguriert sein. <p>Wählen Sie die Ziel-IP-Adresse der gewünschten Route aus.</p> <p>Sie können unter allen Routen und allen erweiterten Routen wählen.</p>
<p>IP-Adresse zur Nachverfolgung</p>	<p>Mit dem Parameter IP-Adresse zur Nachverfolgung können Sie eine bestimmte Route überwachen lassen.</p> <p>Mithilfe dieses Parameters kann der Lastverteilungsstatus der Schnittstelle bzw. Status der mit der Schnittstelle verbundenen Routen beeinflusst werden. Das bedeutet, dass Routen unabhängig vom Operation Status der Schnittstelle aktiviert bzw. deaktiviert werden können. Die Überwachung der Verbindung erfolgt hierbei über die Host-Überwachungsfunktion des Gateways. Zur Verwendung dieser Funktion ist somit die Konfiguration von Host-Überwachungseinträgen zwingend erforderlich. Konfiguriert werden kann dies im Menü Lokale Dienste->Überwachung->Hosts. Hierbei ist wichtig, dass im Lastverteilungskontext nur Host-Überwachungseinträge mit der Aktion Überwachung berücksichtigt werden. Über die Konfiguration der IP-Adresse zur Nachverfolgung im Menü Lastverteilung->>Last-</p>

Feld	Beschreibung
	<p>verteilungsgruppen->Erweiterte Einstellungen erfolgt die Verknüpfung zwischen der Lastverteilungsfunktion und der Host-Überwachungsfunktion. Der Lastverteilungsstatus der Schnittstelle wechselt nun in Abhängigkeit zum Status des zugewiesenen Host-Überwachungseintrages.</p> <p>Wählen Sie die IP-Adresse der Route, die überwacht werden soll.</p> <p>Sie können unter den IP-Adressen wählen, die Sie im Menü Lokale Dienste->Überwachung->Hosts->Neu unter Überwachte IP-Adresse eingegeben haben und die mit Hilfe des Feldes Auszuführende Aktion überwacht werden (Aktion = <i>überwachen</i>).</p>

12.3.2 Special Session Handling

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

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

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

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


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

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

Wenn Sie unter **Unveränderliche Parameter** für die beide Parameter **Zieladresse** und

Zielport die Standardeinstellung *aktiviert* belassen, so werden die HTTPS-Pakete mit derselben Quell-IP-Adresse wie das erste HTTPS-Paket über Port 443 zur selben **Zieladresse** über dieselbe Schnittstelle wie das erste HTTPS-Paket geroutet.

12.3.2.1 Bearbeiten oder Neu

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

Lastverteilungsgruppen Special Session Handling

Basisparameter	
Admin-Status	<input checked="" type="checkbox"/> Aktiviert
Beschreibung	<input type="text"/>
Dienst	Benutzerdefiniert ▾
Protokoll	nicht überprüfen ▾
Ziel-IP-Adresse/Netzmaske	Beliebig ▾
Ziel-Port/Bereich	-Alle- ▾ -1 bis -1
Quellschnittstelle	Keine ▾
Quell-IP-Adresse/Netzmaske	Beliebig ▾
Quell-Port/Bereich	-Alle- ▾ -1 bis -1
Special Handling Timer	900 Sekunden

Erweiterte Einstellungen

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

OK
Abbrechen

Abb. 108: **Netzwerk->Lastverteilung->Special Session Handling->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	<p>Wählen Sie aus, ob Special Session Handling aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den Eintrag ein.
Dienst	<p>Wählen Sie, falls gewünscht, einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>
Protokoll	Wählen Sie, falls gewünscht, ein Protokoll aus. Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.
Ziel-IP-Adresse/Netzmaske	<p>Definieren Sie, falls gewünscht, die Ziel-IP-Adresse und die Netzmaske der Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i>: Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Ziel-Port/Bereich	<p>Geben Sie, falls gewünscht, eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Zielport ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Ziel-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Ziel-Port-Bereich ein.

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

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

Felder im Menü **Erweiterte Einstellungen**

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

Feld	Beschreibung
	<p>Belassen Sie die Voreinstellung <i>Aktiviert</i> bei einem oder bei beiden Parametern, so muss der Wert des jeweiligen Parameters bei den später gesendeten Datenpaketen derselbe sein wie beim ersten Datenpaket.</p> <p>Sie können, falls gewünscht, einen oder beide Parameter deaktivieren.</p> <p>Der Parameter Quell-IP-Adresse muss bei später gesendeten Datenpaketen immer denselben Wert haben wie beim ersten Datenpaket. Er kann daher nicht deaktiviert werden.</p>

12.4 QoS

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

Die QoS-Konfiguration besteht aus drei Teilen:

- IP-Filter anlegen
- Daten klassifizieren
- Daten priorisieren

12.4.1 QoS-Filter

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

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

12.4.1.1 Neu

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

QoS-Filter
QoS-Klassifizierung
QoS-Schnittstellen/Richtlinien

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	Benutzerdefiniert ▾
Protokoll	Beliebig ▾
Ziel-IP-Adresse/Netzmaske	Beliebig ▾
Quell-IP-Adresse/Netzmaske	Beliebig ▾
DSCP/TOS-Filter (Layer 3)	Nicht beachten ▾
COS-Filter (802.1p/Layer 2)	Nicht beachten ▾

OK
Abbrechen

Abb. 109: Netzwerk->QoS->QoS-Filter->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung des Filters an.
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>
Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Die Option <i>Beliebig</i> (Standardwert) passt auf jedes Protokoll.</p>

Feld	Beschreibung
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Wählen Sie einen Typ aus.</p> <p>Mögliche Werte: <i>Beliebig, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply.</i></p> <p>Siehe RFC 792.</p> <p>Standardwert ist <i>Beliebig</i>.</p>
Verbindungsstatus	<p>Bei Protokoll = <i>TCP</i> können Sie ein Filter definieren, das den Status von TCP-Verbindungen berücksichtigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Hergestellt</i>: Das Filter passt auf diejenigen TCP-Pakete, die beim Routing über das Gateway keine neue TCP-Verbindung öffnen würden. • <i>Beliebig</i> (Standardwert): Das Filter passt auf alle TCP-Pakete.
Ziel-IP-Adresse/Netzmaske	<p>Geben Sie die Ziel-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p>
Ziel-Port/Bereich	<p>Nur für Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie eine Ziel-Port-Nummer bzw. einen Bereich von Ziel-Port-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Ziel-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Zielport-Bereich ein.
Quell-IP-Adresse/Netzmaske	<p>Geben Sie die Quell-IP-Adresse der Datenpakete und die zugehörige Netzmaske ein.</p>
Quell-Port/Bereich	<p>Nur für Protokoll = <i>TCP</i> oder <i>UDP</i></p> <p>Geben Sie eine Quell-Port-Nummer bzw. einen Bereich von</p>

Feld	Beschreibung
	<p>Quell-Port-Nummern ein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>-Alle-</i> (Standardwert): Der Ziel-Port ist nicht näher spezifiziert. • <i>Port angeben</i>: Geben Sie einen Ziel-Port ein. • <i>Portbereich angeben</i>: Geben Sie einen Ziel-Port-Bereich ein.
<p>DSCP/TOS-Filter (Layer 3)</p>	<p>Wählen Sie die Art des Dienstes aus (TOS, Type of Service).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Nicht beachten</i> (Standardwert): Die Art des Dienstes wird nicht berücksichtigt. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format, 6 Bit). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
<p>COS-Filter (802.1p/Layer 2)</p>	<p>Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS).</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7. Wertebereich 0 bis 7.</p> <p>Der Standardwert ist <i>Nicht beachten</i>.</p>

12.4.2 QoS-Klassifizierung

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

12.4.2.1 Neu

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


Abb. 110: **Netzwerk->QoS->QoS-Klassifizierung->Neu**

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

Felder im Menü Basisparameter

Feld	Beschreibung
Klassenplan	<p>Wählen Sie den Klassenplan, den Sie anlegen oder bearbeiten wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Neu</i> (Standardwert): Mit dieser Einstellung legen Sie einen neuen Klassenplan an. <i><Name des Klassenplans></i>: Zeigt einen bereits angeleg-

Feld	Beschreibung
	ten Klassenplan, den Sie auswählen und bearbeiten können. Sie können neue Filter hinzufügen.
Beschreibung	Nur für Klassenplan = <i>Neu</i> Geben Sie die Bezeichnung des Klassenplans ein.
Filter	Wählen Sie ein IP-Filter aus. Bei einem neuen Klassenplan wählen Sie das Filter, das an die erste Stelle des Klassenplans gesetzt werden soll. Bei einem bestehenden Klassenplan wählen Sie das Filter, das an den Klassenplan angehängt werden soll. Um ein Filter auswählen zu können, muss mindestens ein Filter im Menü Netzwerk->QoS->QoS-Filter konfiguriert sein.
Richtung	Wählen Sie die Richtung der Datenpakete, die klassifiziert werden sollen. Mögliche Werte: <ul style="list-style-type: none">• <i>Eingehend</i>: Eingehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet.• <i>Ausgehend</i> (Standardwert): Ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet.• <i>Beide</i>: Eingehende und ausgehende Datenpakete werden der im Folgenden zu definierenden Klasse (Klassen-ID) zugeordnet.
High-Priority-Klasse	Aktivieren oder deaktivieren Sie die High-Priority-Klasse. Wenn die High-Priority-Klasse aktiv ist, werden die Datenpakete der Klasse mit der höchsten Priorität zugeordnet, die Priorität 0 wird automatisch gesetzt. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Klassen-ID	Nur für High-Priority-Klasse nicht aktiv. Wählen Sie eine Zahl, welche die Datenpakete einer Klasse zu-

Feld	Beschreibung
	<p>weist.</p> <div data-bbox="544 266 1322 457" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;">  <p>Hinweis</p> <p>Die Klassen-ID ist ein Label, um Datenpakete bestimmten Klassen zuzuordnen. (Die Klassen-ID legt keine Priorität fest.)</p> </div> <p>Mögliche Werte sind ganze Zahlen zwischen 1 und 254.</p>
<p>Setze DSCP/TOS Wert (Layer 3)</p>	<p>Hier können Sie den DSCP/TOS-Wert der IP-Datenpakete in Abhängigkeit zur definierten Klasse (Klassen-ID) setzen bzw. ändern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Erhalten</i> (Standardwert): Der DSCP/TOS-Wert der IP-Datenpakete bleibt unverändert. • <i>DSCP-Binärwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in binärem Format). • <i>DSCP-Dezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in dezimalem Format). • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
<p>Setze COS Wert (802.1p/Layer 2)</p>	<p>Hier können Sie die Serviceklasse (Layer-2-Priorität) im VLAN Ethernet Header der IP-Pakete in Abhängigkeit zur definierten Klasse (Klassen-ID) setzen/ändern.</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Standardwert ist <i>Erhalten</i>.</p>

Feld	Beschreibung
Schnittstellen	<p>Nur für Klassenplan = <i>Neu</i></p> <p>Wählen Sie beim Anlegen eines neuen Klassenplans diejenigen Schnittstellen, an die Sie den Klassenplan binden wollen. Ein Klassenplan kann mehreren Schnittstellen zugeordnet werden.</p>

12.4.3 QoS-Schnittstellen/Richtlinien

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



Hinweis

Daten können nur ausgehend priorisiert werden.

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

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

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

12.4.3.1 Neu

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

QoS-Filter
QoS-Klassifizierung
QoS-Schnittstellen/Richtlinien

Basisparameter											
Schnittstelle	en1-0 ▼										
Priorisierungsalgorithmus	Priority Queueing ▼										
Traffic Shaping	<input type="checkbox"/> Aktiviert										
Queues/Richtlinien	<p>Durch das Erstellen einer QoS-Richtlinie wird automatisch ein Standardeintrag mit der niedrigsten Priorität erstellt.</p> <table border="1" style="width: 100%; border-collapse: collapse; font-size: small;"> <thead> <tr> <th style="width: 40%;">Beschreibung</th> <th style="width: 15%;">Typ</th> <th style="width: 15%;">Klassen-ID</th> <th style="width: 15%;">Priorität</th> <th style="width: 15%;">Bandbreite für Traffic Shaping</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"> <input type="button" value="Hinzufügen"/> </td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping	<input type="button" value="Hinzufügen"/>				
Beschreibung	Typ	Klassen-ID	Priorität	Bandbreite für Traffic Shaping							
<input type="button" value="Hinzufügen"/>											

OK
Abbrechen

Abb. 111: Netzwerk->QoS->QoS-Schnittstellen/Richtlinien->Neu

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
Traffic Shaping	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate in Senderichtung.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upload-Geschwindigkeit	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie für die Queue eine maximale Datenrate in kBits pro Sekunde in Senderichtung ein.</p> <p>Mögliche Werte sind <i>0</i> bis <i>1000000</i>.</p> <p>Der Standardwert ist <i>0</i>, d. h. es erfolgt keine Begrenzung, die Queue kann die maximale Bandbreite belegen.</p>
Größe des Protokoll-Headers unterhalb Layer 3	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Wählen Sie den Schnittstellentyp, um die Größe des jeweiligen Overheads eines Datagramms in die Berechnung der Bandbreite einzubeziehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Benutzerdefiniert</i> Wert in Byte. <p>Mögliche Werte sind <i>0</i> bis <i>100</i>.</p> <ul style="list-style-type: none"> • <i>Undefiniert (Protocol Header Offset=0)</i> (Standardwert) <p>Nur für Ethernet-Schnittstellen auswählbar</p> <ul style="list-style-type: none"> • <i>Ethernet</i> • <i>Ethernet und VLAN</i> • <i>PPP over Ethernet</i> • <i>PPPoE und VLAN</i> <p>Nur für IPSec-Schnittstellen auswählbar:</p> <ul style="list-style-type: none"> • <i>IPSec über Ethernet</i> • <i>IPSec über Ethernet und VLAN</i> • <i>IPSec via PPP over Ethernet</i> • <i>IPSec via PPPoE und VLAN</i>

Feld	Beschreibung
Verschlüsselungsmethode	<p>Nur wenn als Schnittstelle ein IPSec Peer gewählt ist, Traffic Shaping <i>Aktiviert</i> ist und die Größe des Protokoll-Headers unterhalb Layer 3 nicht <i>Undefiniert (Protocol Header Offset=0)</i> ist.</p> <p>Wählen Sie die Verschlüsselungsmethode, die für die IPSec-Verbindung genutzt wird. Der Verschlüsselungsalgorithmus bestimmt die Länge der Blockchiffre, die bei der Bandbreitenkalkulation berücksichtigt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DES, 3DES, Blowfish, Cast</i> - (Cipher-Blockgröße = 64 Bit) • <i>AES128, AES192, AES256, Twofish</i> - (Cipher-Blockgröße = 128 Bit)
Real Time Jitter Control	<p>Nur für Traffic Shaping = aktiviert</p> <p>Real Time Jitter Control führt zu einer Optimierung des Latenzverhaltens bei der Weiterleitung von Real-Time-Datagrammen. Die Funktion sorgt für eine Fragmentierung großer Datenpakete in Abhängigkeit von der verfügbaren Upload-Bandbreite.</p> <p>Real Time Jitter Control ist nützlich bei geringen Upload-Bandbreiten (< 800 kBit/s).</p> <p>Aktivieren oder deaktivieren Sie Real Time Jitter Control.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Kontrollmodus	<p>Nur für Real Time Jitter Control = aktiviert.</p> <p>Wählen Sie den Modus für die Optimierung der Sprachübertragung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert. Die Funktion aktiviert den RTP-Stream-Detection-Mechanismus zum automatischen Erkennen von RTP-Streams. In diesem Modus wird der Real-Time-Jitter-Control-Mechanismus aktiv, sobald ein RTP-Stream

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

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

Felder im Menü Queue/Richtlinie bearbeiten

Feld	Beschreibung
Beschreibung	Geben Sie die Bezeichnung der Queue/Richtlinie an.
Ausgehende Schnittstelle	Zeigt die Schnittstelle an, für die QoS-Queues konfiguriert werden.
Priorisierungsqueue	<p>Wählen Sie den Typ für die Priorisierung der Queue aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Klassenbasiert</i> (Standardwert): Queue für "normal"-klassifizierte Daten. • <i>Hohe Priorität</i>: Queue für "high-priority"-klassifizierte

Feld	Beschreibung
	<p>Daten.</p> <ul style="list-style-type: none"> • <i>Standard</i>: Queue für Daten, die nicht klassifiziert wurden bzw. für deren Klasse keine Queue angelegt worden ist.
Klassen-ID	<p>Nur für Priorisierungsqueue = <i>Klassenbasiert</i></p> <p>Wählen Sie die QoS-Paketklasse, für die diese Queue gelten soll.</p> <p>Dazu muss vorher im Menü Netzwerk->QoS->QoS-Klassifizierung mindestens eine Klassen-ID vergeben worden sein.</p>
Priorität	<p>Nur für Priorisierungsqueue = <i>Klassenbasiert</i></p> <p>Wählen Sie die Priorität der Queue. Mögliche Werte sind <i>1 (hohe Priorität) bis 254 (niedrige Priorität)</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
Gewichtung	<p>Nur für Priorisierungsalgorithmus = <i>Weighted Round Robin oder Weighted Fair Queueing</i></p> <p>Wählen Sie die Gewichtung der Queue. Mögliche Werte sind <i>1 bis 254</i>.</p> <p>Der Standardwert ist <i>1</i>.</p>
RTT-Modus (Realtime-Traffic-Modus)	<p>Aktivieren oder deaktivieren Sie die Echtzeitübertragung der Daten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Der RTT-Modus sollte für QoS-Klassen aktiviert werden, in denen Realtime-Daten priorisiert werden. Dieser Modus führt zu einer Verbesserung des Latenzverhaltens bei der Weiterleitung von Realtime-Datagrammen.</p> <p>Es ist möglich, mehrere Queues mit aktiviertem RTT-Modus zu konfigurieren. Queues mit aktiviertem RTT-Modus müssen immer eine höhere Priorität als Queues mit inaktivem RTT-Modus haben.</p>

Feld	Beschreibung
Traffic Shaping	<p>Aktivieren oder deaktivieren Sie eine Begrenzung der Datenrate (=Traffic Shaping) in Senderichtung.</p> <p>Die Begrenzung der Datenrate gilt für die gewählte Queue. (Es handelt sich dabei nicht um die Begrenzung, die an der Schnittstelle festgelegt werden kann.)</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Maximale Upload-Geschwindigkeit	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie eine maximale Datenrate in kBit pro Sekunde für die Queue ein.</p> <p>Mögliche Werte sind 0 bis 1000000.</p> <p>Der Standardwert ist 0.</p>
Überbuchen zugelassen	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Aktivieren oder deaktivieren Sie die Funktion. Die Funktion steuert das Bandbreitenbegrenzungsverhalten.</p> <p>Bei aktiviertem Überbuchen zugelassen kann die Bandbreitenbegrenzung überschritten werden, die für die Queue eingestellt ist, sofern freie Bandbreite auf der Schnittstelle vorhanden ist.</p> <p>Bei deaktiviertem Überbuchen zugelassen kann die Queue niemals Bandbreite über die eingestellte Bandbreitenbegrenzung hinaus belegen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Burst-Größe	<p>Nur für Traffic Shaping = aktiviert.</p> <p>Geben Sie die maximale Anzahl an Bytes ein, die kurzfristig noch übertragen werden darf, wenn die für diese Queue erlaubte Datenrate bereits erreicht ist.</p> <p>Mögliche Werte sind 0 bis 64000.</p> <p>Der Standardwert ist 0.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Dropping-Algorithmus	<p>Wählen Sie das Verfahren, nach dem Pakete in der QoS-Queue verworfen werden, wenn die maximale Größe der Queue überschritten wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Tail Drop</i> (Standardwert): Das neu hinzugekommene Paket wird verworfen. • <i>Head Drop</i>: Das älteste Paket in der Queue wird verworfen. • <i>Random Drop</i>: Ein zufällig ausgewähltes Paket aus der Queue wird verworfen.
Vermeidung von Datenstau (RED)	<p>Aktivieren oder deaktivieren Sie das präventive Löschen von Datenpaketen.</p> <p>Pakete, deren Datengröße zwischen Min. Queue-Größe und Max. Queue-Größe liegt, werden vorbeugend verworfen, um einen Queue-Überlauf zu verhindern (RED=Random Early Detection). Dieses Verfahren sorgt bei TCP-basiertem Datenverkehr für eine insgesamt kleinere Queue, sodass selbst Traffic-Bursts meist ohne größere Paketverluste übertragen werden können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Min. Queue-Größe	<p>Geben Sie den unteren Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 0.</p>
Max. Queue-Größe	<p>Geben Sie den oberen Schwellwert für das Verfahren Vermeidung von Datenstau (RED) in Byte ein.</p> <p>Mögliche Werte sind 0 bis 262143.</p> <p>Der Standardwert ist 16384.</p>

12.5 Zugriffsregeln

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

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

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

Möchten z. B. Standorte, deren LANs über ein Teldat-Gateway miteinander verbunden sind, alle eingehenden FTP-Anfragen ablehnen, oder Telnet-Sitzungen nur zwischen bestimmten Hosts zulassen, sind Access-Listen ein effektives Mittel.

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

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

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

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

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

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

oder

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

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

oder

Kombination aus den beiden oben beschriebenen Möglichkeiten.

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

Sie können jeder Schnittstelle individuell eine Regelkette zuweisen.



Achtung

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

Greifen Sie zur Filter-Konfiguration möglichst über die serielle Konsolen-Schnittstelle oder mit ISDN-Login auf Ihr Gateway zu.

12.5.1 Zugrifffilter


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

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



Abb. 112: **Netzwerk->Zugriffsregeln->Zugriffsfiler**

12.5.1.1 Bearbeiten oder Neu

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

Zugriffsfiler Regelketten Schnittstellenzuweisung

Basisparameter	
Beschreibung	<input type="text"/>
Dienst	Benutzerdefiniert ▾
Protokoll	Bellebig ▾
Ziel-IP-Adresse/Netzmaske	Bellebig ▾
Quell-IP-Adresse/Netzmaske	Bellebig ▾
DSCP/TOS-Filter (Layer 3)	Nicht beachten ▾
COS-Filter (802.1p/Layer 2)	Nicht beachten ▾

OK Abbrechen

Abb. 113: Netzwerk->Zugriffsregeln->Zugriffsfiler->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für das Filter ein.
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus. Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i> • <i>chargen</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>Standardwert ist <i>Benutzerdefiniert</i>.</p>

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

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>DSCP-Hexadezimalwert</i>: Differentiated Services Code Point nach RFC 3260 wird zur Signalisierung der Priorität der IP-Pakete verwendet (Angabe in hexadezimalen Format). • <i>TOS-Binärwert</i>: Der TOS-Wert wird im binären Format angegeben, z. B. 00111111. • <i>TOS-Dezimalwert</i>: Der TOS-Wert wird im dezimalen Format angegeben, z. B. 63. • <i>TOS-Hexadezimalwert</i>: Der TOS-Wert wird im hexadezimalen Format angegeben, z. B. 3F.
COS-Filter (802.1p/Layer 2)	<p>Tragen Sie die Serviceklasse der IP-Pakete ein (Class of Service, CoS).</p> <p>Mögliche Werte sind ganze Zahlen zwischen 0 und 7.</p> <p>Standardwert ist <i>Nicht beachten</i>.</p>

12.5.2 Regelketten


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

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



Abb. 114: **Netzwerk->Zugriffsregeln->Regelketten**

12.5.2.1 Bearbeiten oder Neu

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

[Zugriffsfilter](#) | [Regelketten](#) | [Schnittstellenzuweisung](#)

Basisparameter	
Regelkette	Neu ▾
Beschreibung	<input type="text"/>
Zugriffsfilter	Eines auswählen ▾
Aktion	Zulassen, wenn Filter passt ▾


Abb. 115: **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 des Klassenplans></i>: Wählen Sie eine bereits angelegte Regelkette aus und fügen ihr somit eine weitere Regel hinzu.
Beschreibung	Geben Sie die Bezeichnung der Regelkette ein.
Zugriffsfilter	<p>Wählen Sie ein IP-Filter aus.</p> <p>Bei einer neuen Regelkette wählen Sie das Filter, das an die erste Stelle der Regelkette gesetzt werden soll.</p> <p>Bei einer bestehenden Regelkette wählen Sie das Filter, das an die Regelkette angehängt werden soll.</p>
Aktion	<p>Legen Sie fest, wie mit einem gefilterten Datenpaket verfahren wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zulassen, wenn Filter passt</i> (Standardwert): Paket annehmen, wenn das Filter passt. • <i>Zulassen, wenn Filter nicht passt</i>: Paket anneh-

Feld	Beschreibung
	<p>men, wenn das Filter nicht passt.</p> <ul style="list-style-type: none"> • <i>Verweigern, wenn Filter passt</i>: Paket abweisen, wenn das Filter passt. • <i>Verweigern, wenn Filter nicht 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.

12.5.3 Schnittstellenzuweisung


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

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



Abb. 116: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung**

12.5.3.1 Bearbeiten oder Neu

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

Zugriffsfilter
Regelketten
Schnittstellenzuweisung

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

OK
Abbrechen

Abb. 117: **Netzwerk->Zugriffsregeln->Schnittstellenzuweisung->Neu**

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

Felder im Menü Basisparameter

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

12.6 Drop-In

Mit dem Drop-In-Modus können Sie ein Netzwerk in mehrere Segmente aufteilen, ohne das IP-Netzwerk in Subnetze teilen zu müssen. Dazu können mehrere Schnittstellen in einer Drop-In-Gruppe zusammengefasst und einem Netzwerk zugeordnet werden. Alle Schnittstellen sind dann mit der gleichen IP-Adresse konfiguriert.

Die Netzwerkkomponenten eines Segments, die an einem Anschluss angeschlossen sind, können dann gemeinsam z. B. mit einer Firewall geschützt werden. Der Datenverkehr von Netzwerkkomponenten zwischen einzelnen Segmenten, die unterschiedlichen Ports zugeordnet sind, wird dann entsprechend der konfigurierten Firewall-Regeln kontrolliert.

12.6.1 Drop-In-Gruppen

Im Menü **Netzwerk->Drop-In->Drop-In-Gruppen** wird eine Liste aller **Drop-In-Gruppen** angezeigt. Eine **Drop-In-Gruppe** repräsentiert jeweils ein Netzwerk.

12.6.1.1 Neu

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

Drop-In-Gruppen

Basisparameter	
Gruppenbeschreibung	<input type="text"/>
Modus	Transparent <input type="button" value="v"/>
Netzwerkconfiguration	Statisch <input type="button" value="v"/>
Netzwerkadresse	<input type="text"/>
Netzmaske	<input type="text"/>
Lokale IP-Adresse	<input type="text"/>
ARP Lifetime	3600 Sekunden
DNS-Zuweisung über DHCP	Unverändert <input type="button" value="v"/>
Vom NAT ausnehmen (DMZ)	<input type="checkbox"/> Aktiviert
Schnittstellenauswahl	<div style="border: 1px solid gray; padding: 2px;"> Schnittstelle <input type="text"/> </div> <input type="button" value="Hinzufügen"/>

Abb. 118: **Netzwerk->Drop-In->Drop-In-Gruppen->Neu**

Das Menü **Netzwerk->Drop-In->Drop-In-Gruppen->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Gruppenbeschreibung	Geben Sie eine eindeutige Bezeichnung für die Drop-In -Gruppe ein.
Modus	<p>Wählen Sie, welcher Modus für die Übermittlung der MAC-Adressen von Netzwerkkomponenten verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Transparent</i> (Standardwert): ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden transparent (unverändert) weitergeleitet. • <i>Proxy</i>: ARP-Pakete und dem Drop-In-Netzwerk zugehörige IP-Pakete werden mit der MAC-Adresse der entsprechenden Schnittstelle weitergeleitet.
Netzwerkconfiguration	<p>Wählen Sie aus, auf welche Weise den Netzwerkkomponenten eine IP-Adresse zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert) • <i>DHCP</i>
Netzwerkadresse	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die Netzwerkadresse des Drop-In-Netzwerks ein.</p>
Netzmaske	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die zugehörige Netzmaske ein.</p>
Lokale IP-Adresse	<p>Nur für Netzwerkconfiguration = <i>Statisch</i></p> <p>Geben Sie die lokale IP-Adresse ein. Diese IP-Adresse muss für alle Ethernet-Ports eines Netzwerks identisch sein.</p>
DHCP Client an Schnittstelle	<p>Nur für Netzwerkconfiguration = <i>DHCP</i></p> <p>Hier können Sie eine Ethernet-Schnittstelle Ihres Routers wählen, die als DHCP-Client agieren soll.</p> <p>Diese Einstellung benötigen Sie zum Beispiel, wenn der Router</p>

Feld	Beschreibung
	<p>Ihres Providers als DHCP-Server dient.</p> <p>Sie können unter den Schnittstellen wählen, welche Ihr Gerät zur Verfügung stellt, die Schnittstelle muss jedoch Mitglied der Drop-In-Gruppe sein.</p>
ARP Lifetime	<p>Legt die Zeitspanne fest, während derer ARP-Einträge im Cache gehalten werden.</p> <p>Der Standardwert ist <i>3600</i> Sekunden.</p>
DNS-Zuweisung über DHCP	<p>Das Gateway kann DHCP-Pakete, die die Drop-In-Gruppe durchlaufen, modifizieren und sich selbst als angebotenen DNS-Server eintragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Unverändert</i> (Standardwert) • <i>Eigene IP-Adresse</i>
Vom NAT ausnehmen (DMZ)	<p>Hier können Sie Datenverkehr von NAT ausnehmen.</p> <p>Verwenden Sie diese Funktion, um zum Beispiel die Erreichbarkeit bestimmter Web-Server in einer DMZ sicherzustellen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Schnittstellenauswahl	<p>Wählen Sie alle Ports aus, die in der Drop-In-Gruppe (im Netzwerk) enthalten sein sollen.</p> <p>Fügen Sie mit Hinzufügen weitere Einträge hinzu.</p>

Kapitel 13 Routing-Protokolle

13.1 RIP

Die Einträge in der Routing-Tabelle können entweder statisch festgelegt werden oder es erfolgt eine laufende Aktualisierung der Routing-Tabelle durch dynamischen Austausch der Routing-Informationen zwischen mehreren Geräten. Diesen Austausch regelt ein sogenanntes Routing-Protokoll, z. B. RIP (Routing Information Protocol). Standardmäßig ungefähr alle 30 Sekunden (dieser Wert kann in **Aktualisierungstimer** verändert werden) sendet ein Gerät Meldungen zu entfernten Netzwerken, wobei es Informationen aus seiner eigenen aktuellen Routing-Tabelle verwendet. Dabei wird immer die gesamte Routing-Tabelle ausgetauscht. Mit Triggered RIP findet nur ein Austausch statt, wenn sich Routing-Informationen geändert haben. In diesem Fall werden nur die geänderten Informationen versendet.

Durch Beobachtung der Informationen, die von anderen Geräten verschickt werden, werden neue Routen und kürzere Wege für bestehende Routen in der Routing-Tabelle gespeichert. Da Routen zwischen Netzwerken unerreichbar werden können, entfernt RIP Routen, die älter als 5 Minuten sind (d. h. Routen, die in den letzten 300 Sekunden - **Garbage Collection Timer** + **Routentimeout** - nicht verifiziert wurden). Mit Triggered RIP gelernte Routen werden jedoch nicht gelöscht.

Ihr Gerät unterstützt sowohl Version 1 als auch Version 2 von RIP, wahlweise einzeln oder gemeinsam.

13.1.1 RIP-Schnittstellen

Im Menü **Routing-Protokolle -> RIP -> RIP-Schnittstellen** wird eine Liste aller RIP-Schnittstellen angezeigt.

RIP-Schnittstellen RIP-Filter RIP-Optionen

Nr.	Schnittstelle	Version in Senderichtung	Version in Empfangsrichtung	Routenankündigung	
1	en1-4	Keine	Keine	Nur aktiv	
2	en1-0	Keine	Keine	Nur aktiv	

Seite: 1, Objekte: 1 - 2

Abb. 119: **Routing-Protokolle -> RIP -> RIP-Schnittstellen**

13.1.1.1 Bearbeiten


Für jede RIP-Schnittstelle sind über das -Menü die Optionen *Version in Senderichtung*, *Version in Empfangsrichtung* und *Routenankündigung* auswählbar.

RIP-Schnittstellen RIP-Filter RIP-Optionen

RIP-Parameter für: en1-4

Version in Senderichtung	Keine 
Version in Empfangsrichtung	Keine 
Routenankündigung	Nur aktiv 

OK Abbrechen

Abb. 120: Routing-Protokolle->RIP->RIP-Schnittstellen-> 

Das Menü **Netzwerk->RIP->RIP-Schnittstellen->**  besteht aus folgenden Feldern:

Felder im Menü RIP-Parameter für

Feld	Beschreibung
Version in Senderichtung	<p>Entscheiden Sie, ob über RIP Routen propagiert werden sollen, und wenn ja, wählen Sie die RIP-Version für das Senden von RIP-Paketen über die Schnittstelle in Senderichtung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): RIP ist nicht aktiv. • <i>RIP V1</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • <i>RIP V2</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • <i>RIP V1/V2</i>: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • <i>RIP V2 Multicast</i>: Ermöglicht das Senden von RIP-V2-Nachrichten über die Multicast-Adresse 224.0.0.9. • <i>RIP V1 Triggered</i>: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • <i>RIP V2 Triggered</i>: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet

Feld	Beschreibung
	(Triggered RIP).
Version in Empfangsrichtung	<p>Entscheiden Sie, ob über RIP Routen importiert werden sollen und wenn ja, wählen Sie die RIP-Version für das Empfangen von RIP-Paketen über die Schnittstelle in Empfangsrichtung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): RIP ist nicht aktiv. • <i>RIP V1</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 1. • <i>RIP V2</i>: Ermöglicht Senden bzw. Empfangen von RIP-Paketen der Version 2. • <i>RIP V1/V2</i>: Ermöglicht Senden bzw. Empfangen sowohl von RIP-Paketen der Version 1 als auch der Version 2. • <i>RIP V1 Triggered</i>: RIP-V1-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP). • <i>RIP V2 Triggered</i>: RIP-V2-Nachrichten werden gemäß RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP).
Routenankündigung	<p>Wählen Sie aus, wann ggf. aktivierte Routing-Protokolle (z. B. RIP) die für diese Schnittstelle definierten IP-Routen propagieren sollen.</p> <p>Beachten Sie: Diese Einstellung hat keinen Einfluss auf die oben erwähnte Schnittstellen-spezifische RIP-Konfiguration.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv oder Ruhend</i> (nicht für LAN-Schnittstellen, Schnittstellen im Bridge-Modus und Schnittstellen für Standleitungen): Routen werden propagiert, wenn der Status der Schnittstelle auf aktiv oder bereit steht. • <i>Nur aktiv</i> (Standardwert): Routen werden nur propagiert, wenn der Status der Schnittstelle auf aktiv steht. • <i>Immer</i>: Routen werden immer propagiert unabhängig vom Betriebsstatus.

13.1.2 RIP-Filter

Im diesem Menü können Sie exakt festlegen, welche Routen exportiert oder importiert werden sollen oder nicht.

Hierbei können Sie nach folgenden Strategien vorgehen:

- Sie deaktivieren das Importieren bzw. Exportieren bestimmter Routen explizit. Der Import bzw. Export aller anderen Routen, die nicht aufgeführt werden, bleibt erlaubt.
- Sie aktivieren das Importieren bzw. Exportieren bestimmter Routen explizit. Dann müssen Sie den Import bzw. Export aller anderen Routen auch explizit deaktivieren. Dieses erreichen Sie mittels eines Filters für **IP-Adresse/Netzmaske** = kein Eintrag (dies entspricht der IP-Adresse 0.0.0.0 mit der Netzmaske 0.0.0.0). Damit dieses Filter als letztes angewendet wird, muss es an der niedrigsten Position eingeordnet werden.


Ein Filter für eine Standard-Route konfigurieren Sie mit folgenden Werten:


- **IP-Adresse/Netzmaske** = für IP-Adresse keine Eintrag (dies entspricht der IP-Adresse 0.0.0.0), für Netzmaske = 255.255.255.255

Im Menü **Routing-Protokolle->RIP->RIP-Filter** wird eine Liste aller RIP-Filter angezeigt.



Abb. 121: **Routing-Protokolle->RIP->RIP-Filter**

Mit der Schaltfläche  können Sie vor dem Listeneintrag ein weiteres Filter einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen eines neuen Filters.

Mit der Schaltfläche  können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position das Filter verschoben werden soll.

13.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere RIP-Filter einzurichten.

RIP-Schnittstellen | RIP-Filter | RIP-Optionen

Basisparameter	
Schnittstelle	Keine ▾
IP-Adresse/Netzmaske	<input type="text"/> / <input type="text"/>
Richtung	<input checked="" type="radio"/> Importieren <input type="radio"/> Exportieren
Metrik-Offset für Aktive Schnittstellen	0 ▾
Metrik-Offset für Inaktive Schnittstellen	0 ▾

OK Abbrechen

Abb. 122: Routing-Protokolle->RIP->RIP-Filter->Neu

Das Menü **Routing-Protokolle->RIP->RIP-Filter->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie aus, für welche Schnittstelle die zu konfigurierende Regel gilt.
IP-Adresse/Netzmaske	<p>Geben Sie die IP-Adresse und Netzmaske ein, auf welche die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen.</p> <p>Die Regeln für eingehende und ausgehende RIP-Pakete (Importieren oder Exportieren) müssen für dieselbe IP-Adresse getrennt konfiguriert werden.</p> <p>Sie können einzelne Host-Adressen ebenso angeben wie Netz-adressen.</p>
Richtung	<p>Wählen Sie aus, ob das Filter für das Exportieren oder das Im-portieren von Routen gilt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Importieren</i> (Standardwert) • <i>Exportieren</i>
Metrik-Offset für Aktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Ak-tiv" ist. Beim Export wird der Wert der exportierten Metrik hinzu-gefügt, wenn der Status der Schnittstelle "Aktiv" ist.

Feld	Beschreibung
	Mögliche Werte sind -16 bis 16 . Der Standardwert ist 0 .
Metrik-Offset für Inaktive Schnittstellen	Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Ruhend" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Ruhend" ist. Mögliche Werte sind -16 bis 16 . Der Standardwert ist 0 .

13.1.3 RIP-Optionen

RIP-Schnittstellen RIP-Filter **RIP-Optionen**

Globale RIP-Parameter	
RIP-UDP-Port	520
Standardmäßige Routenverteilung	<input checked="" type="checkbox"/> Aktiviert
Poisoned Reverse	<input type="checkbox"/> Aktiviert
RFC 2453-Variabler Timer	<input checked="" type="checkbox"/> Aktiviert
RFC 2091-Variabler Timer	<input type="checkbox"/> Aktiviert
Timer für RIP V2 (RFC 2453)	
Aktualisierungstimer	30 Sekunden
Routentimeout	180 Sekunden
Garbage Collection Timer	120 Sekunden
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 123: Routing-Protokolle->RIP->RIP-Optionen

Das Menü **Routing-Protokolle->RIP->RIP-Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale RIP-Parameter

Feld	Beschreibung
RIP-UDP-Port	Die Einstellungsmöglichkeit des UDP-Ports, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, dass Ihr Gerät auf einem Port sendet und lauscht, den keine weiteren Geräte benutzen. Der Stan-

Feld	Beschreibung
	<p>Standardwert <i>520</i> sollte eingestellt bleiben.</p>
<p>Standardmäßige Routenverteilung</p>	<p>Wählen Sie aus, ob die Standard-Route Ihres Geräts über RIP-Updates propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>Poisoned Reverse</p>	<p>Wählen Sie das Verfahren zur Verhinderung von Routing-Schleifen.</p> <p>Bei Standard RIP werden die gelernten Routen über alle Schnittstellen mit aktiviertem RIP SENDEN propagiert. Bei Poisoned Reverse propagiert Ihr Gerät jedoch über die Schnittstelle, über die es die Routen gelernt hat, diese mit der Metrik (Next Hop Count) 16 (= "Netz ist nicht erreichbar").</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>RFC 2453-Variabler Timer</p>	<p>Wählen Sie aus, ob für die in RFC 2453 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für RIP V2 (RFC 2453) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Wenn Sie die Funktion deaktivieren, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.</p>
<p>RFC 2091-Variabler Timer</p>	<p>Wählen Sie aus, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für Triggered RIP (RFC 2091) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion nicht aktiv ist, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.</p>

Felder im Menü Timer für RIP V2 (RFC 2453)

Feld	Beschreibung
Aktualisierungstimer	<p>Nur für RFC 2453-Variabler Timer = <i>Aktiviert</i></p> <p>Nach Ablauf dieses Zeitraums wird eine RIP-Aktualisierung gesendet.</p> <p>Der Standardwert ist <i>30</i> (Sekunden).</p>
Routentimeout	<p>Nur für RFC 2453-Variabler Timer = <i>Aktiviert</i></p> <p>Nach der letzten Aktualisierung einer Route wird der Routentimeout aktiv.</p> <p>Nach dessen Ablauf wird die Route deaktiviert und der Garbage Collection Timer gestartet.</p> <p>Der Standardwert ist <i>180</i> (Sekunden).</p>
Garbage Collection Timer	<p>Nur für RFC 2453-Variabler Timer = <i>Aktiviert</i></p> <p>Der Garbage Collection Timer wird gestartet, sobald der Routentimeout abgelaufen ist.</p> <p>Nach Ablauf dieses Zeitraums wird die ungültige Route aus der IPROUTETABLE gelöscht, sofern keine Aktualisierung für die Route erfolgt.</p> <p>Der Standardwert ist <i>120</i> (Sekunden).</p>

Felder im Menü Timer für Triggered RIP (RFC 2091)

Feld	Beschreibung
Hold Down Timer	<p>Nur für RFC 2091-Variabler Timer = <i>Aktiviert</i></p> <p>Der Hold Down Timer wird aktiv, sobald Ihr Gerät eine unerreichbare Route (Metric 16) erhält. Nach Ablauf dieses Zeitraums wird die Route ggf. gelöscht.</p> <p>Der Standardwert ist <i>120</i> (in Sekunden).</p>
Retransmission Timer	<p>Nur für RFC 2091-Variabler Timer = <i>Aktiviert</i></p> <p>Nach Ablauf dieses Zeitraums werden Update-Request- bzw. Update-Response-Pakete erneut versendet, bis ein Update-Flush- bzw. Update-Acknowledge-Paket eintrifft.</p>

Feld	Beschreibung
	Der Standardwert ist 5 (in Sekunden).

Kapitel 14 Multicast

Was ist Multicasting?

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

Weitere Anwendungsbereiche

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

Adressbereich für Multicast

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

Multicast Grundlagen

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

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

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

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

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

Membership-Management-Protokoll

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

Ihr Gerät unterstützt folgende Multicast-Mechanismen:

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



Tipp

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

14.1 Allgemein

14.1.1 Allgemein

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



Abb. 124: **Multicast->Allgemein->Allgemein**

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

Felder im Menü Grundeinstellungen

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

14.2 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.

14.2.1 IGMP

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

14.2.1.1 Bearbeiten oder Neu

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

IGMP Optionen

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

Erweiterte Einstellungen

IGMP Proxy	<input type="checkbox"/> Aktiviert
------------	------------------------------------

OK Abbrechen

Abb. 125: Multicast->IGMP->IGMP->Neu

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

Felder im Menü IGMP-Einstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der IGMP aktiviert werden soll, d.h. Queries werden versendet und Antworten akzeptiert.
Abfrage Intervall	<p>Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen.</p> <p>Möglich Werte sind 0 bis 600.</p> <p>Der Standardwert ist 125.</p>
Maximale Antwortzeit	<p>Geben Sie für das Senden von Queries an, in welchem Zeitintervall in Sekunden Hosts auf jeden Fall antworten müssen. Die Hosts wählen aus diesem Intervall zufällig eine Verzögerung, bis die Antwort gesendet wird. Damit können Sie bei Netzen mit vielen Hosts eine Streuung und somit eine Entlastung erreichen.</p> <p>Möglich Werte sind 0,0 bis 25,0.</p> <p>Der Standardwert ist 10,0.</p>
Robustheit	<p>Wählen Sie den Multiplikator zur Steuerung interner Timer-Werte aus. Mit einem höheren Wert kann z. B. in einem verlustreichen Netzwerk ein Paketverlust kompensiert werden. Durch einen zu hohen Wert kann sich aber auch die Zeit zwischen dem Abmelden und dem Stopp des eingehenden Datenverkehrs erhöhen (Leave Latency).</p> <p>Möglich Werte sind 2 bis 8.</p> <p>Der Standardwert ist 2.</p>
Antwortintervall (Letztes Mitglied)	<p>Bestimmen Sie, wie lang der Router nach einer Query an eine Gruppe auf Antwort wartet.</p> <p>Wenn Sie den Wert verkleinern, wird schneller erkannt, ob das letzte Mitglied eine Gruppe verlassen hat und somit keine Pakete mehr für diese Gruppe an diese Schnittstelle weitergeleitet werden müssen.</p> <p>Möglich Werte sind 0,0 bis 25,0.</p> <p>Der Standardwert ist 1,0.</p>

Feld	Beschreibung
Maximale Anzahl der IGMP-Staumeldungen	Limitieren Sie die Anzahl der Reports/Queries pro Sekunde für die gewählte Schnittstelle.
Modus	<p>Wählen Sie aus, ob die hier definierte Schnittstelle nur im Host-Modus oder auch im Routing Modus arbeitet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Routing</i> (Standardwert): Die Schnittstelle wird im Routing-Modus betrieben. • <i>Host</i>: Die Schnittstelle wird nur im Host-Modus betrieben.

IGMP Proxy

Mit IGMP Proxy können mehrere lokal angeschlossene Schnittstellen als ein Subnetz zu einem benachbarten Router simuliert werden. Auf der IGMP-Proxy-Schnittstelle eingehende Queries werden in die lokalen Subnetze weitergeleitet. Lokale Reports werden auf der IGMP-Proxy-Schnittstelle weitergeleitet.

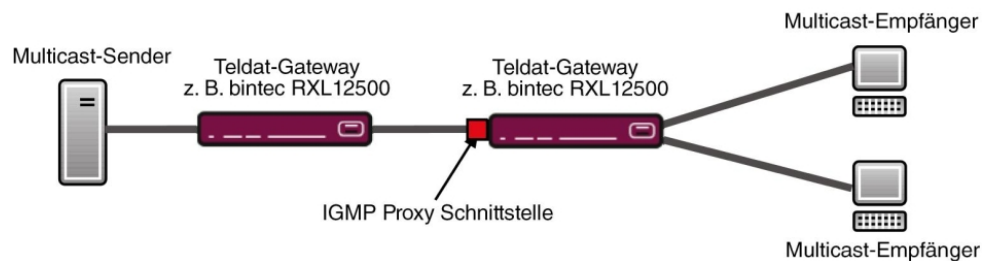


Abb. 126: IGMP Proxy

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

Felder im Menü Erweiterte Einstellungen

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

14.2.2 Optionen

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

Grundeinstellungen	
IGMP-Status	<input type="radio"/> Aktiv <input type="radio"/> Inaktiv <input checked="" type="radio"/> Auto
Modus	<input checked="" type="radio"/> Kompatibilitätsmodus <input type="radio"/> Nur Version 3
Maximale Gruppen	<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

Abb. 127: Multicast->IGMP->Optionen

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

Felder im Menü Grundeinstellungen

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

Feld	Beschreibung
	<p>konnte.</p> <ul style="list-style-type: none"> • <i>Nur Version 3</i>: Nur IGMP Version 3 wird verwendet.
Maximale Gruppen	Geben Sie ein, wie viele Gruppen sowohl intern als auch in Reports maximal möglich sein sollen.
Maximale Quellen	Geben Sie die maximale Anzahl der Quellen ein, die in den Reports der Version 3 spezifiziert sind, als auch die maximale Anzahl der intern verwalteten Quellen pro Gruppe.
Maximale Anzahl der IGMP-Statusmeldungen	<p>Geben Sie die maximale Anzahl der insgesamt möglichen eingehenden Queries bzw. Meldungen pro Sekunde ein.</p> <p>Der Standardwert ist 0, d. h. die Anzahl der IGMP-Statusmeldungen ist nicht begrenzt.</p>

14.3 Weiterleiten

14.3.1 Weiterleiten

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

14.3.1.1 Neu

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

Weiterleiten

Basisparameter	
Alle Multicast-Gruppen	<input type="checkbox"/> Aktiviert
Multicast-Gruppen-Adresse	<input type="text"/>
Quellschnittstelle	Keine ▾
Zielschnittstelle	Keine ▾

Abb. 128: 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	Wählen Sie die Schnittstelle Ihres Geräts aus, an dem die gewünschte Multicast-Gruppe eingeht.
Zielschnittstelle	Wählen Sie die Schnittstelle Ihres Geräts aus, zu der die gewünschte Multicast-Gruppe weitergeleitet werden soll.

14.4 PIM

Protocol Independent Multicast (PIM) ist ein Multicast-Routingverfahren, das dynamisches Routing von Multicast-Paketen ermöglicht. Bei PIM wird die Informationsverteilung über einen zentralen Punkt geregelt, der als Rendezvous Point bezeichnet wird. Dorthin werden die Datenpakete initial geleitet und auf Anfrage anderer Router den Empfängern zur Verfügung gestellt.

Bei Multicast-Routing-Protokollen unterscheidet man grundsätzlich zwischen Sparse Mode und Dense Mode. Beim Dense Mode werden alle Pakete weitergeleitet und nur die Pakete an Gruppen verworfen, die explizit abbestellt wurden. Beim Sparse Mode werden nur Pakete an Gruppen weitergeleitet, die von diesen bestellt wurden. Ihr Gerät verwendet PIM im Sparse Mode.


14.4.1 PIM-Schnittstellen

Im Menü **Multicast->PIM->PIM-Schnittstellen** wird eine Liste aller PIM-Schnittstellen angezeigt.

The screenshot shows a web interface for configuring PIM interfaces. At the top, there are three tabs: **PIM-Schnittstellen** (selected), **PIM-Rendezvous-Punkte**, and **PIM-Optionen**. Below the tabs is a control bar with 'Ansicht' set to 20, 'pro Seite' with navigation arrows, 'Filtern in' set to 'Keiner', and a 'Los' button. A table header is visible with columns: Schnittstelle, IP-Version, Designated Router (DR), Stub Interface Mode, Status, and Aktion. The table content shows 'Seite: 1'. At the bottom center, there is a button labeled **Neu**.

Abb. 129: **Multicast->PIM->PIM-Schnittstellen**

14.4.1.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um PIM-Schnittstellen zu konfigurieren.

The screenshot shows the configuration dialog for a PIM interface. At the top, there are three tabs: **PIM-Schnittstellen** (selected), **PIM-Rendezvous-Punkte**, and **PIM-Optionen**. The dialog is titled 'PIM-Schnittstelleneinstellungen' and contains the following fields:

- Schnittstelle: Eine auswählen (dropdown)
- PIM-Modus: Sparse Mode (SM)
- Stub Interface Mode: Aktiviert
- Designated-Router-Priorität: 1

Below these fields is a section titled 'Erweiterte Einstellungen' with the following fields:

- Hello-Intervall: 30 Sekunden
- Triggered-Hello-Intervall: 5 Sekunden
- Hello Hold Time: 105 Sekunden
- Join/Prune-Intervall: 60 Sekunden
- Join/Prune Hold Time: 210 Sekunden
- Propagation Delay: 1 Sekunden
- Override Interval: 3 Sekunden

At the bottom of the dialog, there are two buttons: **OK** and **Abbrechen**.

Abb. 130: **Multicast->PIM->PIM-Schnittstellen->Neu**

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

Felder im Menü PIM-Schnittstelleneinstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle, die für PIM benutzt werden soll, d.h. über die Multicast Routing betrieben werden soll.
PIM-Modus	Zeigt den Modus an, der für PIM benutzt wird. Ihr Gerät verwendet den PIM Sparse Mode. Der Eintrag kann nicht verändert werden.
Stub Interface Mode	<p>Bestimmen Sie, ob die Schnittstelle für PIM-Datenpakete genutzt werden soll. Mit diesem Parameter können Sie z. B. eine Schnittstelle für IGMP benutzen, aber vor (gefälschten) PIM-Nachrichten schützen.</p> <p>Ist diese Funktion deaktiviert (Standardwert), werden die PIM-Datenpakete für diese Schnittstelle blockiert.</p> <p>Wenn die Funktion aktiv ist, ist die Schnittstelle für die PIM-Datenpakete freigegeben.</p>
Designated-Router-Priorität	<p>Bestimmen Sie den Wert der Designated Router Priority, der in die Option Designated-Router-Priorität eingefügt wird.</p> <p>Je höher dieser Wert ist, desto größer ist die Wahrscheinlichkeit, dass der entsprechende Router als Designated Router verwendet wird.</p> <p>Standardwert ist <i>1</i>.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Hello-Intervall	<p>Bestimmen Sie, in welchen Zeitabständen (in Sekunden) PIM Hello Messages über diese Schnittstelle gesendet werden.</p> <p>Der Wert <i>0</i> bedeutet, dass auf dieser Schnittstelle keine PIM Hello Messages gesendet werden.</p> <p>Wertebereich: <i>0</i> bis <i>18000</i> Sekunden.</p> <p>Standardwert ist <i>30</i>.</p>
Triggered-Hello-Intervall	Bestimmen Sie, wie lange maximal gewartet werden darf, bis eine PIM Hello Message nach einem Systemstart oder nach einem

Feld	Beschreibung
	<p>Neustart eines Nachbarn gesendet wird.</p> <p>Der Wert <i>0</i> bedeutet, dass PIM Hello Messages immer sofort gesendet werden.</p> <p>Wertebereich: <i>0</i> bis <i>60</i> Sekunden.</p> <p>Standardwert ist <i>5</i>.</p>
Hello Hold Time	<p>Bestimmen Sie den Wert des Holdtime Feldes in einer PIM Hello Message.</p> <p>Daraus ergibt sich, wie lange ein PIM-Router als verfügbar gilt. Sobald die Hello Hold Time abgelaufen ist und keine weitere Hello Message empfangen wurde, wird dieser PIM-Router als nicht erreichbar betrachtet.</p> <p>Wertebereich: <i>0</i> bis <i>65535</i> Sekunden.</p> <p>Standardwert ist <i>105</i>.</p>
Join/Prune-Intervall	<p>Bestimmen Sie die Häufigkeit, mit der PIM Join/Prune Messages auf der Schnittstelle gesendet werden sollen.</p> <p>Der Wert <i>0</i> bedeutet, dass auf dieser Schnittstelle keine periodischen PIM Join/Prune Messages gesendet werden.</p> <p>Wertebereich: <i>0</i> bis <i>18000</i> Sekunden.</p> <p>Standardwert ist <i>60</i>.</p>
Join/Prune Hold Time	<p>Bestimmen Sie den Wert, der in das Holdtime Feld einer PIM Join/Prune Message eingefügt wird.</p> <p>Dies ist die Zeitspanne, die ein Empfänger den Join/Prune State halten muss.</p> <p>Wertebereich: <i>0</i> bis <i>65535</i> Sekunden.</p> <p>Standardwert ist <i>210</i>.</p>
Propagation Delay	<p>Bestimmen Sie den Wert, der in das Propagation Delay Feld eingefügt wird. Dieses Feld ist ein Bestandteil der LAN Prune Delay Option in den PIM Hello Messages, die auf dieser Schnittstelle gesendet werden.</p>

Feld	Beschreibung
	<p>Propagation Delay und Override Interval stellen die sogenannten LAN-Prune-Delay-Einstellungen dar. Sie bewirken eine verzögerte Verarbeitung von Prune-Messages bei Upstream Routern.</p> <p>Wenn Propagation Delay zu klein ist, kann es zum Abbruch der Übertragung von Multicast-Paketen kommen, bevor ein Downstream Router eine Prune Override Message geschickt hat.</p> <p>Wertebereich: 0 bis 32 Sekunden.</p> <p>Standardwert ist 1.</p>
Override Interval	<p>Bestimmen Sie den Wert, den das Gateway in das Feld Override Interval der LAN Prune Delay Option einfügt.</p> <p>Override Interval bestimmt, wie lange ein Downstream Router höchstens warten darf, bis er eine Prune Override Message schickt.</p> <p>Wertebereich: 0 bis 65 Sekunden.</p> <p>Standardwert ist 3.</p>

14.4.2 PIM-Rendezvous-Punkte


Im Menü **Multicast->PIM->PIM-Rendezvous-Punkte** können Sie festlegen, welcher Rendezvous Point für welche Gruppen zuständig sein soll.

Es wird eine Liste aller PIM Rendezvous Points angezeigt.



Abb. 131: Multicast->PIM->PIM-Rendezvous-Punkte

14.4.2.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um PIM Rendezvous Points zu konfigurieren.

PIM-Schnittstellen
PIM-Rendezvous-Punkte
PIM-Optionen

Einstellungen für PIM-Rendezvous-Punkt	
Multicast-Gruppenbereich	Bestimmter Bereich ▼
Multicast-Gruppen-Adresse	<input style="width: 100%;" type="text"/>
Präfixlänge der Multicast-Gruppe	<input style="width: 100%;" type="text" value="4"/>
Rendezvous Point IP-Adresse	<input style="width: 100%;" type="text"/>
Vorrang	<input style="width: 100%;" type="text" value="0"/>

OK
Abbrechen

Abb. 132: Multicast->PIM->PIM-Rendezvous-Punkte->Neu

Das Menü **Multicast->PIM->PIM-Rendezvous-Punkte->Neu** besteht aus folgenden Feldern:

Felder im Menü Einstellungen für PIM-Rendezvous-Punkt

Feld	Beschreibung
Multicast-Gruppenbereich	Wählen Sie die Multicast-Gruppen für den PIM Rendezvous Point aus. Sie können <ul style="list-style-type: none"> • <i>Alle Gruppen</i> (Standardwert) angeben oder mit Auswahl von • <i>Bestimmter Bereich</i> ein Multicast-Netzwerksegment spezifizieren.
Multicast-Gruppen-Adresse	Nur bei Multicast-Gruppenbereich = <i>Bestimmter Bereich</i> Geben Sie hier die IP-Adresse des Multicast-Netzwerksegments ein.
Präfixlänge der Multicast-Gruppe	Nur bei Multicast-Gruppenbereich = <i>Bestimmter Bereich</i> Geben Sie hier die Netzmaskenlänge des Multicast-Netzwerksegments ein. 224.0.0.0/4 bezeichnet das komplette Multicast Class D Segment.

Feld	Beschreibung
	Wertebereich: 4 (Standardwert) bis 32.
Rendezvous Point IP-Adresse	Geben Sie die IP-Adresse oder den Hostnamen des Rendezvous Points ein.
Vorrang	<p>Geben Sie den Wert für pimGroupMappingPrecedence ein, der für statische RP Konfigurationen verwendet werden soll. Dieses erlaubt die genaue Kontrolle darüber, welche Konfiguration durch diese statische Konfiguration ersetzt werden soll.</p> <p>Wenn die Funktion aktiviert ist, wird pimStaticRPOverrideDynamic ignoriert. Die absoluten Werte dieses Objekts haben nur Bedeutung auf dem lokalen Router und müssen nicht mit anderen Routern abgestimmt werden.</p> <p>Die Funktion ist mit dem Standardwert 0 deaktiviert. Wenn die Funktion durch Setzen eines Wertes nicht 0 aktiviert wird, kann das verschiedene Auswirkungen auf andere Router haben. Verwenden Sie daher diese Funktion nicht, wenn eine genaue Kontrolle des Verhaltens des statischen RP nicht benötigt wird.</p>

14.4.3 PIM-Optionen

[PIM-Schnittstellen](#) | [PIM-Rendezvous-Punkte](#) | **PIM-Optionen**

Grundeinstellungen	
PIM-Status	<input type="checkbox"/> Aktiviert
Keepalive-Periode	210 Sekunden
Register Suppression Timer	60 Sekunden

Abb. 133: Multicast->PIM->PIM-Optionen

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

Felder im Menü Grundeinstellungen

Feld	Beschreibung
PIM-Status	Wählen Sie aus ob PIM aktiviert werden soll. Mit Auswahl von <i>Aktivieren</i> wird die Funktion aktiv.

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Keepalive-Periode	<p>Geben Sie die Zeitspanne in Sekunden ein, in der eine Keepalive Nachricht gesendet werden muss.</p> <p>Mögliche Werte: 0 bis 65535.</p> <p>Der Standardwert ist 210.</p>
Register Suppression Timer	<p>Geben Sie die Zeit in Sekunden an, nach der ein PIM Designated Router (DR) keine register-encapsulated Daten mehr zum Rendezvous Point (RP) schicken soll, nachdem die Register-Stop-Nachricht empfangen wurde. Dieses Objekt wird verwendet, um sowohl am DR als auch am RP Timer zu nutzen. Dieser Zeitraum wird in der PIM-SM Spezifikation Register_Suppression_Time genannt.</p> <p>Mögliche Werte: 0 bis 65535.</p> <p>Der Standardwert ist 60.</p>

Kapitel 15 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.

15.1 Internet + Einwählen

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

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

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







Hinweis

Beachten Sie die Vorgaben Ihres Providers!

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

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

Mögliche Werte für Status

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

Authentifizierung

Wenn ein Ruf eingeht, wird je nach Konfiguration eine PPP-Authentifizierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird. Dazu benötigt Ihr Gerät Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentifizierungsverhandlung ausgeführt werden soll, anschließend tragen Sie ein gemeinsames Passwort und zwei Kennungen ein. Diese Daten erhalten Sie z. B. von Ihrem Internet Service Provider oder dem Systemadministrator der Firmenzentrale. Stimmen die von Ihnen auf Ihrem Gerät eingetragenen Daten mit den Daten des Anrufers überein, wird der Ruf angenommen. Stimmen die Daten nicht überein, wird der Ruf abgewiesen.

Default Route

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

NAT aktivieren

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

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

Timeout bei Inaktivität festlegen

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

Blockieren nach Verbindungsfehler

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

15.1.1 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.

15.1.1.1 Neu

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

Basisparameter	
Beschreibung	<input type="text"/>
PPPoE-Modus	<input checked="" type="radio"/> Standard <input type="radio"/> Mehrfachverbindung
PPPoE-Ethernet-Schnittstelle	Eine auswählen <input type="button" value="v"/>
Benutzername	<input type="text"/>
Passwort	••••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	300 <input type="text"/> Sekunden
IP-Modus und Routen	
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Blockieren nach Verbindungsfehler für	60 <input type="text"/> Sekunden
Maximale Anzahl der erneuten Einwählversuche	5 <input type="text"/>
Authentifizierung	PAP <input type="button" value="v"/>
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
MTU	<input checked="" type="checkbox"/> Automatisch
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 134: 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>Mehrfachverbindung</i> , so können Sie mehrere DSL-Verbindungen eines Providers über PPP als stati-

Feld	Beschreibung
	<p>sche 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 PP-PoE-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 Physikalische Schnittstellen->ATM->Profile->Neu für diese Verbindung konfigurierte EthoA-Schnittstelle aus.</p>
PPPoE-Schnittstelle für Mehrfachlink	<p>Nur für PPPoE-Modus= <i>Mehrfachverbindung</i></p> <p>Wählen Sie alle Schnittstellen aus, die Sie für Ihre Internetverbindung nutzen wollen. Klicken Sie die Hinzufügen-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>

Feld	Beschreibung
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist.</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von <i>0</i> bis <i>3600</i> (Sekunden). <i>0</i> deaktiviert den Shorthold.</p> <p>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 IP-Modus und Routen

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

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

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. 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 diesen Verbindungspartner aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p>

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

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

15.1.2 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.

15.1.2.1 Neu

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

Basisparameter	
Beschreibung	<input type="text"/>
PPTP-Ethernet-Schnittstelle	Eine auswählen ▾
Benutzername	<input type="text"/>
Passwort	••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	300 Sekunden
IP-Modus und Routen	
IP-Adressmodus	<input type="radio"/> Statisch <input checked="" type="radio"/> IP-Adresse abrufen
Standardroute	<input checked="" type="checkbox"/> Aktiviert
NAT-Eintrag erstellen	<input checked="" type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Blockieren nach Verbindungsfehler für	60 Sekunden
Maximale Anzahl der erneuten Einwählversuche	5
Authentifizierung	PAP ▾
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
PPTP-Adressmodus	Statisch
Lokale PPTP-IP-Adresse	10.0.0.140
Entfernte PPTP-IP-Adresse	10.0.0.138
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 135: WAN->Internet + Einwählen->PPTP->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen beliebigen Namen ein, um die Internetverbindung eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.</p>
PPTP-Ethernet-Schnittstelle	<p>Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden.</p> <p>Bei Verwendung eines externen DSL-Modems, wählen Sie hier</p>

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

Felder im Menü IP-Modus und Routen

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

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

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät un-

Feld	Beschreibung
	ternommen werden soll. Standardwert ist <i>60</i> .
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte sind <i>0</i> bis <i>100</i>.</p> <p>Der Standardwert ist <i>5</i>.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i>: Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keiner</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für</p>

Feld	Beschreibung
	<p>asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
PPTP-Adressmodus	<p>Zeigt den Adressmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i>: Die Lokale PPTP-IP-Adresse wird dem ausgewählten Ethernet-Port zugewiesen.
Lokale PPTP-IP-Adresse	<p>Weisen Sie der PPTP-Schnittstelle eine IP-Adresse zu, die als Quelladresse verwendet wird.</p> <p>Standardwert ist <i>10.0.0.140</i>.</p>
Entfernte PPTP-IP-Adresse	<p>Geben Sie die IP-Adresse des PPTP-Partners ein.</p> <p>Standardwert ist <i>10.0.0.138</i>.</p>
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

15.1.3 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.

15.1.3.1 Bearbeiten oder Neu

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

PPPoE PPTP PPPoA ISDN **IP Pools**

Basisparameter					
IP-Poolname	<input style="width: 90%;" type="text"/>				
IP-Adressbereich	<input style="width: 45%;" type="text"/> - <input style="width: 45%;" type="text"/>				
DNS-Server	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Primär</td> <td style="padding: 2px;"><input style="width: 65%;" type="text"/></td> </tr> <tr> <td style="padding: 2px;">Sekundär</td> <td style="padding: 2px;"><input style="width: 65%;" type="text"/></td> </tr> </table>	Primär	<input style="width: 65%;" type="text"/>	Sekundär	<input style="width: 65%;" type="text"/>
Primär	<input style="width: 65%;" type="text"/>				
Sekundär	<input style="width: 65%;" type="text"/>				

OK Abbrechen

Abb. 136: WAN->Internet + Einwählen+IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

15.2 Real Time Jitter Control

Bei Telefongesprächen über das Internet haben Sprachdaten-Pakete normalerweise höchste Priorität. Trotzdem können bei geringer Bandbreite der Upload Verbindung während eines Telefongesprächs merkbare Verzögerungen bei der Sprachübertragung auftreten, wenn gleichzeitig andere Datenpakete geroutet werden.

Die Funktion Real Time Jitter Control löst dieses Problem. Um die "Leitung" für die Sprachdaten-Pakete nicht zu lange zu blockieren, wird die Größe der übrigen Datenpakete während eines Telefongesprächs bei Bedarf reduziert.

15.2.1 Regulierte Schnittstellen

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

15.2.1.1 Neu

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

Regulierte Schnittstellen

Grundeinstellungen	
Schnittstelle	Keine ▾
Kontrollmodus	Nur kontrollierte RTP-Streams ▾
Maximale Upload-Geschwindigkeit	0 kbit/s

Abb. 137: **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.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Nur kontrollierte RTP-Streams</i> (Standardwert): Anhand der Daten, die über das Media Gateway geroutet werden, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung.• <i>Alle RTP-Streams</i>: Alle RTP-Streams werden optimiert.• <i>Inaktiv</i>: Die Optimierung für die Übertragung der Sprachdaten wird nicht durchgeführt.• <i>Immer</i>: Die Optimierung für die Übertragung der Sprachdaten wird immer durchgeführt.
Maximale Upload-Geschwindigkeit	Geben Sie die maximal zur Verfügung stehende Bandbreite in Upload-Richtung in kbit/s für die gewählte Schnittstelle ein.

Kapitel 16 VPN

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

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

Zum Aufbau eines VPN-Tunnels stehen verschiedene Protokolle zur Verfügung, wie z. B. IPSec oder PPTP.

Die Authentifizierung der Verbindungspartner erfolgt über ein Passwort, mithilfe von Pre-shared Keys oder über Zertifikate.

Bei IPSec wird die Verschlüsselung der Daten z. B. mit Hilfe von AES oder 3DES erledigt, bei PPTP kann MPPE benutzt werden.

16.1 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 122) integriert werden. Die IPSec-Implementierung erreicht dieses Ziel zum einen durch die Benutzung des Authentication-Header-(AH)-Protokolls und des Encapsulated-Security-Payload-(ESP)-Protokolls. Zum anderen werden kryptografische Schlüsselverwaltungsmechanismen wie das Internet-Key-Exchange-(IKE)-Protokoll verwendet.

Zusätzlicher Filter des Datenverkehrs

Teldat Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode ist ausschließlich über das Setup Tool konfigurierbar. Mit dem GUI verwenden Sie die Routing-basierte Methode. (Letztere ist zusätzlich auch über das Setup Tool verfügbar.)

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IPSec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IPSec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IPSec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des Datenverkehrs**, so wird es verworfen.

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



Hinweis

Der Parameter **Zusätzlicher Filter des Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.



Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

16.1.1 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 angezeigt.

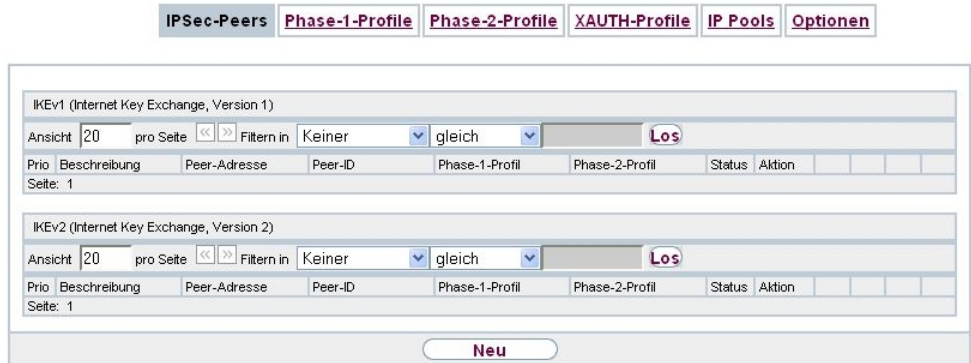



Abb. 138: VPN->IPSec->IPSec-Peers

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 487.

16.1.1.1 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	<input type="text" value="Peer-1"/>															
Peer-Adresse	<input type="text"/>															
Peer-ID	Fully Qualified Domain Name (FQDN) <input type="text" value="Peer-1"/>															
IKE (Internet Key Exchange)	<input type="text" value="IKEv1"/>															
Preshared Key	<input type="text"/>															
Schnittstellenrouten																
IP-Adressenvergabe	<input type="text" value="Statisch"/>															
Standardroute	<input type="checkbox"/> Aktiviert															
Lokale IP-Adresse	<input type="text"/>															
Routeneinträge	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Entfernte IP-Adresse</th> <th style="width: 20%;">Netzmaske</th> <th style="width: 10%;">Metrik</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text" value="1"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="button" value="Hinzufügen"/>						
Entfernte IP-Adresse	Netzmaske	Metrik														
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>													
<input type="button" value="Hinzufügen"/>																
Zusätzlicher Filter des Datenverkehrs																
Zusätzlicher Filter des Datenverkehrs	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Beschreibung</th> <th style="width: 10%;">Protokoll</th> <th style="width: 20%;">Quell-IP/Maske:Port</th> <th style="width: 20%;">Ziel-IP/Maske:Port</th> <th style="width: 10%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="5" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </tbody> </table>	Beschreibung	Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Hinzufügen"/>				
Beschreibung	Protokoll	Quell-IP/Maske:Port	Ziel-IP/Maske:Port													
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>												
<input type="button" value="Hinzufügen"/>																

Erweiterte Einstellungen

Erweiterte IPSec-Optionen	
Phase-1-Profil	<input type="text" value="Keines (Standardprofil verwenden)"/>
Phase-2-Profil	<input type="text" value="Keines (Standardprofil verwenden)"/>
XAUTH-Profil	<input type="text" value="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 Quell-IP-Adresse	<input type="checkbox"/> Aktiviert
Überprüfung der Rückroute	<input type="checkbox"/> Aktiviert
Proxy ARP	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv
IPSec-Callback	
Modus	<input type="text" value="Inaktiv"/>

Abb. 139: VPN->IPSec->IPSec-Peers->Neu

Das Menü VPN->IPSec->IPSec-Peers->Neu besteht aus folgenden Feldern:

Felder im Menü Peer-Parameter

Feld	Beschreibung
Administrativer Status	<p>Wählen Sie den Zustand aus, in den Sie den Peer nach dem Speichern der Peer-Konfiguration versetzen wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Der Peer steht nach dem Speichern der Konfiguration sofort für den Aufbau eines Tunnels zur Verfügung. • <i>Inaktiv</i>: Der Peer steht nach dem Speichern der Konfiguration zunächst nicht zur Verfügung.
Beschreibung	<p>Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
Peer-Adresse	<p>Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein.</p> <p>Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.</p>
Peer-ID	<p>Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein.</p> <p>Die Eingabe kann in bestimmten Konfigurationen entfallen.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p> <p>Mögliche ID-Typen:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüssel-ID</i>: Beliebige Zeichenkette <p>Auf dem Peer-Gerät entspricht diese ID dem Parameter Lokaler ID-Wert.</p>
IKE (Internet Key Exchange)	<p>Für Geräte der WLxxxxn-Serie nicht verfügbar. Diese Geräte unterstützen nur IKEv1.</p>

Feld	Beschreibung
	<p>Wählen Sie die Version des Internet-Key-Exchange-Protokolls, die verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>IKEv1</i> (Standardwert): Internet Key Exchange Protocol Version 1 • <i>IKEv2</i>: Internet Key Exchange Protocol Version 2
Authentifizierungsmethode	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv2</i></p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Preshared Keys wählen. Diese werden bei der Peerkonfiguration im Menü IPSec-Peers konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert.
Lokaler ID-Typ	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv2</i></p> <p>Wählen Sie den Typ der lokalen ID aus.</p> <p>Mögliche ID-Typen:</p> <ul style="list-style-type: none"> • <i>Fully Qualified Domain Name (FQDN)</i> • <i>E-Mail-Adresse</i> • <i>IPV4-Adresse</i> • <i>ASN.1-DN (Distinguished Name)</i> • <i>Schlüssel-ID</i>: Beliebige Zeichenkette
Lokale ID	<p>Nur für IKE (Internet Key Exchange) = <i>IKEv2</i></p> <p>Geben Sie die ID Ihres Geräts ein.</p> <p>Für Authentifizierungsmethode = <i>DSA-Signatur</i> oder <i>RSA-Signatur</i> wird die Option Subjektname aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektname aus Zertifikat verwenden</p>

Feld	Beschreibung
	<p>aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektnamen des Zertifikats verwendet.</p> <p>Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe Zertifikate auf Seite 122), 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>

Felder im Menü Schnittstellenrouten

Feld	Beschreibung
IP-Adressenvergabe	<p>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Geben Sie eine statische IP-Adresse ein. • <i>Client im IKE-Konfigurationsmodus</i>: Nur für IKEv1 auswählbar. Wählen Sie diese Option, wenn Ihr Gateway als IPSec-Client vom Server eine IP-Adresse erhalten soll. • <i>Server im IKE-Konfigurationsmodus</i>: Wählen Sie diese Option, wenn Ihr Gateway als Server sich verbindenden Clients eine IP-Adresse vergeben soll. Diese wird aus dem gewählten IP-Zuordnungspool entnommen.
Konfigurationsmodus	<p>Nur bei IP-Adressenvergabe = <i>Server im IKE-Konfigurationsmodus</i> oder <i>Client im IKE-Konfigurationsmodus</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Pull</i> (Standardwert): Der Client erfragt die IP-Adresse und das Gateway beantwortet die Anfrage. • <i>Push</i>: Das Gateway schlägt dem Client eine IP-Adresse vor und der Client muss diese akzeptieren oder zurückweisen.

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

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

Felder im Menü **Zusätzlicher Filter des Datenverkehrs**

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

Zusätzlicher Filter des Datenverkehrs

Teldat Gateways unterstützen zwei verschiedene Methoden zum Aufbau von IPSec-Verbindungen:

- eine Richtlinien-basierte Methode und
- eine Routing-basierte Methode.

Die Richtlinien-basierte Methode ist ausschließlich über das Setup Tool konfigurierbar. Mit dem GUI verwenden Sie die Routing-basierte Methode. (Letztere ist zusätzlich auch über das Setup Tool verfügbar.)

Die Richtlinien-basierte Methode nutzt Filter für den Datenverkehr zur Aushandlung der IP-Sec-Phase-2-SAs. Damit ist eine sehr "feinkörnige" Filterung der IP-Pakete bis auf Protokoll- und Portebene möglich.

Die Routing-basierte Methode bietet gegenüber der Richtlinien-basierte Methode verschiedene Vorteile, wie z. B. NAT/PAT innerhalb eines Tunnels, IPSec in Verbindung mit Routing-Protokollen und Realisierung von VPN-Backup-Szenarien. Bei der Routing-basierten Methode werden zur Aushandlung der IP-Sec-Phase-2-SAs die konfigurierten oder dynamisch gelernten Routen genutzt. Diese Methode vereinfacht zwar viele Konfigurationen, gleichzeitig kann es aber zu Problemen wegen konkurrierender Routen oder wegen der "gröberen" Filterung des Datenverkehrs kommen.

Der Parameter **Zusätzlicher Filter des Datenverkehrs** behebt dieses Problem. Sie können "feiner" filtern, d.h. Sie können z. B. die Quell-IP-Adresse oder den Quell-Port angeben. Ist ein **Zusätzlicher Filter des Datenverkehrs** konfiguriert, so wird er zur Aushandlung der IP-Sec-Phase-2-SAs herangezogen, die Route bestimmt nur noch, welcher Datenverkehr geroutet werden soll.

Passt ein IP-Paket nicht zum definierten **Zusätzlicher Filter des Datenverkehrs**, so wird es verworfen.

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



Hinweis

Der Parameter **Zusätzlicher Filter des Datenverkehrs** ist ausschließlich für den Initiator der IPSec-Verbindung relevant, er gilt nur für ausgehenden Datenverkehr.



Hinweis

Beachten Sie, dass die Konfiguration der Phase-2-Richtlinien auf beiden IPSec-Tunnel-Endpunkten identisch sein muss.

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

The screenshot shows the configuration interface for an IPSec Peer. The 'Phase-2-Profil' tab is active. A modal dialog titled 'Basisparameter' is open, allowing the user to add a new filter. The dialog contains the following fields:

- Beschreibung:** A text input field.
- Protokoll:** A dropdown menu currently set to 'Beliebig'.
- Quell-IP-Adresse/Netzmaske:** A dropdown menu set to 'Netzwerk' followed by two input fields for IP and mask.
- Ziel-IP-Adresse/Netzmaske:** A dropdown menu set to 'Netzwerk' followed by two input fields for IP and mask.

Buttons for 'Übernehmen' and 'Abbrechen' are located at the bottom of the dialog. Below the dialog, the main configuration form shows fields for 'Administrativer Status' (Aktiv/Inaktiv), 'Beschreibung' (Peer-2), 'Peer-ID', 'IKE (Intern)', 'Preshared', 'Schnittstelle', 'IP-Adresse', 'Standardprotokoll', 'Lokale IP-Adresse' (0.0.0.0), 'Metrik' (1), and 'Zusätzlicher Filter des Datenverkehrs'. A 'Hinzufügen' button is visible at the bottom of the filter section. At the very bottom of the interface are 'Erweiterte Einstellungen', 'OK', and 'Abbrechen' buttons.

Abb. 140: 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	Definieren Sie, falls gewünscht, die Quell-IP-Adresse und die Netzmaske der Datenpakete. Mögliche Werte: <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>Host</i>: Geben Sie die IP-Adresse des Hosts ein. • <i>Netzwerk</i> (Standardwert): Geben Sie die Netzwerk-Adresse und die zugehörige Netzmaske ein.
Quell-Port	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i> Geben Sie den Quell-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.
Ziel-IP-Adresse/Netzmaske	Geben Sie die Ziel-IP-Adresse und die zugehörige Netzmaske der Datenpakete ein.
Ziel-Port	Nur für Protokoll = <i>TCP</i> oder <i>UDP</i> Geben Sie den Ziel-Port der Datenpakete ein. Die Standardeinstellung <i>-Alle-</i> (= -1) bedeutet, dass der Port nicht näher spezifiziert ist.

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

Felder im Menü Erweiterte IPsec-Optionen

Feld	Beschreibung
Phase-1-Profil	Wählen Sie ein Profil für die Phase 1 aus. Neben den benutzerdefinierten Profilen stehen vordefinierte Profile zur Verfügung. Mögliche Werte: <ul style="list-style-type: none"> • <i>Keines (Standardprofil verwenden)</i>: Verwendet das Profil, das in VPN->IPsec->Phase-1-Profile als Standard markiert ist

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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 VPN->IPSec->Phase-1-Profile. • <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.
Startmodus	<p>Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt</p>

Feld	Beschreibung
	<p>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 Quell-IP-Adresse	<p>Wenn Sie mehrere Internetanschlüsse parallel betreiben, können Sie hier diejenige öffentliche IP-Adresse angeben, die für den Datenverkehr des Peers als Quelladresse verwendet werden soll. Wählen Sie aus, ob die Öffentliche Quell-IP-Adresse aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Geben Sie in das Eingabefeld die öffentliche IP-Adresse ein, die als Absendeadresse verwendet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Überprüfung der Rückroute	<p>Wählen Sie aus, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
MobiKE	<p>Nur für Peers mit IKEv2.</p> <p>MobiKE ermöglicht es, bei wechselnden öffentlichen IP-Adressen lediglich diese Adressen in den SAs zu aktualisieren, ohne die SAs selbst neu aushandeln zu müssen.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Beachten Sie, dass MobiKE einen aktuellen IPSec Client voraussetzt, z. B. den aktuellen Windows-7- oder Windows-8-Client oder die neuste Version des Teldat IPSec Clients.</p>
Proxy ARP	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner</p>

Feld	Beschreibung
	<p>beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen IPSec-Peer. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec Peer <i>aktiv</i> (aktiv) oder <i>Ruhend</i> (ruhend) ist. Bei <i>Ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPSec-Peer <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum IP-Sec Peer besteht.

IPSec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das Internet zu ermöglichen, unterstützen Teldat-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 Tun-

nelaufbau 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 Call-back 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.teldat.de. 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 un-

terschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht. Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in *Felder im Menü IPSec-Callback* auf Seite 344 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 Ver-

wendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.



Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Die folgenden Optionen sind nur auf Geräten mit ISDN-Anschluss verfügbar:

Felder im Menü IPSec-Callback

Feld	Beschreibung
Modus	<p>Wählen Sie den Callback-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): IPSec-Callback ist deaktiviert. Das lokale Gerät reagiert weder auf eingehende ISDN-Rufe noch initiiert es ISDN-Rufe zum entfernten Gerät. • <i>Passiv</i>: Das lokale Gerät reagiert lediglich auf eingehende ISDN-Rufe und initiiert ggf. den Aufbau eines IPSec-Tunnels zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. • <i>Aktiv</i>: Das lokale Gerät setzt einen ISDN-Ruf an das entfernte Gerät ab, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen. Auf eingehende ISDN-Rufe reagiert das Gerät nicht. • <i>Beide</i>: Ihr Gerät kann auf eingehende ISDN-Rufe reagieren und ISDN-Rufe an das entfernte Gerät absetzen. Der Aufbau eines IPSec-Tunnels wird sowohl ausgeführt (nach einem eingehenden ISDN-Ruf) als auch veranlasst (durch einen ausgehenden ISDN-Ruf).
Ankommende Rufnummer	<p>Nur für Modus = <i>Passiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.</p>

Feld	Beschreibung
Ausgehende Rufnummer	<p>Nur für Modus = <i>Aktiv</i> oder <i>Beide</i></p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number). Es können auch Wildcards verwendet werden.</p>
Eigene IP-Adresse per ISDN/GSM übertragen	<p>Wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Geräts über ISDN übertragen werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Übertragungsmodus	<p>Nur für Eigene IP-Adresse per ISDN/GSM übertragen = aktiviert</p> <p>Wählen Sie aus, in welchem Modus Ihr Gerät versuchen soll, seine IP-Adresse an den Peer zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung des besten Modus</i>: Ihr Gerät bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird. (Die Verwendung des B-Kanals verursacht Kosten.) • <i>Nur D-Kanalmodi automatisch erkennen</i>: Ihr Gerät bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. • <i>Spezifischen D-Kanalmodus verwenden</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. • <i>Spezifischen D-Kanalmodus versuchen, auf B-Kanal zurückgehen</i>: Ihr Gerät versucht, die IP-Adresse in dem im Feld Modus eingestellten Modus zu übertragen. 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>

Feld	Beschreibung
	<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.

16.1.2 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 pro Seite ◀ ▶ Filtern in Keiner ▼ gleich ▼ Los

Standard	Beschreibung	Proposals	Authentifizierung	Modus	DH-Gruppe	Lebensdauer

Seite: 1

Neues IKEv1-Profil erstellen Neu

IKEv2 (Internet Key Exchange, Version 2)

Ansicht pro Seite ◀ ▶ Filtern in Keiner ▼ gleich ▼ Los

Beschreibung	Proposals	Lebensdauer

Seite: 1

Neues IKEv2-Profil erstellen Neu

OK Abbrechen

Abb. 141: **VPN->IPSec->Phase-1-Profile**

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

16.1.2.1 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"> <thead> <tr> <th>Verschlüsselung</th> <th>Authentifizierung</th> <th>Aktiviert</th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>MD5</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>					Verschlüsselung	Authentifizierung	Aktiviert	AES	MD5	<input checked="" type="checkbox"/>	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>
Verschlüsselung	Authentifizierung	Aktiviert															
AES	MD5	<input checked="" 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 Lebensdauer																
Authentifizierungsmethode	Preshared Keys																
Modus	<input type="radio"/> Main Modus (ID Protect) <input checked="" type="radio"/> Aggressiv <input type="checkbox"/> Strikt																
Lokaler ID-Typ	Fully Qualified Domain Name (FQDN)																
Lokaler ID-Wert	r4402																
Erweiterte Einstellungen																	
Erreichbarkeitsprüfung	Automatische Erkennung																
Blockzeit	30 Sekunden																
NAT-Traversal	Aktiviert																
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>																	

Abb. 142: 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 Al-

Feld	Beschreibung
	<p>gorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird.</p> <ul style="list-style-type: none"> • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. • <i>AES</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird die AES-Schlüssellänge des Partners verwendet. Hat dieser ebenfalls den Parameter <i>AES</i> gewählt, wird eine Schlüssellänge von 128 Bit verwendet. • <i>AES-128</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 128 Bits angewendet. • <i>AES-192</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 Bits angewendet. • <i>AES-256</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speicheranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 Bits angewendet. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i> (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>SHA1</i>: SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IP-Sec verwendet. • <i>RipeMD 160</i>: RipeMD 160 ist ein 160 Bit Hash-Algorithmus. Er wird als sicherer Ersatz für MD5 und RipeMD angewandt. • <i>Tiger192</i>: Tiger 192 ist ein relativ neuer und sehr schneller Algorithmus. <p>Beachten Sie, dass die Beschreibung der Verschlüsselung und Authentifizierung oder der Hash-Algorithmen auf dem Kenntnisstand und der Meinung des Autors zum Zeitpunkt der Erstellung dieses Handbuchs basiert. Die Qualität der Algorithmen im besonderen unterliegt relativen Gesichtspunkten und kann sich aufgrund von mathematischen oder kryptographischen Weiterentwicklungen ändern.</p>
DH-Gruppe	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Die Diffie-Hellman-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von Teldat-Geräten unterstützt wird, steht für "modular exponentiation".</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>2 (1024 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>5 (1536 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	<p>Legen Sie die Lebensdauer für Phase-1-Schlüssel fest.</p> <p>Der Standardwert beträgt gemäß RFC 2407 acht Stunden, das</p>

Feld	Beschreibung
	<p>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-1- Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Standardwert ist <i>14400</i>. • 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. Standardwert ist <i>0</i>. Der Defaultwert lt. RFC wird verwendet, wenn <i>0</i> Sekunden und <i>0</i> KBytes eingetragen werden. <p>Der Standardwert lt. RFC wird verwendet, wenn <i>0</i> Sekunden und <i>0</i> KBytes eingetragen werden.</p>
Authentifizierungsmethode	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Authentifizierungsmethode aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Preshared Keys</i> (Standardwert): Falls Sie für die Authentifizierung keine Zertifikate verwenden, können Sie Pre Shared Keys wählen. Diese werden bei der Peerkonfiguration im Menü VPN->IPSec->IPSec-Peers konfiguriert. Der Preshared Key ist das gemeinsame Passwort. • <i>DSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des DSA-Algorithmus authentifiziert. • <i>RSA-Signatur</i>: Phase-1-Schlüsselberechnungen werden unter Nutzung des RSA-Algorithmus authentifiziert. • <i>RSA-Verschlüsselung</i>: Mit RSA-Verschlüsselung werden als erweiterte Sicherheit zusätzlich die ID-Nutzdaten verschlüsselt.
Lokales Zertifikat	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Nur für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p>

Feld	Beschreibung
	<p>Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>
Modus	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie den Phase-1-Modus aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aggressiv</i> (Standardwert): Der Aggressive Modus ist erforderlich, falls einer der Peers keine statische IP-Adresse hat und Preshared Keys für die Authentifizierung genutzt werden. Er erfordert nur drei Meldungen für die Einrichtung eines sicheren Kanals. • <i>Main Modus (ID Protect)</i>: Dieser Modus (auch als Main Mode bezeichnet) erfordert sechs Meldungen für eine Diffie-Hellman-Schlüsselberechnung und damit für die Einrichtung eines sicheren Kanals, über den die IPSec-SAs ausgehandelt werden. Er setzt voraus, dass beide Peers statische IP-Adressen haben, falls für die Authentifizierung Preshared Keys genutzt werden. <p>Wählen Sie weiterhin aus, ob der gewählte Modus ausschließlich verwendet werden darf (Strikt) oder der Peer auch einen anderen Modus vorschlagen kann.</p>
Lokaler ID-Typ	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie den Typ der lokalen ID aus.</p> <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>

Feld	Beschreibung
	<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 122), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr Partner für Sie konfiguriert, identisch sind.</p>

Erreichbarkeitsprüfung

In der Kommunikation zweier IPSec-Peers kann es dazu kommen, dass einer der beiden z. B. aufgrund von Routing-Problemen oder aufgrund eines Neustarts nicht erreichbar ist. Dies ist aber erst dann feststellbar, wenn das Ende der Lebensdauer der Sicherheitsverbindung erreicht ist. Bis zu diesem Zeitpunkt gehen die Datenpakete verloren. Um dies zu verhindern, gibt es verschiedene Mechanismen einer Erreichbarkeitsprüfung. Im Feld **Erreichbarkeitsprüfung** wählen Sie aus, ob ein Mechanismus angewendet werden soll, um die Erreichbarkeit eines Peers zu überprüfen.

Hierbei stehen zwei Mechanismen zur Verfügung: Heartbeats und Dead Peer Detection.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Erreichbarkeitsprüfung	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Wählen Sie die Methode aus, mit der die Funktionalität der IP-Sec-Verbindung überprüft werden soll.</p> <p>Neben dem Standardverfahren Dead Peer Detection (DPD) ist auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekun-</p>

Feld	Beschreibung
	<p>den Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Ihr Gerät erkennt und verwendet den Modus, den die Gegenstelle unterstützt. • <i>Inaktiv</i>: Ihr Gerät sendet und erwartet keinen Heartbeat. Wenn Sie Geräte anderer Hersteller verwenden, setzen Sie diese Option. • <i>Heartbeats (Nur erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer, sendet selbst aber keinen. • <i>Heartbeats (Nur senden)</i>: Ihr Gerät erwartet keinen Heartbeat vom Peer, sendet aber einen. • <i>Heartbeats (Senden & Erwarten)</i>: Ihr Gerät erwartet einen Heartbeat vom Peer und sendet selbst einen. • <i>Dead Peer Detection</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Erreichbarkeit des Peers nur überprüft, wenn tatsächlich Daten an ihn gesendet werden sollen. • <i>Dead Peer Detection (Idle)</i>: DPD (Dead Peer Detection) gemäß RFC 3706 verwenden. DPD benutzt ein Request-Reply-Protokoll um die Erreichbarkeit der Gegenstelle zu überprüfen, und kann auf beiden Seiten unabhängig konfiguriert werden. Mit dieser Option wird die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vorgenommen. <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>

Feld	Beschreibung
	<p>Zur Verfügung stehen Werte von -1 bis 86400 (Sekunden), der Wert -1 bedeutet die Übernahme des Wertes im Standardprofil, der Wert 0, dass der Peer in keinem Fall blockiert wird.</p> <p>Standardwert ist 30.</p>
<p>NAT-Traversal</p>	<p>NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.</p> <p>Ohne NAT-T kann es zwischen IPSec und NAT zu Inkompatibilitäten kommen (siehe RFC 3715, Abschnitt 2). Diese behindern vor allem den Aufbau eines IPSec-Tunnels von einem Host innerhalb eines LANs und hinter einem NAT-Gerät zu einem anderen Host bzw. Gerät. NAT-T ermöglicht derartige Tunnel ohne Konflikte mit NAT-Geräten, aktiviertes NAT wird vom IPSec-Daemon automatisch erkannt und NAT-T wird verwendet.</p> <p>Nur für <i>IKEv1-Profile</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiviert</i> (Standardwert): NAT-Traversal ist aktiv. • <i>Deaktiviert</i>: NAT-Traversal ist deaktiviert. • <i>Erzwingen</i>: Das Gerät verhält sich in jedem Fall so, als ob NAT eingesetzt würde. <p>Nur für <i>IKEv2-Profile</i></p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>CA-Zertifikate</p>	<p>Nur für Phase-1-Parameter (IKE)</p> <p>Nur für Authentifizierungsmethode = <i>DSA-Signatur, RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Wenn Sie die Option Folgenden CA-Zertifikaten vertrauen aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen.</p> <p>Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.</p>

16.1.3 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 configuration interface with the following elements:

- Navigation tabs: **IPSec-Peers**, **Phase-1-Profile**, **Phase-2-Profile** (selected), **XAUTH-Profile**, **IP Pools**, **Optionen**.
- Table header: Ansicht 20 pro Seite, Filtern in Keiner, gleich, Los.
- Table columns: Standard, Beschreibung, Proposals, PFS-Gruppe, Lebensdauer.
- Table content: One row with 'Standard' checked.
- Buttons: **Neu**, **OK**, **Abbrechen**.

Abb. 143: **VPN->IPSec->Phase-2-Profile**

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

16.1.3.1 Neu

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

The screenshot shows the configuration interface with the following elements:

- Navigation tabs: **IPSec-Peers**, **Phase-1-Profile**, **Phase-2-Profile** (selected), **XAUTH-Profile**, **IP Pools**, **Optionen**.
- Section: **Phase-2-Parameter (IPSEC)**
- Form fields:
 - Beschreibung: IPSec-2
 - Proposals: Table with columns: Verschlüsselung (AES), Authentifizierung (MD5), Aktiviert (checkbox).
 - PFS-Gruppe verwenden: Aktiviert, 1 (768 Bit), 2 (1024 Bit), 5 (1536 Bit)
 - Lebensdauer: 7200 Sekunden, 0 kBytes, Schlüssel erneut erstellen nach 80 %
- Section: **Erweiterte Einstellungen**
- Form fields:
 - IP-Komprimierung: Aktiviert
 - Erreichbarkeitsprüfung: Automatische Erkennung
 - PMTU propagieren: Aktiviert
- Buttons: **OK**, **Abbrechen**.

Abb. 144: **VPN->IPSec->Phase-2-Profile->Neu**

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

Felder im Menü Phase-2-Parameter (IPSEC)

Feld	Beschreibung
Beschreibung	<p>Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert.</p> <p>Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.</p>
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Message-Hash-Algorithmen für IKE Phase 2 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und zwei Nachrichten-Hash-Algorithmen ergibt 12 mögliche Werte in diesem Feld.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <i>3DES</i> (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorithmus, der derzeit unterstützt wird. • <i>-- ALLE --</i>: Alle Optionen können verwendet werden. • <i>AES</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speichieranforderungen, 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 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

Feld	Beschreibung
	<p>von 256 Bits angewendet.</p> <ul style="list-style-type: none"> • <i>Twofish</i>: Twofish war ein finaler Kandidat für den AES (Advanced Encryption Standard). Er wird als genauso sicher eingestuft wie Rijndael (AES), ist aber langsamer. • <i>Blowfish</i>: Blowfish ist ein sehr sicherer und zugleich schneller Algorithmus. Twofish kann als Nachfolger von Blowfish angesehen werden. • <i>CAST</i>: CAST ist ebenfalls ein sehr sicherer Algorithmus, etwas langsamer als Blowfish, aber schneller als 3DES. • <i>DES</i>: DES ist ein älterer Verschlüsselungsalgorithmus, der aufgrund seiner kleinen effektiven Länge von 56 Bit als schwach eingestuft wird. <p>Hash-Algorithmen (Authentifizierung):</p> <ul style="list-style-type: none"> • <i>MD5</i> (Standardwert): MD5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • <i>-- ALLE --</i>: Alle Optionen können verwendet werden. • <i>SHA1</i>: SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist aber langsamer als MD5. Wird mit 96 Bit Digest Length für IPSec verwendet. <p>Beachten Sie, dass RipeMD 160 und Tiger 192 für Nachricht-Hashing in Phase 2 nicht zur Verfügung stehen.</p>
<p>PFS-Gruppe verwenden</p>	<p>Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (<i>Aktiviert</i>), sind die Optionen die gleichen, wie bei der Konfiguration von DH-Gruppe im Menü VPN->IPSec->Phase-1-Profile . PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind.</p> <p>Das Feld hat folgende Optionen:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation

Feld	Beschreibung
	<p>mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.</p> <ul style="list-style-type: none"> • <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. Standardwert ist 7200. • Eingabe in kBytes: Geben Sie die Lebensdauer für Phase-2- Schlüssel als Menge der verarbeiteten Daten in kBytes ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Standardwert ist 0. <p>Schlüssel erneut erstellen nach: Legen Sie fest, bei welchem Prozentsatz des Ablaufes der Lebensdauer die Schlüssel der Phase 2 neu erstellt werden.</p> <p>Die eingegebene Prozentzahl wird sowohl auf die Lebensdauer in Sekunden als auch auf die Lebensdauer in kBytes angewendet.</p> <p>Standardwert ist 80 %.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
IP-Komprimierung	<p>Wählen Sie aus, ob eine Kompression vor der Datenverschlüsselung eingeschaltet wird. Das kann bei gut komprimierbaren Daten zu einer höheren Performance und geringerem zu übertragenden Datenvolumen führen. Bei schnellen Leitungen oder nicht komprimierbaren Daten wird von der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erreichbarkeitsprüfung	<p>Wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden.</p> <p>Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, ist ein Teldat IPSec-Heartbeat implementiert worden. Dieser sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatische Erkennung</i> (Standardwert): Automatische Erkennung, ob die Gegenstelle ein Teldat-Gerät ist. Wenn ja, wird <i>Heartbeats (Senden &Erwarten)</i> (bei Gegenstelle mit Teldat) oder <i>Inaktiv</i> (bei Gegenstelle ohne Teldat) 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>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.

16.1.4 XAUTH-Profil

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

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

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

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

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

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

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

16.1.4.1 Neu

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

[IPSec-Peers](#) | [Phase-1-Profil](#) | [Phase-2-Profil](#) | **[XAUTH-Profil](#)** | [IP Pools](#) | [Optionen](#)

Basisparameter	
Beschreibung	<input type="text"/>
Rolle	Server ▾
Modus	RADIUS ▾
RADIUS-Server Gruppen-ID	Kein RADIUS-Server für XAUTH konfiguriert

Abb. 145: VPN->IPSec->XAUTH-Profil->Neu

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

Felder im Menü Basisparameter

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


Feld	Beschreibung
Passwort	Nur für Rolle = Client Geben Sie das Authentifizierungspasswort ein.
RADIUS-Server Gruppen-ID	Nur für Rolle = Server Wählen Sie die gewünschte in Systemverwaltung -> Remote Authentifizierung -> RADIUS konfigurierte RADIUS-Gruppe aus.
Benutzer	Nur für Rolle = Server und Modus = Lokal Ist Ihr Gateway als XAuth-Server konfiguriert, können die Clients über eine lokal konfigurierte Benutzerliste authentifiziert werden. Definieren Sie hier die Mitglieder der Benutzergruppe dieses XAUTH-Profiles, indem Sie den Authentifizierungsnamen des Clients (Name) und das Authentifizierungspasswort (Passwort) eingeben. Fügen Sie weitere Mitglieder mit Hinzufügen hinzu.

16.1.5 IP Pools

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

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

16.1.5.1 Bearbeiten oder Neu

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

[IPSec-Peers](#) | [Phase-1-Profile](#) | [Phase-2-Profile](#) | [XAUTH-Profile](#) | **IP Pools** | [Optionen](#)

Basisparameter	
IP-Poolname	<input type="text"/>
IP-Adressbereich	<input type="text"/> - <input type="text"/>
DNS-Server	Primär <input type="text"/>
	Sekundär <input type="text"/>

Abb. 146: VPN->IPSec+IP Pools->Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adress aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

16.1.6 Optionen

IPSec-Peers Phase-1-Profil Phase-2-Profil XAUTH-Profil IP Pools Optionen	
Globale Optionen	
IPSec aktivieren	<input type="checkbox"/> Aktiviert
Vollständige IPSec-Konfiguration löschen	
IPSec-Debug-Level	Debug <input type="button" value="v"/>
Erweiterte Einstellungen	
IPSec über TCP	<input type="checkbox"/> NCPPath Finder Technologie
Initial Contact Message senden	<input checked="" type="checkbox"/> Aktiviert
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<input type="checkbox"/> Aktiviert
Zero Cookies verwenden	<input checked="" type="checkbox"/> Aktiviert
Größe der Zero Cookies	32 Bit
Dynamische RADIUS-Authentifizierung	<input type="checkbox"/> Aktiviert
PKI-Verarbeitungsoptionen	
Zertifikatsanforderungs-Payloads nicht beachten	<input type="checkbox"/> Aktiviert
Zertifikatsanforderungs-Payloads senden	<input checked="" type="checkbox"/> Aktiviert
Zertifikatsketten senden	<input checked="" type="checkbox"/> Aktiviert
CRLs senden	<input type="checkbox"/> Aktiviert
Key Hash Payloads senden	<input checked="" type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 147: VPN->IPSec->Optionen

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

Felder im Menü Globale Optionen

Feld	Beschreibung
IPSec aktivieren	Wählen Sie, ob Sie IPSec aktivieren wollen. Mit <i>Aktiviert</i> wird die Funktion aktiv. Sobald ein IPSec Peer konfiguriert wird, ist die Funktion aktiv.
Vollständige IPSec-Konfiguration löschen	Wenn Sie das -Symbol klicken, löschen Sie die vollständige IPSec-Konfiguration Ihres Geräts. Dieses macht alle Einstellungen rückgängig, die während der IPSec-Konfiguration vorgenommen worden sind. Nachdem die

Feld	Beschreibung
	<p>Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen.</p> <p>Das Löschen der Konfiguration ist nur möglich mit IPSec aktivieren = nicht aktiviert.</p>
IPSec-Debug-Level	<p>Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Informationen</i> • <i>Debug</i> (Standardwert, niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level "Debug" sämtliche erzeugten Meldungen aufgezeichnet werden.</p>

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen Teldat-Geräten zusammenarbeitet, so dass Sie diese Werte nur ändern müssen, wenn die Gegenseite ein Fremdprodukt ist oder Ihnen bekannt ist, dass sie besondere Einstellungen benötigt. Dies kann beispielsweise notwendig sein, wenn die entfernte Seite mit älteren IPSec-Implementierungen arbeitet.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
IPSec über TCP	<p>Wählen Sie aus, ob IPSec über TCP verwendet werden soll.</p> <p>IPSec über TCP basiert auf der NCP-Path-Finder-Technologie. Diese Technologie sorgt dafür, dass der Datenverkehr (IKE,</p>

Feld	Beschreibung
	<p>ESP, AH) zwischen den Peers in eine Pseudo-HTTPS-Session eingebettet wird.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>Initial Contact Message senden</p>	<p>Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
<p>SAs mit dem Status der ISP-Schnittstelle synchronisieren</p>	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von <i>aktiv</i> zu <i>inaktiv</i>, <i>ruhend</i> oder <i>blockiert</i> geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
<p>Zero Cookies verwenden</p>	<p>Wählen Sie aus, ob auf Null gesetzte ISAKMP Cookies gesendet werden sollen.</p> <p>Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall <i>Aktiviert</i>.</p>
<p>Größe der Zero Cookies</p>	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten und auf Null gesetzten SPI in Bytes ein.</p> <p>Der Standardwert ist 32.</p>
<p>Dynamische RADIUS-Authentifizierung</p>	<p>Wählen Sie aus, ob die RADIUS-Authentifizierung über IPsec aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.

Felder im Menü PKI-Verarbeitungsoptionen

Feld	Beschreibung
Zertifikatsanforderungs-Payloads nicht beachten	<p>Wählen Sie aus, ob Zertifikatanforderungen, die während IKE (Phase 1) von der entfernten Seite empfangen wurden, ignoriert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zertifikatsanforderungs-Payloads senden	<p>Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatanforderungen gesendet werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Zertifikatsketten senden	<p>Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.</p>
CRLs senden	<p>Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Key Hash Payloads senden	<p>Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen.</p> <p>Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung. Aktivieren Sie diese Funktion mit <i>Aktiviert</i>, um dieses Verhalten</p>

Feld	Beschreibung
	zu unterdrücken.

16.2 L2TP

Das Layer-2-Tunnelprotokoll (L2TP) ermöglicht das Tunneling von PPP-Verbindungen über eine UDP-Verbindung.

Ihr Teldat-Gerät unterstützt die folgenden zwei Modi:

- L2TP-LNS-Modus (L2TP Network Server): nur für eingehende Verbindungen
- L2TP-LAC-Modus (L2TP Access Concentrator): nur für ausgehende Verbindungen.

Folgendes ist bei der Konfiguration von Server und Client zu beachten: Auf beiden Seiten (LAC und LNS) muss jeweils ein L2TP-Tunnelprofil angelegt werden. Auf der Auslöserseite (LAC) wird das entsprechende L2TP-Tunnelprofil für den Verbindungsaufbau verwendet. Auf der Responderseite (LNS) wird das L2TP-Tunnelprofil für die Verbindungsannahme benötigt.

16.2.1 Tunnelprofile

Im Menü **VPN->L2TP->Tunnelprofile** wird eine Liste aller konfigurierter Tunnelprofile angezeigt.

16.2.1.1 Neu

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

Tunnelprofile Benutzer Optionen

Basisparameter	
Beschreibung	<input type="text" value="L2TP1"/>
Lokaler Hostname	<input type="text"/>
Entfernter Hostname	<input type="text"/>
Passwort	<input type="password" value="••••••••"/>
Parameter des LAC-Modus	
Entfernte IP-Adresse	<input type="text"/>
UDP-Quellport	<input type="checkbox"/> Fest eingestellt
UDP-Zielport	<input type="text" value="1701"/>
Erweiterte Einstellungen	
Lokale IP-Adresse	<input type="text"/>
Hello-Intervall	<input type="text" value="30"/> Sekunden
Minimale Zeit zwischen Versuchen	<input type="text" value="1"/> Sekunden
Maximale Zeit zwischen Versuchen	<input type="text" value="16"/> Sekunden
Maximale Anzahl Wiederholungen	<input type="text" value="5"/>
Sequenznummern der Datenpakete	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 148: VPN->L2TP->Tunnelprofile->Neu

Das Menü VPN->L2TP->Tunnelprofile->Neu besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie eine Beschreibung für das aktuelle Profil ein.</p> <p>Ihr Gerät benennt die Profile automatisch mit <i>L2TP</i> und nummeriert diese, der Wert kann jedoch geändert werden.</p>
Lokaler Hostname	<p>Geben Sie den Hostnamen für LNS bzw. LAC ein.</p> <ul style="list-style-type: none"> <i>LAC</i>: Der lokale Hostname wird in abgehenden Tunnelaufbaumeldungen zur Identifizierung dieses Geräts aufgenommen und wird dem entfernten Hostnamen eines der am LNS konfigurierten Tunnelprofile zugeordnet. Bei diesen Tunnelaufbaumeldungen handelt es sich um die vom LAC ausgesandten SCCRQs (Start Control Connection Request) und die vom LNS ausgesandten SCCRPs (Start Control Connection Reply).

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>LNS</i>: Entspricht dem Wert für Entfernter Hostname der eingehenden Tunnelaufbaumeldung vom LAC.
Entfernter Hostname	<p>Geben Sie den Hostnamen des LNS bzw. LAC ein:</p> <ul style="list-style-type: none"> • <i>LAC</i>: Definiert den Wert für Lokaler Hostname des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRPs). Ein im LAC konfigurierter Lokaler Hostname muss zu Entfernter Hostnamen passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. • <i>LNS</i>: Definiert den Lokaler Hostnamen des LAC. Falls das Feld Entfernter Hostname auf dem LNS leer bleibt, wird das dazugehörige Profil als Standardeintrag qualifiziert, der für alle ankommenden Rufe benutzt wird, für die kein Profil mit passendem entfernten Hostnamen gefunden werden kann.
Passwort	<p>Geben Sie das Passwort ein, welches für die Tunnel-Authentifizierung benutzt wird. Die Authentifizierung zwischen LAC und LNS erfolgt in beiden Richtungen, d. h. der LNS prüft den Lokaler Hostnamen und das Passwort, die in der SCCRQ des LAC enthalten sind und vergleicht sie mit denen, die im relevanten Profil angegeben sind. Der LAC macht das Gleiche mit den jeweiligen Feldern der SCCRP des LNS.</p> <p>Falls dieses Feld leer gelassen wird, werden Authentifizierungsdaten in den Tunnelaufbaumeldungen weder gesandt noch berücksichtigt.</p>

Felder im Menü Parameter des LAC-Modus

Feld	Beschreibung
Entfernte IP-Adresse	<p>Geben Sie die feste IP-Adresse des LNS ein, die als Zieladresse für Verbindungen genutzt wird, die auf diesem Profil aufbauen.</p> <p>Das Ziel muss ein Gerät sein, welches sich wie ein LNS verhalten kann.</p>
UDP-Quellport	<p>Geben Sie an, wie die Portnummer ermittelt werden soll, die als Quellport für alle abgehenden L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.</p> <p>Standardmäßig ist die Option Fest eingestellt deaktiviert, was</p>

Feld	Beschreibung
	<p>bedeutet, dass den Verbindungen, die dieses Profil nutzen, Ports dynamisch zugeordnet werden.</p> <p>Wenn Sie einen fixen Port eingeben möchten, aktivieren Sie die Option <i>Fest eingestellt</i>. Wenn Sie Probleme mit der Firewall bzw. NAT feststellen, wählen Sie diese Option.</p> <p>Verfügbare Werte sind dann 0 bis 65535.</p>
UDP-Zielport	<p>Geben Sie die Zielportnummer ein, die für alle Rufe genutzt wird, die auf diesem Profil aufbauen. Der entfernte LNS, der den Ruf empfängt, muss diesen Port auf L2TP-Verbindungen überwachen.</p> <p>Mögliche Werte sind 0 bis 65535.</p> <p>Der Standardwert ist 1701 (RFC 2661).</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Lokale IP-Adresse	<p>Geben Sie die IP-Adresse ein, die als Quelladresse für alle L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.</p> <p>Falls dieses Feld frei gelassen wird, nutzt Ihr Gerät die IP-Adresse der Schnittstelle, über das der L2TP-Tunnel die entfernte IP-Adresse erreicht.</p>
Hello-Intervall	<p>Geben Sie den Zeitabstand (in Sekunden) zwischen dem Senden von zwei L2TP-HELLO-Meldungen ein. Diese Meldungen dienen dazu, den Tunnel offen zu halten.</p> <p>Verfügbare Werte sind 0 bis 255, der Standardwert ist 30. Der Wert 0 bedeutet, dass keine L2TP-HELLO-Meldungen gesandt werden.</p>
Minimale Zeit zwischen Versuchen	<p>Geben Sie die Mindestzeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat.</p> <p>Die Wartezeit wird dynamisch verlängert, bis sie die Maximale Zeit zwischen Versuchen erreicht hat. Verfügbare Werte sind</p>

Feld	Beschreibung
	1 bis 255, der Standardwert ist 1.
Maximale Zeit zwischen Versuchen	<p>Geben Sie die maximale Zeit (in Sekunden) ein, die Ihr Gerät warten soll, bevor es ein L2TP-Steuerpaket erneut aussendet, auf das es keine Antwort erhalten hat.</p> <p>Verfügbare Werte sind 8 bis 255, der Standardwert ist 16.</p>
Maximale Anzahl Wiederholungen	<p>Geben Sie ein, wie oft Ihr Gerät maximal versuchen soll, das L2TP-Steuerpaket, auf das es keine Antwort erhalten hat, erneut auszusenden.</p> <p>Verfügbare Werte sind 8 bis 255, der Standardwert ist 5.</p>
Sequenznummern der Datenpakete	<p>Wählen Sie aus, ob Ihr Gerät für Datenpakete, die durch einen Tunnel auf Grundlage dieses Profils gesandt werden, Folge-nummern benutzen soll oder nicht.</p> <p>Die Funktion wird derzeit nicht verwendet.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

16.2.2 Benutzer

Im Menü **VPN->L2TP->Benutzer** wird eine Liste aller konfigurierter L2TP-Partner angezeigt.

16.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere L2TP-Partner einzurichten.

Tunnelprofile Benutzer Optionen

Basisparameter							
Beschreibung	<input type="text"/>						
Verbindungstyp	<input checked="" type="radio"/> LNS <input type="radio"/> LAC						
Benutzername	<input type="text"/>						
Passwort	••••••••						
Immer aktiv	<input type="checkbox"/> Aktiviert						
Timeout bei Inaktivität	<input type="text" value="300"/> Sekunden						
IP-Modus und Routen							
IP-Adressmodus	<input checked="" type="radio"/> Statisch <input type="radio"/> IP-Adresse bereitstellen						
Standardroute	<input type="checkbox"/> Aktiviert						
NAT-Eintrag erstellen	<input type="checkbox"/> Aktiviert						
Lokale IP-Adresse	<input type="text"/>						
Routeneinträge	<table border="1"> <thead> <tr> <th>Entfernte IP-Adresse</th> <th>Netzmaske</th> <th>Metrik</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td>1</td> </tr> </tbody> </table> <input type="button" value="Hinzufügen"/>	Entfernte IP-Adresse	Netzmaske	Metrik	<input type="text"/>	<input type="text"/>	1
Entfernte IP-Adresse	Netzmaske	Metrik					
<input type="text"/>	<input type="text"/>	1					
Erweiterte Einstellungen							
Blockieren nach Verbindungsfehler für	<input type="text" value="300"/> Sekunden						
Authentifizierung	MS-CHAPv2						
Verschlüsselung	<input type="radio"/> Keine <input checked="" type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel						
Komprimierung	<input checked="" type="radio"/> Keine <input type="radio"/> STAC <input type="radio"/> MS-STAC <input type="radio"/> MPPC						
LCP-Erreichbarkeitsprüfung	<input checked="" type="checkbox"/> Aktiviert						
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert						
IP-Optionen							
OSPF-Modus	<input checked="" type="radio"/> Passiv <input type="radio"/> Aktiv <input type="radio"/> Inaktiv						
Proxy-ARP-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv						
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert						
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>							

Abb. 149: VPN->L2TP->Benutzer->Neu

Das Menü VPN->L2TP->Benutzer->Neu besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	<p>Geben Sie einen beliebigen Namen ein, um den L2TP-Partner eindeutig zu benennen.</p> <p>In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.</p>

Feld	Beschreibung
	Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.
Verbindungstyp	<p>Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerkserver (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LNS</i> (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • <i>LAC</i>: Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.
Tunnelprofil	<p>Nur für Verbindungstyp = <i>LAC</i></p> <p>Wählen Sie ein im Menü Tunnelprofil erstelltes Profil für die Verbindung zu diesem L2TP-Partner aus.</p>
Benutzername	Geben Sie die Kennung Ihres Geräts ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv deaktiviert ist</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wie viele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Zur Verfügung stehen Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Short Hold. Der Standardwert ist 300.</p>

Felder im Menü IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	<p>Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine statische IP-Adresse ein. • <i>IP-Adresse bereitstellen</i>: Nur für Verbindungstyp = <i>LNS</i>. Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Nur für Verbindungstyp = <i>LAC</i>. Ihr Gerät erhält dynamisch eine IP-Adresse.
IP-Zuordnungspool (IPCP)	<p>Nur für IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>Wählen Sie einen im Menü WAN->Internet + Einwählen->IP Pools konfigurierten IP Pool aus.</p>
Standardroute	<p>Nur für IP-Adressmodus = <i>IP-Adresse abrufen</i> und <i>Statisch</i></p> <p>Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv .</p>
NAT-Eintrag erstellen	<p>Nur für IP-Adressmodus = <i>IP-Adresse abrufen</i> und <i>Statisch</i></p> <p>Wählen Sie aus, ob Network Address Translation (NAT) für diese Verbindung aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die WAN-IP-Adresse Ihres Geräts ein.</p>
Routeneinträge	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie Entfernte IP-Adresse und Netzmaske des LANs</p>

Feld	Beschreibung
	des L2TP-Partners und die dazugehörige Metrik ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach einem fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Der Standardwert ist <i>300</i>.</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP/CHAP/MS-CHAP</i> (Standardwert): Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>PAP</i>: Nur PAP (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur CHAP (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen. • <i>Keine</i>: Einige Provider verwenden keine Authentifizierung. Wählen Sie in dem Fall diese Option.
Verschlüsselung	<p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiviert ist. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i>: Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i> (Standardwert): Die MPP-Verschlüsselung V2 mit 128 Bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 Bit wird kompatibel zu Microsoft und Cisco angewendet.
Komprimierung	<p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Wenn Verschlüsselung gesetzt ist, muss es die Gegenstelle ebenfalls unterstützen, sonst kommt keine Verbindung zustande.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Es wird keine Verschlüsselung angewendet. • <i>STAC</i> • <i>MS-STAC</i> • <i>MPPC</i>: Microsoft Point-to-Point Compression
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü IP-Optionen

Feld	Beschreibung
OSPF-Modus	Wählen Sie aus, ob und wie über die Schnittstellerouten propa-

Feld	Beschreibung
	<p>giert und/oder OSPF-Protokoll-Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing-Informationen berücksichtigt und über aktive Schnittstellen propagiert. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen L2TP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen L2TP-Partner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>aktiv</i> (aktiv) oder <i>ruhend</i> (ruhend) ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum L2TP-Partner <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum L2TP-Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server und WINS-Server Primär und Sekundär vom L2TP-Partner erhalten soll oder diese zum L2TP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

16.2.3 Optionen

Abb. 150: VPN->L2TP->Optionen

Das Menü **VPN->L2TP->Optionen** besteht aus folgenden Feldern:

Felder im Menü Globale Optionen

Feld	Beschreibung
UDP-Zielport	<p>Geben Sie den Port ein, der vom LNS auf ankommende L2TP-Tunnelverbindungen überwacht werden soll.</p> <p>Verfügbare Werte sind alle ganzen Zahlen von 1 bis 65535, der Standardwert ist 1701, wie es in RFC 2661 vorgegeben ist.</p>
UDP-Quellportauswahl	<p>Wählen Sie aus, ob der LNS nur den überwachten Port (UDP-Zielport) als lokalen Quellport für die L2TP-Verbindung nutzen soll.</p> <p>Mit <i>Fest eingestellt</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

16.3 GRE

Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, das dazu dient, andere Protokolle einzukapseln und so in Form von IP-Tunneln zu den spezifizierten Empfänger zu transportieren.

Die Spezifikation des GRE-Protokolls liegt in zwei Versionen vor:

- GRE V.1 zur Verwendung in PPTP-Verbindungen (RFC 2637, Konfiguration im Menü **PPTP**)
- GRE V.0 (RFC 2784) zur allgemeinen Enkapsulierung mittels GRE

Im diesem Menü können Sie ein virtuelles Interface zur Nutzung von GRE V.0 konfigurieren. Der Datenverkehr, der über dieses Interface geroutet wird, wird dann mittels GRE enkapsuliert und an den spezifizierten Empfänger gesendet.

16.3.1 GRE-Tunnel

Im Menü **VPN->GRE->GRE-Tunnel** wird eine Liste aller konfigurierten GRE-Tunnel angezeigt.

16.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere GRE-Tunnel einzurichten.

GRE-Tunnel

Basisparameter													
Beschreibung	<input type="text"/>												
Lokale GRE-IP-Adresse	<input type="text"/>												
Entfernte GRE-IP-Adresse	<input type="text"/>												
Standardroute	<input type="checkbox"/> Aktiviert												
Lokale IP-Adresse	<input type="text"/>												
Routeneinträge	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Entfernte IP-Adresse</th> <th style="width: 30%;">Netzmaske</th> <th style="width: 10%;">Metrik</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td style="text-align: center;">1</td> <td style="text-align: center;">▼</td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Hinzufügen"/></td> </tr> </tbody> </table>	Entfernte IP-Adresse	Netzmaske	Metrik		<input type="text"/>	<input type="text"/>	1	▼	<input type="button" value="Hinzufügen"/>			
Entfernte IP-Adresse	Netzmaske	Metrik											
<input type="text"/>	<input type="text"/>	1	▼										
<input type="button" value="Hinzufügen"/>													
MTU	<input type="text" value="1500"/>												
Schlüssel verwenden	<input type="checkbox"/> Aktiviert												

Abb. 151: VPN->GRE->GRE-Tunnel->Neu

Das Menü **VPN->GRE->GRE-Tunnel->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	<p>Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein.</p> <p>Wird keine IP-Adresse (dies entspricht der IP-Adresse 0.0.0.0) angegeben, wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt,</p>

Feld	Beschreibung
	über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse der GRE-Pakete zum GRE-Partner ein.
Standardroute	<p>Wenn Sie die Standardroute aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	Geben Sie hier die (LAN-seitige) IP-Adresse ein, die als Quelladresse Ihre Gerätes für eigene Pakete durch den GRE-Tunnel verwendet werden soll.
Routeneinträge	<p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standard-Netzmaske. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0... 15). Der Standardwert ist 1.
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf.</p> <p>Mögliche Werte sind 1 bis 8192.</p> <p>Der Standardwert ist 1500.</p>
Schlüssel verwenden	<p>Aktivieren Sie die Eingabe einer Kennung für die GRE-Verbindung, welche die Unterscheidung mehrerer parallel laufender GRE-Verbindungen zwischen zwei GRE-Partnern ermöglicht (siehe RFC 1701).</p> <p>Mit <i>Aktiviert</i> wird die Kennung aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
Schlüsselwert	<p>Nur wenn Schlüssel verwenden aktiviert ist.</p> <p>Geben Sie die GRE-Verbindungsnummer ein.</p> <p>Mögliche Werte sind 0 bis 2147483647.</p> <p>Der Standardwert ist 0.</p>

Kapitel 17 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen Teldat Gateways über eine leistungsfähige Sicherheitsfunktion.

Zusätzlich zur sogenannten statischen Paketfilterung hat eine SIF durch dynamische Paketfilterung einen entscheidenden Vorteil: Die Entscheidung, ob ein Paket weitergeleitet wird, kann nicht nur aufgrund von Quell- und Zieladressen oder Ports, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung zu einem Partner gefällt werden.

Es können also auch solche Pakete weitergeleitet werden, die zu einer bereits aktiven Verbindung gehören. Dabei akzeptiert die SIF auch Pakete, die zu einer "Tochterverbindung" gehören. Die Aushandlung einer FTP-Verbindung findet zum Beispiel über den Port 21 statt, der eigentliche Datenaustausch kann aber über einen völlig anderen Port erfolgen.

SIF und andere Sicherheitsfunktionen

Die Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der Teldat-Geräte ein. Systemen wie Network Address Translation (NAT) und IP-Zugriffs-Listen (IPAL) gegenüber ist der Konfigurationsaufwand der SIF vergleichbar einfach.

Da SIF, NAT und IPAL gleichzeitig im System aktiv sind, muss man auf mögliche Wechselwirkungen achten: Wenn ein beliebiges Paket von einer der Sicherheitsinstanzen verworfen wird, so geschieht dies unmittelbar, d. h. es ist irrelevant, ob es von einer anderen Instanz zugelassen werden würde. Daher sollte man den eigenen Bedarf an Sicherheitsfunktionen genau analysieren.

Der wesentliche Unterschied zwischen SIF und NAT/IPAL besteht darin, dass die Regeln der SIF generell global angewendet werden, d. h. nicht auf eine Schnittstelle beschränkt sind.

Grundsätzlich werden aber dieselben Filterkriterien auf den Datenverkehr angewendet wie bei NAT und IPAL:

- Quell- und Zieladresse des Pakets (mit einer zugehörigen Netzmaske)
- Dienst (vorkonfiguriert, z. B. Echo, FTP, HTTP)
- Protokoll
- Portnummer(n)

Um die Unterschiede in der Paketfilterung zu verdeutlichen, folgt eine Aufstellung der ein-

zelen Sicherheitsinstanzen und ihrer Funktionsweise.

NAT

Eine der Grundfunktionen von NAT ist die Umsetzung lokaler IP-Adressen Ihres LANs in die globalen IP-Adressen, die Ihnen von Ihrem ISP zugewiesen werden, und umgekehrt. Dabei werden zunächst alle von außen initiierten Verbindungen abgeblockt, d. h. jedes Paket, welches Ihr Gerät nicht einer bereits bestehenden Verbindung zuordnen kann, wird abgewiesen. Auf diese Art kann eine Verbindung lediglich von innen nach außen aufgebaut werden. Ohne explizite Genehmigungen wehrt NAT jeden Zugriff aus dem WAN auf das LAN ab.

IP Access Listen

Hier werden Pakete ausschließlich aufgrund der oben aufgeführten Kriterien zugelassen oder abgewiesen, d. h. der Zustand der Verbindung wird nicht berücksichtigt (außer bei **Dienste** = *TCP*).

SIF

Die SIF sondert alle Pakete aus, die nicht explizit oder implizit zugelassen werden. Dabei gibt es sowohl ein "Verweigern", bei dem keine Fehlermeldung an den Sender des zurückgewiesenen Pakets ausgegeben wird, als auch ein "Ablehnen", bei dem der Sender über die Ablehnung des Pakets informiert wird.

Die eingehenden Pakete werden folgendermaßen bearbeitet:

- Zunächst überprüft die SIF, ob ein eingehendes Paket einer bereits bestehenden Verbindung zugeordnet werden kann. Ist dies der Fall, wird es weitergeleitet. Kann das Paket keiner bestehenden Verbindung zugeordnet werden, wird überprüft, ob eine entsprechende Verbindung zu erwarten ist (z. B. als Tochterverbindung einer bereits bestehenden). Ist dies der Fall, wird das Paket ebenfalls akzeptiert.
- Wenn das Paket keiner bestehenden und auch keiner zu erwartenden Verbindung zugeordnet werden kann, werden die SIF-Filterregeln angewendet: Trifft auf das Paket eine Deny-Regel zu, wird es abgewiesen, ohne dass eine Fehlermeldung an den Sender des Pakets geschickt wird; trifft eine Reject-Regel zu, wird das Paket abgewiesen und eine ICMPHost-Unreachable-Meldung an den Sender des Paktes ausgegeben. Nur wenn auf das Paket eine Accept-Regel zutrifft, wird es weitergeleitet.
- Alle Pakete, auf die keine Regel zutrifft, werden nach Kontrolle aller vorhandenen Regeln ohne Fehlermeldung an den Sender abgewiesen (= Standardverhalten).

17.1 Richtlinien

17.1.1 Filterregeln


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


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

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



Abb. 152: **Firewall->Richtlinien->Filterregeln**

Mit der Schaltfläche  können Sie vor dem Listeneintrag eine weitere Richtlinie einfügen. Es öffnet sich das Konfigurationsmenü zum Erstellen einer neuen Richtlinie.

Mit der Schaltfläche  können Sie den Listeneintrag verschieben. Es öffnet sich ein Dialog, in dem Sie auswählen können, an welche Position die Richtlinie verschoben werden soll.

17.1.1.1 Neu

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

Filterregeln QoS Optionen

Basisparameter	
Quelle	— INTERFACE ALIASES —
Ziel	— INTERFACE ALIASES —
Dienst	— SERVICES —
Aktion	Zugriff
QoS anwenden	<input type="checkbox"/> Aktiviert

OK Abbrechen

Abb. 153: Firewall->Richtlinien->Filterregeln->Neu

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

Felder im Menü Basisparameter

Feld	Beschreibung
Quelle	<p>Wählen Sie einen der vorkonfigurierten Aliase für die Quelle des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Quell-Schnittstelle noch Quell-Adresse überprüft werden.</p>
Ziel	<p>Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall->Schnittstellen->Gruppen), Adressen (siehe Firewall->Adressen->Adressliste) und Adressgruppen (siehe Firewall->Adressen->Gruppen) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfi-</p>

Feld	Beschreibung
	<p>guriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>ftp</i> • <i>telnet</i> • <i>smtp</i> • <i>dns</i> • <i>http</i> • <i>nntp</i> • <i>Internet</i> • <i>Netmeeting</i> <p>Weitere Dienste werden in Firewall->Dienste->Diensteliste angelegt.</p> <p>Außerdem stehen die in Firewall->Dienste->Gruppen konfigurierten Dienstegruppen zur Auswahl.</p>
Aktion	<p>Wählen Sie die Aktion aus, die auf ein gefiltertes Paket angewendet werden soll.</p> <p>Möglichen Werte:</p> <ul style="list-style-type: none"> • <i>Zugriff</i> (Standardwert): Die Pakete werden entsprechend den Angaben weitergeleitet. • <i>Verweigern</i>: Die Pakete werden abgewiesen. • <i>Zurückweisen</i>: Die Pakete werden abgewiesen. Eine Fehlermeldung wird an den Sender des Pakets ausgegeben.
QoS anwenden	<p>Nur für Aktion = <i>Zugriff</i></p> <p>Wählen Sie aus, ob Sie QoS für diese Richtlinie mit der in Priorität ausgewählten Priorität aktivieren möchten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Option nicht aktiv.</p> <p>Wenn QoS für diese Richtlinie nicht aktiv ist, beachten Sie, dass auch sendeseitig keine Priorisierung der Daten erfolgen kann.</p> <p>Eine Richtlinie, für die QoS aktiviert wurde, ist auch für die Firewall eingestellt. Beachten Sie daher, dass Datenverkehr, der</p>

Feld	Beschreibung
	nicht ausdrücklich zugelassen wurde, von der Firewall geblockt wird!
Priorität	<p>Nur für QoS anwenden = <i>Aktiviert</i></p> <p>Wählen Sie aus, mit welcher Priorität die von der Richtlinie spezifizierten Daten sendeseitig behandelt werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Keine Priorität. • <i>Low Latency</i>: Low Latency Transmission (LLT), d. h. Behandlung der Daten mit der geringstmöglichen Latenz, z. B. geeignet für VoIP-Daten. • <i>Hoch</i> • <i>Mittel</i> • <i>Niedrig</i>

17.1.2 QoS

Immer mehr Anwendungen benötigen immer größere Bandbreiten. Nicht immer stehen diese zur Verfügung. Quality of Service (QoS) ermöglicht es, verfügbare Bandbreiten effektiv und intelligent zu verteilen. Bestimmte Anwendungen können bevorzugt behandelt werden und es kann Bandbreite für diese reserviert werden.

Im Menü **Firewall->Richtlinien->QoS** wird eine Liste aller QoS-Regeln angezeigt.

17.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere QoS-Regeln einzurichten.

Filterregeln QoS Optionen

QoS-Schnittstelle konfigurieren

Schnittstelle	Eine auswählen ▾
Traffic Shaping	<input type="checkbox"/> Aktiviert
Filterregeln	Quelle Ziel Dienst Priorität Verwenden Bandbreite (Bit/s) Fest

OK Abbrechen

Abb. 154: **Firewall->Richtlinien->QoS->Neu**

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

Felder im Menü QoS-Schnittstelle konfigurieren

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der das Bandbreitenmanagement erfolgen soll.
Traffic Shaping	<p>Wählen Sie aus, ob Sie für die gewählte Schnittstelle das Bandbreitenmanagement aktivieren wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Bandbreite angeben	<p>Nur für Traffic Shaping = <i>Aktiviert</i></p> <p>Geben Sie die maximal zur Verfügung stehende Bandbreite in kBit/s für die gewählte Schnittstelle ein.</p>
Filterregeln	<p>Dieses Feld enthält eine Liste aller konfigurierten Firewall-Richtlinien, für die QoS aktiviert wurde (QoS anwenden = <i>Aktiviert</i>). Für jeden Listeneintrag stehen folgende Optionen zur Verfügung:</p> <ul style="list-style-type: none"> • Verwenden: Wählen Sie aus, ob dieser Eintrag der QoS-Schnittstelle zugeordnet werden soll. Standardmäßig ist diese Option nicht aktiv. • Bandbreite: Geben Sie die maximal zur Verfügung stehende Bandbreite in Bit/s für den unter Dienst genannten Dienst ein. Standardmäßig ist 0 eingetragen. • Fest: Wählen Sie aus, ob eine längerfristige Überschreitung der in Bandbreite definierten Bandbreite zulässig ist. Die Aktivierung dieses Feldes schließt eine solche Überschreitung aus. Ist die Option deaktiviert, ist die Überschreitung zulässig und die übersteigende Datenrate wird gemäß der in der entsprechenden Firewall-Richtlinie definierten Priorität behandelt. Standardmäßig ist diese Option nicht aktiv.

17.1.3 Optionen

In diesem Menü können Sie die Firewall aus- bzw. einschalten und Sie können ihre Aktivitäten protokollieren lassen. Darüber hinaus können Sie festlegen, nach wie vielen Sekunden Inaktivität eine Sitzung beendet werden soll.

Filterregeln OoS **Optionen**

Globale Firewall-Optionen	
Firewall Status	<input checked="" type="checkbox"/> Aktiviert
Protokollierte Aktionen	Alle <input type="button" value="v"/>
Vollständige Filterung	<input checked="" type="checkbox"/> Aktivieren
Sitzungstimer	
UDP-Inaktivität	180 <input type="text"/> Sekunden
TCP-Inaktivität	3600 <input type="text"/> Sekunden
PPTP-Inaktivität	86400 <input type="text"/> Sekunden
Andere Inaktivität	30 <input type="text"/> Sekunden

Abb. 155: Firewall->Richtlinien->Optionen

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

Felder im Menü Globale Firewall-Optionen

Feld	Beschreibung
Firewall Status	<p>Aktivieren oder deaktivieren Sie die Firewall-Funktion.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiviert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Protokollierte Aktionen	<p>Wählen Sie den Firewall-Syslog-Level aus.</p> <p>Die Ausgabe der Meldungen erfolgt zusammen mit den Meldungen der anderen Subsysteme.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Alle Firewall-Aktivitäten werden angezeigt. • <i>Verweigern</i>: Nur Reject- und Deny-Ereignisse werden angezeigt, vgl. "Aktion".

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Annehmen</i>: Nur Accept-Ereignisse werden angezeigt. • <i>Keine</i>: Systemprotokoll-Nachrichten werden nicht erzeugt.
Vollständige Filterung	<p>Hier legen Sie fest, ob nur Pakete gefiltert werden sollen, die an eine andere Schnittstelle gesendet werden als die, welche die Verbindung erzeugt hat.</p> <p>Mit <i>Aktivieren</i> werden alle Pakete gefiltert (Standardwert).</p>

Felder im Menü Sitzungstimer

Feld	Beschreibung
UDP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine UDP - Session als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i>.</p> <p>Der Standardwert ist <i>180</i>.</p>
TCP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine TCP - Session als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i>.</p> <p>Der Standardwert ist <i>3600</i>.</p>
PPTP-Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine PPTP-Session als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i>.</p> <p>Der Standardwert ist <i>86400</i>.</p>
Andere Inaktivität	<p>Geben Sie ein, nach welcher Zeit der Inaktivität eine Session eines anderen Typs als abgelaufen betrachtet werden soll (in Sekunden).</p> <p>Zur Verfügung stehen Werte von <i>30</i> bis <i>86400</i>.</p> <p>Der Standardwert ist <i>30</i>.</p>

17.2 Schnittstellen

17.2.1 Gruppen

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

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

17.2.1.1 Neu

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

Basisparameter									
Beschreibung	<input type="text"/>								
Mitglieder	<table border="1"> <thead> <tr> <th>Schnittstelle</th> <th>Auswahl</th> </tr> </thead> <tbody> <tr> <td>LOCAL</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-4</td> <td><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-0</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Schnittstelle	Auswahl	LOCAL	<input type="checkbox"/>	LAN_EN1-4	<input type="checkbox"/>	LAN_EN1-0	<input type="checkbox"/>
Schnittstelle	Auswahl								
LOCAL	<input type="checkbox"/>								
LAN_EN1-4	<input type="checkbox"/>								
LAN_EN1-0	<input type="checkbox"/>								
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>									

Abb. 156: **Firewall->Schnittstellen->Gruppen->Neu**

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

Felder im Menü Basisparameter

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

17.3 Adressen

17.3.1 Adressliste

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

17.3.1.1 Neu

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

Abb. 157: **Firewall->Adressen->Adressliste->Neu**

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

Felder im Menü Basisparameter

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

Feld	Beschreibung
Adressbereich	Nur für Adresstyp = <i>Adressbereich</i> Geben Sie die Anfangs-und End-IP-Adresse des Bereiches ein.

17.3.2 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.

17.3.2.1 Neu

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

Basisparameter					
Beschreibung	<input type="text"/>				
Auswahl	<table border="1"> <thead> <tr> <th>Adressen</th> <th>Auswahl</th> </tr> </thead> <tbody> <tr> <td>ANY</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Adressen	Auswahl	ANY	<input type="checkbox"/>
Adressen	Auswahl				
ANY	<input type="checkbox"/>				

Abb. 158: **Firewall->Adressen->Gruppen->Neu**

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

Felder im Menü Basisparameter

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

17.4 Dienste

17.4.1 Diensteliste

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

17.4.1.1 Neu

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

Abb. 159: **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 1 bis 65535.</p>

Feld	Beschreibung
Quellportbereich	<p>Nur für Protokoll = <i>TCP, UDP/TCP</i> oder <i>UDP</i></p> <p>Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port an.</p> <p>Soll ein Portnummernbereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Portbereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Das Feld Typ gibt die Klasse der ICMP-Nachrichten an, das Feld Code spezifiziert die Art der Nachricht genauer.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig (Standardwert)</i> • <i>Echo Reply</i> • <i>Destination Unreachable</i> • <i>Source Quench</i> • <i>Redirect</i> • <i>Echo</i> • <i>Time Exceeded</i> • <i>Parameter Problem</i> • <i>Timestamp</i> • <i>Timestamp Reply</i> • <i>Information Request</i> • <i>Information Reply</i> • <i>Address Mask Request</i> • <i>Address Mask Reply</i>
Code	<p>Nur für Typ = <i>Destination Unreachable</i> stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none">• <i>Beliebig (Standardwert)</i>• <i>Net Unreachable</i>• <i>Host Unreachable</i>• <i>Protocol Unreachable</i>• <i>Port Unreachable</i>• <i>Fragmentation Needed</i>• <i>Communication with Destination Network is Administratively Prohibited</i>• <i>Communication with Destination Host is Administratively Prohibited</i>

17.4.2 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.

17.4.2.1 Neu

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

Diensteliste Gruppen

Basisparameter																																															
Beschreibung	<input style="width: 95%;" type="text"/>																																														
Mitglieder	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #e0e0e0;"> <th style="text-align: left; padding: 2px;">Dienst</th> <th style="text-align: left; padding: 2px;">Auswahl</th> </tr> </thead> <tbody> <tr><td>activity</td><td><input type="checkbox"/></td></tr> <tr><td>any</td><td><input type="checkbox"/></td></tr> <tr><td>apple-qt</td><td><input type="checkbox"/></td></tr> <tr><td>auth</td><td><input type="checkbox"/></td></tr> <tr><td>chargen</td><td><input type="checkbox"/></td></tr> <tr><td>clients_1</td><td><input type="checkbox"/></td></tr> <tr><td>clients_2</td><td><input type="checkbox"/></td></tr> <tr><td>daytime</td><td><input type="checkbox"/></td></tr> <tr><td>dhcp</td><td><input type="checkbox"/></td></tr> <tr><td>discard</td><td><input type="checkbox"/></td></tr> <tr><td>dns</td><td><input type="checkbox"/></td></tr> <tr><td>echo</td><td><input type="checkbox"/></td></tr> <tr><td>exec</td><td><input type="checkbox"/></td></tr> <tr><td>finger</td><td><input type="checkbox"/></td></tr> <tr><td>ftp</td><td><input type="checkbox"/></td></tr> <tr><td>unpriv</td><td><input type="checkbox"/></td></tr> <tr><td>ups</td><td><input type="checkbox"/></td></tr> <tr><td>uucp-path</td><td><input type="checkbox"/></td></tr> <tr><td>who</td><td><input type="checkbox"/></td></tr> <tr><td>whois</td><td><input type="checkbox"/></td></tr> <tr><td>wins</td><td><input type="checkbox"/></td></tr> <tr><td>x400</td><td><input type="checkbox"/></td></tr> </tbody> </table>	Dienst	Auswahl	activity	<input type="checkbox"/>	any	<input type="checkbox"/>	apple-qt	<input type="checkbox"/>	auth	<input type="checkbox"/>	chargen	<input type="checkbox"/>	clients_1	<input type="checkbox"/>	clients_2	<input type="checkbox"/>	daytime	<input type="checkbox"/>	dhcp	<input type="checkbox"/>	discard	<input type="checkbox"/>	dns	<input type="checkbox"/>	echo	<input type="checkbox"/>	exec	<input type="checkbox"/>	finger	<input type="checkbox"/>	ftp	<input type="checkbox"/>	unpriv	<input type="checkbox"/>	ups	<input type="checkbox"/>	uucp-path	<input type="checkbox"/>	who	<input type="checkbox"/>	whois	<input type="checkbox"/>	wins	<input type="checkbox"/>	x400	<input type="checkbox"/>
Dienst	Auswahl																																														
activity	<input type="checkbox"/>																																														
any	<input type="checkbox"/>																																														
apple-qt	<input type="checkbox"/>																																														
auth	<input type="checkbox"/>																																														
chargen	<input type="checkbox"/>																																														
clients_1	<input type="checkbox"/>																																														
clients_2	<input type="checkbox"/>																																														
daytime	<input type="checkbox"/>																																														
dhcp	<input type="checkbox"/>																																														
discard	<input type="checkbox"/>																																														
dns	<input type="checkbox"/>																																														
echo	<input type="checkbox"/>																																														
exec	<input type="checkbox"/>																																														
finger	<input type="checkbox"/>																																														
ftp	<input type="checkbox"/>																																														
unpriv	<input type="checkbox"/>																																														
ups	<input type="checkbox"/>																																														
uucp-path	<input type="checkbox"/>																																														
who	<input type="checkbox"/>																																														
whois	<input type="checkbox"/>																																														
wins	<input type="checkbox"/>																																														
x400	<input type="checkbox"/>																																														
OK Abbrechen																																															

Abb. 160: Firewall->Dienste->Gruppen->Neu

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

Felder im Menü Basisparameter

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

Kapitel 18 Lokale Dienste

Dieses Menü stellt Ihnen Dienste zu folgenden Themenkreisen zur Verfügung:

- Namensauflösung (DNS)
- Konfiguration über einen Web-Browser (HTTPS)
- Auffinden dynamischer IP-Adressen mit Hilfe eines DynDNS-Providers
- Konfiguration des Gateways als DHCP-Server (Vergabe von IP-Adressen)
- Automatisieren von Aufgaben nach einem Zeitplan (Scheduling)
- Erreichbarkeitsprüfungen von Hosts oder Schnittstellen, Ping-Test
- Automatische Erkennung und Konfiguration von Teldat-Geräten
- Bereitstellung öffentlicher Internetzugänge (Hotspot).

18.1 DNS

Jedes Gerät in einem TCP/IP-Netz wird normalerweise durch seine IP-Adresse angesprochen. Da in Netzwerken oft Host-Namen benutzt werden, um verschiedene Geräte anzusprechen, muss die zugehörige IP-Adresse bekanntgegeben werden. Diese Aufgabe übernimmt z. B. ein DNS-Server. Er löst die Host-Namen in IP-Adressen auf. Eine Namensauflösung kann alternativ auch über die sogenannte HOSTS-Datei erfolgen, die auf jedem Rechner zur Verfügung steht.

Ihr Gerät bietet zur Namensauflösung folgende Möglichkeiten:

- DNS-Proxy, um DNS-Anfragen, die an Ihr Gerät gestellt werden, an einen geeigneten DNS-Server weiterzuleiten. Dieses schließt auch spezifisches Forwarding definierter Domains (Domänenweiterleitung) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Statische Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring (Statistik), um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Name-Server

Unter **Lokale Dienste->DNS->Globale Einstellungen->Basisparameter** werden die IP-Adressen von Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen

nicht selbst oder durch Forwarding-Einträge beantworten kann. Es können sowohl globale Name-Server eingetragen werden als auch Name-Server, die an eine Schnittstelle gebunden sind.

Die Adressen der globalen Name-Server kann Ihr Gerät auch dynamisch via PPP oder DHCP erhalten bzw. diese ggf. übermitteln.

Strategie zur Namensauflösung auf Ihrem Gerät

Eine DNS-Anfrage wird von Ihrem Gerät folgendermaßen behandelt:

- (1) Falls möglich, wird die Anfrage aus dem statischen oder dynamischen Cache direkt mit IP-Adresse oder negativer Antwort beantwortet.
- (2) Ansonsten wird, falls ein passender Forwarding-Eintrag vorhanden ist, der entsprechende DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (3) Ansonsten werden, falls Name-Server eingetragen sind, unter Berücksichtigung der konfigurierten Priorität und wenn der entsprechenden Schnittstellenstatus "up" ist, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (4) Ansonsten werden, falls eine Internet- oder Einwählverbindung als Standard-Schnittstelle ausgewählt ist, die dazugehörigen DNS-Server befragt, je nach Konfiguration von Internet- oder Einwählverbindungen ggf. unter Aufbau einer kostenpflichtigen WAN-Verbindung. Falls einer der DNS-Server den Namen auflösen kann, wird die Information weitergeleitet und ein dynamischer Eintrag im Cache erzeugt.
- (5) Ansonsten wird, falls im Menü **WAN->Internet + Einwählen** ein Eintrag angelegt wurde und das Überschreiben der Adressen der globalen Name-Server zulässig ist (**Schnittstellenmodus = Dynamisch**), eine Verbindung zur ersten Internet- bzw. Einwählverbindung ggf. kostenpflichtig aufgebaut, die so konfiguriert ist, dass DNS-Server-Adressen von DNS-Servern angefordert werden können (**DNS-Aushandlung = Aktiviert**) - soweit dies vorher noch nicht versucht wurde. Bei erfolgreicher Name-Server-Aushandlung stehen diese Name-Server somit für weitere Anfragen zur Verfügung.
- (6) Ansonsten wird die initiale Anfrage mit Serverfehler beantwortet.

Wenn einer der DNS-Server mit `non-existent domain` antwortet, wird die initiale Anfrage sofort dementsprechend beantwortet und ein entsprechender Negativ-Eintrag in den DNS-Cache Ihres Geräts aufgenommen.

18.1.1 Globale Einstellungen

Globale Einstellungen		DNS-Server	Statische Hosts	Domänenweiterleitung	Cache	Statistik
Basisparameter						
Domänenname	<input type="text"/>					
WINS-Server	Primär	<input type="text" value="0.0.0.0"/>				
	Sekundär	<input type="text" value="0.0.0.0"/>				
Erweiterte Einstellungen						
Positiver Cache	<input checked="" type="checkbox"/> Aktiviert					
Negativer Cache	<input checked="" type="checkbox"/> Aktiviert					
Cache-Größe	<input type="text" value="100"/>		Einträge			
Maximale TTL für positive Cacheeinträge	<input type="text" value="86400"/>		Sekunden			
Maximale TTL für negative Cacheeinträge	<input type="text" value="300"/>		Sekunden			
Alternative Schnittstelle, um DNS-Server zu erhalten	<input type="text" value="Automatisch"/> <input type="button" value="v"/>					
Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse						
Als DHCP-Server	<input type="radio"/> Keine <input checked="" type="radio"/> Eigene IP-Adresse <input type="radio"/> DNS-Einstellung					
Als IPCP-Server	<input type="radio"/> Keine <input type="radio"/> Eigene IP-Adresse <input checked="" type="radio"/> DNS-Einstellung					
<input type="button" value="OK"/>		<input type="button" value="Abbrechen"/>				

Abb. 161: 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	Wählen Sie aus, ob der positive dynamische Cache aktiviert

Feld	Beschreibung
	<p>werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Negativer Cache	<p>Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Cache-Größe	<p>Geben Sie die maximale Gesamtzahl der statischen und dynamischen Einträge ein.</p> <p>Wird dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird Cache-Größe vom Benutzer heruntersgesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. Cache-Größe kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden.</p> <p>Mögliche Werte: <i>0.. 1000</i>.</p> <p>Standardwert ist <i>100</i>.</p>
Maximale TTL für positive Cacheeinträge	<p>Geben Sie den Wert ein, auf den die TTL für einen positiven dynamischen DNS-Eintrag im Cache gesetzt werden soll, wenn dessen TTL <i>0</i> ist oder dessen TTL den Wert für Maximale TTL für positive Cacheeinträge überschreitet.</p> <p>Standardwert ist <i>86400</i>.</p>
Maximale TTL für negative Cacheeinträge	<p>Geben Sie den Wert ein, auf den die TTL bei einem negativen dynamischen Eintrag im Cache gesetzt werden soll.</p> <p>Standardwert ist <i>86400</i>.</p>
Alternative Schnittstel-	<p>Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur</p>

Feld	Beschreibung
le, um DNS-Server zu erhalten	<p>Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.</p> <p>Standardwert ist <i>Automatisch</i>, d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.</p>


Felder im Menü Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse

Feld	Beschreibung
Als DHCP-Server	<p>Wählen Sie aus, welche Name-Server-Adressen dem DHCP-Client übermittelt werden, wenn Ihr Gerät als DHCP-Server genutzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i>: Es wird keine Name-Server-Adresse übermittelt. • <i>Eigene IP-Adresse</i> (Standardwert): Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • <i>DNS-Einstellung</i>: Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.
Als IPCP-Server	<p>Wählen Sie aus, welche Name-Server-Adressen von Ihrem Gerät bei einer dynamischen Name-Server-Aushandlung übermittelt werden, wenn Ihr Gerät als IPCP-Server für PPP-Verbindungen genutzt wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i>: Es wird keine Name-Server-Adresse übermittelt. • <i>Eigene IP-Adresse</i>: Es wird die Adresse Ihres Geräts als Name-Server-Adresse übermittelt. • <i>DNS-Einstellung</i> (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

18.1.2 DNS-Server

Im Menü **Lokale Dienste->DNS->DNS-Server** wird eine Liste aller konfigurierten DNS-Server angezeigt.

18.1.2.1 Bearbeiten oder Neu

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

Sie können hier sowohl globale DNS-Server konfigurieren als auch DNS-Server, die einer bestimmten Schnittstelle zugewiesen werden sollen.

Einen DNS-Server für eine bestimmte Schnittstelle zu konfigurieren ist zum Beispiel nützlich, wenn Accounts zu verschiedenen Providern über unterschiedliche Schnittstellen eingerichtet sind und Lastverteilung verwendet wird.

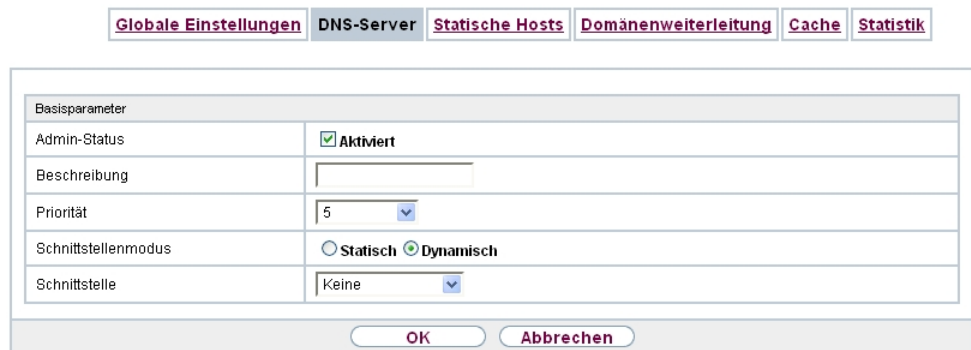


Abb. 162: Lokale Dienste->DNS->DNS-Server->Neu

Das Menü **Lokale Dienste->DNS->DNS-Server->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Admin-Status	Wählen Sie aus, ob der DNS-Server aktiv sein soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Beschreibung	Geben Sie eine Beschreibung für den DNS-Server ein.
Priorität	Weisen Sie dem DNS-Server eine Priorität zu. Sie können einer Schnittstelle (d.h. zum Beispiel einem Ethernet-Port oder einem PPPoE-WAN-Partner) mehrere Paare von DNS-Servern (Primärer DNS-Server und Sekundärer DNS-Server) zuweisen. Verwendet wird das Paar mit der höchsten

Feld	Beschreibung
	<p>Priorität, wenn die Schnittstelle im Zustand "up" ist.</p> <p>Mögliche Werte von 0 (höchste Priorität) bis 9 (niedrigste Priorität).</p> <p>Standardwert ist 5.</p>
Schnittstellenmodus	<p>Wählen Sie aus, ob die IP-Adressen von Name-Servern für die Namensauflösung von Internet-Adressen automatisch bezogen oder ob abhängig von der Priorität bis zu zwei feste DNS-Server-Adressen eingetragen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> • <i>Dynamisch</i> (Standardwert)
Schnittstelle	<p>Wählen Sie diejenige Schnittstelle, welcher das DNS-Server-Paar zugewiesen werden soll.</p> <p>Bei Schnittstellenmodus = <i>Dynamisch</i></p> <p>Mit der Einstellung <i>Keine</i> wird ein globaler DNS-Server angelegt.</p> <p>Bei Schnittstellenmodus = <i>Statisch</i></p> <p>Mit der Einstellung <i>Beliebig</i> wird ein DNS-Server für alle Schnittstellen konfiguriert.</p>
Primärer DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Manuell</i></p> <p>Geben Sie die IP-Adresse des ersten Name-Servers für die Namensauflösung von Internet-Adressen ein.</p>
Sekundärer DNS-Server	<p>Nur bei Schnittstellenmodus = <i>Manuell</i></p> <p>Geben Sie optional die IP-Adresse eines alternativen Name-Servers ein.</p>

18.1.3 Statische Hosts

Im Menü **Lokale Dienste->DNS->Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

18.1.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

Abb. 163: Lokale Dienste->DNS->Statische Hosts->Neu

Das Menü **Lokale Dienste->DNS->Statische Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
DNS-Hostname	<p>Geben Sie den Host-Namen ein, dem die in diesem Menü definierte IP-Adresse zugeordnet werden soll, wenn eine DNS-Anfrage positiv beantwortet wird. Wenn eine DNS-Anfrage negativ beantwortet wird, wird keine Adresse mitgeteilt.</p> <p>Der Eintrag kann auch mit der Wildcard * beginnen, z. B. *.teldat.de.</p> <p>Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK "<Name.>" ergänzt.</p> <p>Einträge mit Leerzeichen sind nicht erlaubt.</p>
Antwort	<p>Wählen Sie die Art der Antwort auf DNS-Anfragen zu diesem Eintrag aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Negativ</i>: Eine DNS-Anfrage nach DNS-Hostname wird negativ beantwortet. • <i>Positiv</i> (Standardwert): Eine DNS-Anfrage nach DNS-Hostname wird mit der dazugehörigen IP-Adresse beantwortet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Keine</i>: Ein DNS-Request wird ignoriert, es wird keine Antwort gegeben.
IP-Adresse	<p>Nur bei Antwort = <i>Positiv</i></p> <p>Geben Sie die IP-Adresse ein, die nach DNS-Hostname zugeordnet wird.</p>
TTL	<p>Geben Sie die Gültigkeitsdauer der Zuordnung von DNS-Hostname zu IP-Adresse in Sekunden ein (nur relevant bei Antwort = <i>Positiv</i>), die anfragenden Hosts übermittelt wird.</p> <p>Standardwert ist <i>86400</i> (= 24 h).</p>

18.1.4 Domänenweiterleitung

Im Menü **Lokale Dienste->DNS->Domänenweiterleitung** wird eine Liste aller konfigurierter Weiterleitungen für definierte Domänen angezeigt.

18.1.4.1 Neu

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

Abb. 164: **Lokale Dienste->DNS->Domänenweiterleitung->Neu**

Das Menü **Lokale Dienste->DNS->Domänenweiterleitung->Neu** besteht aus folgenden Feldern:

Felder im Menü Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	Wählen Sie aus, ob ein Host oder eine Domäne weitergeleitet

Feld	Beschreibung
	<p>werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Host</i> (Standardwert) • <i>Domäne</i>
Host	<p>Nur für Weiterleiten = <i>Host</i></p> <p>Geben Sie den Namen des Hosts ein, der weitergeleitet werden soll.</p> <p>Der Eintrag kann auch mit dem Wildcard * beginnen, z. B. *.teldat.de. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK " <Default Domain>." ergänzt.</p>
Domäne	<p>Nur für Weiterleiten = <i>Domäne</i></p> <p>Geben Sie den Namen der Domäne ein, die weitergeleitet werden soll.</p> <p>Der Eintrag kann auch mit dem Wildcard * beginnen, z. B. *.teldat.de. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK " <Default Domain>." ergänzt.</p>
Weiterleiten an	<p>Wählen Sie aus, wohin Anfragen an den in Host bzw. Domäne definierten Namen weitergeleitet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnittstelle</i> (Standardwert): Die Anfrage wird an die definierte Schnittstelle weitergeleitet. • <i>DNS-Server</i>: Die Anfrage wird an den definierten DNS-Server weitergeleitet.
Schnittstelle	<p>Nur für Weiterleiten an = <i>Schnittstelle</i></p> <p>Wählen Sie die Schnittstelle aus, über die Anfragen für die definierte Domäne eingehen und an den DNS-Server weitergeleitet werden sollen.</p>
DNS-Server	<p>Nur für Weiterleiten an = <i>DNS-Server</i></p> <p>Geben Sie IP-Adresse des primären und sekundären DNS-</p>

Feld	Beschreibung
	Servers ein.

18.1.5 Cache

Im Menü **Lokale Dienste->DNS->Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

The screenshot shows the 'Cache' management interface. At the top, there is a navigation bar with tabs: 'Globale Einstellungen', 'DNS-Server', 'Statische Hosts', 'Domänenweiterleitung', 'Cache', and 'Statistik'. Below the navigation bar, there is a control area with 'Automatisches Aktualisierungsintervall' set to 60 Sekunden and an 'Übernehmen' button. Below this is a table with columns: 'Beschreibung', 'IP-Adresse', 'Antwort', 'TTL', 'Referenzzähler', and 'Als statisch festlegen'. The table is currently empty. At the bottom, there are 'OK' and 'Abbrechen' buttons.

Abb. 165: **Lokale Dienste->DNS->Cache**

Sie können einzelne Einträge über das Kästchen in der jeweiligen Zeile oder alle gleichzeitig mit der Schaltfläche **Alle auswählen** markieren.

Durch Markieren eines Eintrags und Bestätigen mit **Als statisch festlegen** wird ein dynamischer Eintrag in einen statischen umgewandelt. Der entsprechende Eintrag verschwindet aus dieser Liste und wird in der Liste im Menü **Statische Hosts** angezeigt. Die TTL wird übernommen.

18.1.6 Statistik

Globale Einstellungen	DNS-Server	Statische Hosts	Domänenweiterleitung	Cache	Statistik
---------------------------------------	----------------------------	---------------------------------	--------------------------------------	-----------------------	---------------------------

Automatisches Aktualisierungsintervall	60	Sekunden	Übernehmen
DNS-Statistiken			
Empfangene DNS-Pakete	0		
Ungültige DNS-Pakete	0		
DNS-Anfragen	0		
Cache-Treffer	0		
Weitergeleitete Anfragen	0		
Cache-Trefferrate (%)	0		
Erfolgreich beantwortete Anfragen	0		
Serverfehler	0		

Abb. 166: Lokale Dienste->DNS->Statistik

Im Menü **Lokale Dienste->DNS->Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü DNS-Statistiken

Feld	Beschreibung
Empfangene DNS-Pakete	Zeigt die Anzahl der empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an, einschließlich der Antwortpakete auf weitergeleitete Anfragen.
Ungültige DNS-Pakete	Zeigt die Anzahl der ungültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Pakete an.
DNS-Anfragen	Zeigt die Anzahl der gültigen empfangenen und direkt an Ihr Gerät adressierten DNS-Requests an.
Cache-Treffer	Zeigt die Anzahl der Anfragen an, die mittels der statischen Einträge oder der dynamischen Einträge aus dem Cache beantwortet werden konnten.
Weitergeleitete Anfragen	Zeigt die Anzahl der Anfragen an, die an andere Name-Server weitergeleitet wurden.
Cache-Trefferrate (%)	Zeigt die Anzahl der Cache-Treffer pro DNS-Anfrage in Prozent an.
Erfolgreich beantwortete Anfragen	Zeigt die Anzahl der erfolgreich (positiv und negativ) beantworteten Anfragen an.
Serverfehler	Zeigt die Anzahl der Anfragen an, die kein Name-Server (weder positiv noch negativ) beantworten konnte.

18.2 HTTPS

Die Benutzeroberfläche Ihres Geräts können Sie von jedem PC aus mit einem aktuellen Web-Browser auch über eine HTTPS-Verbindung bedienen.

HTTPS (HyperText Transfer Protocol Secure) ist hierbei das Verfahren, um zwischen dem Browser, der zur Konfiguration verwendet wird, und dem Gerät eine verschlüsselte und authentifizierte Verbindung mittels SSL aufzubauen.

18.2.1 HTTPS-Server

Im Menü **Lokale Dienste->HTTPS->HTTPS-Server** konfigurieren Sie die Parameter der gesicherten Konfigurationsverbindung über HTTPS.

Abb. 167: **Lokale Dienste->HTTPS->HTTPS-Server**

Das Menü **Lokale Dienste->HTTPS->HTTPS-Server** besteht aus folgenden Feldern:

Felder im Menü HTTPS-Parameter

Feld	Beschreibung
HTTPS-TCP-Port	<p>Geben Sie den Port ein, über den die HTTPS-Verbindung aufgebaut werden soll.</p> <p>Möglich sind Werte von 0 bis 65535.</p> <p>Standardwert ist 443.</p>
Lokales Zertifikat	<p>Wählen Sie ein Zertifikat aus, das für die HTTPS-Verbindung verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Intern</i> (Standardwert): Wählen Sie diese Option, wenn Sie das auf dem Gerät voreingestellte Zertifikat verwenden möch-

Feld	Beschreibung
	ten. <ul style="list-style-type: none"> • <i><Zertifikatsname></i>: Wählen Sie ein unter Systemverwaltung->Zertifikate->Zertifikatsliste eingetragenes Zertifikat aus.

18.3 DynDNS-Client

Die Nutzung dynamischer IP-Adressen hat den Nachteil, dass ein Host im Netz nicht mehr aufgefunden werden kann, sobald sich seine IP-Adresse geändert hat. DynDNS sorgt dafür, dass Ihr Gerät auch nach einem Wechsel der IP-Adresse noch erreichbar ist.

Folgende Schritte sind zur Einrichtung notwendig:

- Registrierung eines Hostnamens bei einem DynDNS-Provider
- Konfiguration Ihres Geräts

Registrierung

Bei der Registrierung des Hostnamens legen Sie einen individuellen Benutzernamen für den DynDNS-Dienst fest, z. B. *dyn_client*. Dazu bieten die Service Provider unterschiedliche Domainnamen an, so dass sich ein eindeutiger Hostname für Ihr Gerät ergibt, z. B. *dyn_client.provider.com*. Der DynDNS-Provider übernimmt für Sie die Aufgabe, alle DNS-Anfragen bezüglich des Hosts *dyn_client.provider.com* mit der dynamischen IP-Adresse Ihres Geräts zu beantworten.

Damit der Provider stets über die aktuelle IP-Adresse Ihres Geräts informiert ist, kontaktiert Ihr Gerät beim Aufbau einer neuen Verbindung den Provider und propagiert seine derzeitige IP-Adresse.

18.3.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

18.3.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

DynDNS-Aktualisierung DynDNS-Provider

Basisparameter	
Hostname	<input type="text"/>
Schnittstelle	Eine auswählen ▾
Benutzername	<input type="text"/>
Passwort	••••••••
Provider	dyndns ▾
Aktualisierung aktivieren	<input type="checkbox"/> Aktiviert
Erweiterte Einstellungen	
Mail-Exchanger (MX)	<input type="text"/>
Wildcard	<input type="checkbox"/> Aktiviert
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 168: 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</p>

Feld	Beschreibung
	<p>DynDNS-Client->DynDNS-Provider konfiguriert werden.</p> <p>Standardwert ist <i>DynDNS</i> .</p>
Aktualisierung aktivieren	<p>Wählen Sie aus, ob der hier konfigurierte DynDNS-Eintrag aktiviert werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Mail-Exchanger (MX)	<p>Geben Sie den vollständigen Hostnamen eines Mailservers ein, an den E-Mails weitergeleitet werden sollen, wenn der hier konfigurierte Host keine Mail empfangen soll.</p> <p>Erkundigen Sie sich bei Ihrem Provider nach diesem Weiterleitungsdienst und stellen Sie sicher, dass E-Mails von dem als MX eingetragenen Host angenommen werden können.</p>
Wildcard	<p>Wählen Sie aus, ob die Weiterleitung aller Unterdomänen von Hostname zur aktuellen IP-Adresse von Schnittstelle aktiviert werden soll (Erweiterte Namensauflösung).</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

18.3.2 DynDNS-Provider

Im Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider** wird eine Liste aller konfigurierten DynDNS-Provider angezeigt.

18.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

DynDNS-Aktualisierung
DynDNS-Provider

Basisparameter	
Providername	<input type="text"/>
Server	<input type="text"/>
Aktualisierungspfad	<input type="text"/>
Port	<input type="text" value="80"/>
Protokoll	<input type="text" value="DynDNS"/> ▼
Aktualisierungsintervall	<input type="text" value="300"/> Sekunden

OK
Abbrechen

Abb. 169: Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu

Das Menü **Lokale Dienste->DynDNS-Client->DynDNS-Provider->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Providername	Tragen Sie einen Namen für diesen Eintrag ein.
Server	Geben Sie den Host-Namen oder die IP-Adresse des Servers ein, auf dem der DynDNS-Service des Providers läuft.
Aktualisierungspfad	Geben Sie den Pfad auf dem Server des Providers ein, auf dem das Skript zur Verwaltung der IP-Adresse Ihres Geräts zu finden ist. Fragen Sie Ihren Provider nach dem zu verwendenden Pfad.
Port	Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll. Erfragen Sie den entsprechenden Port bei Ihrem Provider. Standardwert ist <i>80</i> .
Protokoll	Wählen Sie eines der implementierten Protokolle aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>DynDNS</i> (Standardwert) • <i>Static DynDNS</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>ODS</i> • <i>HN</i> • <i>DYNS</i> • <i>GnuDIP-HTML</i> • <i>GnuDIP-TCP</i> • <i>Custom DynDNS</i> • <i>DnsExit</i>
Aktualisierungsintervall	<p>Geben Sie die Zeitdauer (in Sekunden) an, die Ihr Gerät mindestens warten muss, bevor es seine aktuelle IP-Adresse erneut beim DynDNS-Provider propagieren darf.</p> <p>Standardwert ist <i>300</i> Sekunden.</p>

18.4 DHCP-Server

Sie können Ihr Gerät als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) konfigurieren.

Jeder Rechner in Ihrem LAN benötigt, wie auch Ihr Gerät, eine eigene IP-Adresse. Eine Möglichkeit, IP-Adressen in Ihrem LAN zuzuweisen, bietet das Dynamic Host Configuration Protocol (DHCP). Wenn Sie Ihr Gerät als DHCP-Server einrichten, vergibt es anfragenden Rechnern im LAN automatisch IP-Adressen aus einem definierten IP-Adress-Pool.


Wenn ein Client erstmals eine IP-Adresse benötigt, schickt er eine DHCP-Anfrage (mit seiner MAC-Adresse) als Netzwerk-Broadcast an die verfügbaren DHCP-Server. Daraufhin erhält der Client (im Zuge einer kurzen Kommunikation) vom Teldat seine IP-Adresse.

Sie müssen so den Rechnern keine festen IP-Adressen zuweisen, der Konfigurationsaufwand für Ihr Netzwerk verringert sich. Dazu richten Sie einen Pool an IP-Adressen ein, aus dem Ihr Gerät jeweils für einen definierten Zeitraum IP-Adressen an Hosts im LAN vergibt. Ein DHCP-Server übermittelt auch die Adressen des statisch oder per PPP-Aushandlung eingetragenen Domain-Name-Servers (DNS), des NetBIOS Name Servers (WINS) und des Standard-Gateways.

18.4.1 IP-Pool-Konfiguration

Im Menü **Lokale Dienste->DHCP-Server+IP-Pool-Konfiguration** wird eine Liste aller konfigurierten IP-Pools angezeigt. Diese Liste ist global und zeigt auch in anderen Menüs konfigurierte Pools an.

18.4.1.1 Bearbeiten oder Neu

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

IP-Pool-Konfiguration
DHCP-Konfiguration
IP/MAC-Bindung
DHCP-Relay-Einstellungen

Basisparameter	
IP-Poolname	<input style="width: 90%;" type="text"/>
IP-Adressbereich	<input style="width: 45%;" type="text"/> - <input style="width: 45%;" type="text"/>
DNS-Server	Primär <input style="width: 60%;" type="text"/>
	Sekundär <input style="width: 60%;" type="text"/>
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 170: Lokale Dienste->DHCP-Server+IP-Pool-Konfiguration +Neu

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool eindeutig zu benennen.
IP-Adressbereich	Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.
DNS-Server	<p>Primär: Geben Sie die IP-Adresse des DNS-Servers ein, der von Clients, die eine Adresse aus diesem Pool beziehen, bevorzugt verwendet werden soll.</p> <p>Sekundär: Geben Sie die IP-Adresse eines alternativen DNS-Servers ein.</p>

18.4.2 DHCP-Konfiguration

Um Ihr Gerät als DHCP-Server zu aktivieren, müssen Sie zunächst IP-Adress-Pools definieren, aus denen die IP-Adressen an die anfragenden Clients verteilt werden.

Im Menü **Lokale Dienste->DHCP-Server+DHCP-Konfiguration** wird eine Liste aller konfigurierter IP-Adresspools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Status** die Möglichkeit, die angelegten DH-


CP-Pools zu aktivieren bzw. deaktivieren.



Hinweis

Im Auslieferungszustand ist der DHCP-Pool mit den IP-Adressen 192.168.0.10 bis 192.168.0.49 vorkonfiguriert, und wird verwendet, wenn kein anderer DHCP-Server im Netzwerk verfügbar ist.

18.4.2.1 Bearbeiten oder Neu

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

IP-Pool-Konfiguration
DHCP-Konfiguration
IP/MAC-Bindung
DHCP-Relay-Einstellungen

Basisparameter							
Schnittstelle	Eine auswählen ▼						
IP-Poolname	Noch nicht definiert ▼						
Pool-Verwendung	Lokal ▼						
Erweiterte Einstellungen:							
Gateway	Router als Gateway verwenden ▼						
Lease Time	120 Minuten						
DHCP-Optionen	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="border-bottom: 1px solid black; width: 60%; padding: 2px;">Option</td> <td style="border-bottom: 1px solid black; width: 30%; padding: 2px;">Wert</td> <td style="border-bottom: 1px solid black; width: 10%;"></td> </tr> <tr> <td colspan="3" style="text-align: center; padding: 5px;">Hinzufügen</td> </tr> </table>	Option	Wert		Hinzufügen		
Option	Wert						
Hinzufügen							
OK Abbrechen							

Abb. 171: 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	Wählen Sie die Schnittstelle aus, über welche die in IP-Adressbereich definierten Adressen an anfragende DHCP-Clients vergeben werden. Wenn eine DHCP-Anfrage über diese Schnittstelle eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.
IP-Poolname	Geben Sie eine beliebige Beschreibung ein, um den IP-Pool

Feld	Beschreibung
	eindeutig zu benennen.
Pool-Verwendung	<p>Wählen Sie aus, ob der IP-Pool für DHCP-Anfragen im gleichen Subnetz verwendet werden soll oder für DHCP-Anfragen, die aus einem anderen Subnetz zu Ihrem Gerät weitergeleitet wurden. In diesem Fall ist es möglich, IP-Adressen aus einem anderen Netz zu definieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokal</i> (Standardwert): Der DHCP-Pool wird nur für DHCP-Anfragen im selben Subnetz verwendet. • <i>Relais</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetz verwendet. • <i>Lokal/Relais</i>: Der DHCP-Pool wird für DHCP-Anfragen im selben Subnetz und aus anderen Subnetzen verwendet.

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


Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Gateway	<p>Wählen Sie aus, welche IP-Adresse dem DHCP-Client als Gateway übermittelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Router als Gateway verwenden</i> (Standardwert): Hier wird die für die Schnittstelle definierte IP-Adresse übertragen. • <i>Kein Gateway</i>: Hier wird keine IP-Adresse übermittelt. • <i>Angeben</i>: Geben Sie die entsprechende IP-Adresse ein.
Lease Time	<p>Geben Sie ein, wie lange (in Minuten) eine Adresse aus dem Pool einem Host zugewiesen werden soll.</p> <p>Nachdem Lease Time abgelaufen ist, kann die Adresse durch den Server neu vergeben werden.</p> <p>Standardwert ist <i>120</i>.</p>
DHCP-Optionen	Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen.

Feld	Beschreibung
	<p>Mögliche Werte für Option:</p> <ul style="list-style-type: none"> • <i>Zeitserver</i> (Standardwert): Geben Sie die IP-Adresse des Zeitserver ein, die dem Client übermittelt werden soll. • <i>DNS-Server</i>: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • <i>DNS-Domänenname</i>: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • <i>WINS/NBNS-Server</i>: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • <i>WINS/NBT Node Type</i>: Wählen Sie den Typ des WINS/NBT Nodes, der dem Client übermittelt werden soll. • <i>TFTP-Server</i>: Geben Sie die IP-Adresse des TFTP-Servers ein, die dem Client übermittelt werden soll. • <i>CAPWAP Controller</i>: Geben Sie die IP-Adresse des CAPWAP Controllers ein, die dem Client übermittelt werden soll. • <i>URL (Provisionierungsserver)</i>: Mit dieser Option können Sie einem Client eine beliebige URL übermitteln. <p>Verwenden Sie diese Option, um anfragenden IP1x0-Telefonen die URL des Provisionierungsservers zu übermitteln, wenn eine automatische Provisionierung der Telefone vorgenommen werden soll. Die URL muss dann die Form <i>http://<IP-Adresse des Provisionierungsservers>/eg_prov</i> haben.</p> <ul style="list-style-type: none"> • <i>Herstellergruppe</i> (Vendor Specific Information): Mit dieser Option können Sie dem Client in einem beliebigen Text-String ggf. herstellerspezifische Informationen übermitteln. <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche Hinzufügen ein.</p>

Bearbeiten

Im Menü **Lokale Dienste -> DHCP-Server +DHCP-Konfiguration->Erweiterte Einstellungen** können Sie einen Eintrag im Feld **DHCP-Optionen** bearbeiten, wenn **Option = Herstellergruppe** gewählt ist.

Wählen Sie das Symbol , um einen vorhandenen Eintrag zu bearbeiten. Im Popup-Menü konfigurieren Sie herstellerspezifische Einstellungen im DHCP-Server für bestimmte Telefone.

Felder im Menü Basisparameter

Feld	Beschreibung
Hersteller auswählen	<p>Dieser Parameter wird von Ihrem Gerät aktuell nicht verwendet.</p> <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 (code 3)	<p>Dieser Parameter wird von Ihrem Gerät aktuell nicht verwendet.</p> <p>Geben Sie ein, welcher herstellerepezifische 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>

18.4.3 IP/MAC-Bindung

Im Menü **Lokale Dienste->DHCP-Server->IP/MAC-Bindung** wird eine Liste aller Clients angezeigt, die per DHCP eine IP-Adresse von Ihrem Gerät erhalten haben.

Sie haben die Möglichkeit, bestimmten MAC-Adressen eine gewünschte IP-Adresse aus einem definierten IP-Adress-Pool zuzuweisen. Dazu können Sie in der Liste die Option **Statische Bindung** wählen, um einen Listeneintrag als feste Bindung zu übernehmen, oder Sie legen manuell eine feste IP/MAC-Bindung an, indem Sie diese im Untermenü **Neu** konfigurieren.



Hinweis

Neue statische IP/MAC-Bindungen können erst angelegt werden, wenn in **Lokale Dienste->DHCP-Server+DHCP-Konfiguration** IP-Adressbereiche konfiguriert wurden.

18.4.3.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

[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"/>

Abb. 172: 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.

18.4.4 DHCP-Relay-Einstellungen

Wenn Ihr Gerät für das lokale Netz keine IP-Adressen per DHCP an die Clients verteilt, kann es dennoch die DHCP-Anforderungen aus dem lokalen Netzwerk stellvertretend an einen entfernten DHCP-Server weiterleiten. Der DHCP-Server vergibt Ihrem Gerät dann eine IP-Adresse aus seinem Pool, die dieser wiederum an den Client ins lokale Netzwerk schickt.

Abb. 173: Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen

Das Menü **Lokale Dienste->DHCP-Server->DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Primärer DHCP-Server	Geben Sie die IP-Adresse eines Servers ein, an den BootP- oder DHCP-Anfragen weitergeleitet werden sollen.
Sekundärer DHCP-Server	Geben Sie die IP-Adresse eines alternativen BootP- oder DHCP-Servers ein.

18.5 Scheduling

Ihr Gerät verfügt über einen Aufgabenplaner, mit dem bestimmte Standardaktionen (beispielsweise Aktivierung bzw. Deaktivierung von Schnittstellen) durchgeführt werden können. Außerdem ist jede vorhandene MIB-Variable mit jedem beliebigen Wert konfigurierbar.

Sie legen die gewünschten **Aktionen** fest und definieren die **Auslöser**, die steuern, wann bzw. unter welchen Bedingungen die **Aktionen** durchgeführt werden sollen. Ein **Auslöser** kann ein einzelnes Ereignis sein oder eine Folge von Ereignissen, die in einer **Ereignisliste** zusammengefasst sind. Für ein einzelnes Ereignis legen Sie ebenfalls eine Ereignisliste an, die jedoch nur ein Element enthält.

Es ist möglich, zeitgesteuert Aktionen auszulösen. Außerdem kann der Status oder die Erreichbarkeit von Schnittstellen oder deren Datenverkehr zur Ausführung der konfigurierten Aktionen führen, oder aber auch die Gültigkeit von Lizenzen. Auch hier ist es möglich, jede beliebige MIB-Variable mit jedem beliebigen Wert als Auslöser einzurichten.

Um den Aufgabenplaner in Betrieb zu nehmen, aktivieren Sie das **Schedule-Intervall** unter **Optionen**. Dieses Intervall gibt den Zeitabstand vor, in dem das System prüft, ob mindestens ein Ereignis eingetreten ist. Dieses Ereignis dient als Auslöser für eine konfigurierte Aktion.



Achtung

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise der Teldat Gateways. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration z. B. auf Ihrem PC.



Hinweis

Voraussetzung für den Betrieb des Aufgabenplaners ist ein auf Ihrem Gerät eingestelltes Datum ab dem 1.1.2000.

18.5.1 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.

18.5.1.1 Neu

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

Auslöser
Aktionen
Optionen

Basisparameter	
Ereignisliste	Neu ▾
Beschreibung	<input type="text"/>
Ereignistyp	Zeit ▾
Zeitintervall auswählen	
Zeitbedingung	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> Bedingungstyp <input type="radio"/> Wochentag <input checked="" type="radio"/> Perioden <input type="radio"/> Tag des Monats </div> <div style="width: 50%;"> Bedingungeinstellungen <div style="border: 1px solid gray; padding: 2px;"> Montag ▾ Täglich ▾ 1 ▾ </div> </div> </div>
	Startzeit
Stopzeit	Stunde <input type="text"/> Minute <input type="text"/>
OK Abbrechen	

Abb. 174: **Lokale Dienste->Scheduling->Auslöser->Neu**

Das Menü **Lokale Dienste->Scheduling->Auslöser->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Ereignisliste	<p>Mit <i>Neu</i> (Standardwert) können Sie eine neue Ereignisliste anlegen. Mit Beschreibung geben Sie dieser Liste einen Namen. Mit Hilfe der übrigen Parameter legen Sie das erste Ereignis in der Liste an.</p> <p>Wenn Sie eine bestehende Ereignisliste erweitern wollen, wählen Sie die gewünschte Ereignisliste aus und fügen ihr mindestens ein Ereignis hinzu.</p> <p>Über Ereignislisten können auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden. Die Ereignisse werden in derselben Reihenfolge abgearbeitet wie sie in der Liste angelegt sind.</p>
Beschreibung	<p>Nur für Ereignisliste = <i>Neu</i></p> <p>Geben Sie eine beliebige Bezeichnung für die Ereignisliste ein.</p>
Ereignistyp	<p>Wählen Sie den Typ des Ereignisses aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Zeit</i> (Standardwert): Die in Aktionen konfigurierten und zugewiesenen Aktionen werden zu bestimmten Zeitpunkten ausgelöst. • <i>MIB/SNMP</i>: Die in Aktionen konfigurierten und zugewiesenen Aktionen werden ausgelöst, wenn die definierten MIB-Variablen die angegebenen Werte annehmen. • <i>Schnittstellenstatus</i>: Die in Aktionen konfigurierten und zugewiesenen 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 zugewiesenen Aktionen werden ausgelöst, wenn die angegebene IP-Adresse erreichbar bzw. nicht erreichbar ist. • <i>Lebensdauer eines Zertifikats</i>: Die in Aktionen kon-

Feld	Beschreibung
	<p>figurierten und zugewiesene Aktionen werden ausgelöst, wenn die definierte Gültigkeitsdauer erreicht ist.</p>
Überwachte Variable	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie die MIB-Variable aus, deren definierter Wert als Auslöser konfiguriert werden soll. Wählen Sie zunächst das System aus, in dem die MIB-Variable gespeichert ist, dann die MIB-Tabelle und dann die MIB-Variable selber. Es werden nur die MIB-Tabellen und MIB-Variablen angezeigt, die im jeweiligen Bereich vorhanden sind.</p>
Vergleichsbedingung	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie aus, ob die MIB-Variable <i>Größer</i> (Standardwert), <i>Gleich</i>, <i>Kleiner</i>, <i>Ungleich</i> dem in <i>Vergleichswert</i> angegebenen Wert sein oder innerhalb von <i>Bereich</i> liegen muss, um die Aktion auszulösen.</p>
Vergleichswert	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Geben Sie den Wert der MIB-Variable ein.</p>
Indexvariablen	<p>Nur für Ereignistyp <i>MIB/SNMP</i></p> <p>Wählen Sie bei Bedarf MIB-Variablen aus, um einen bestimmten Datensatz in der MIB-Tabelle eindeutig zu kennzeichnen, z.B. <i>ConnIfIndex</i>. Aus der Kombination von Indexvariable (in der Regel eine Indexvariable, die mit * gekennzeichnet ist) und Indexwert ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.</p> <p>Legen Sie weitere Indexvariablen mit Hinzufügen an.</p>
Überwachte Schnittstelle	<p>Nur für Ereignistyp <i>Schnittstellenstatus</i> und <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Schnittstelle aus, deren definierter Status ein Ereignis auslösen soll.</p>
Schnittstellenstatus	<p>Nur für Ereignistyp <i>Schnittstellenstatus</i></p> <p>Wählen Sie den Status aus, den die Schnittstelle einnehmen muss, um die gewünschte Aktion auszulösen.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiv</i> (Standardwert): Die Schnittstelle ist aktiv. • <i>Inaktiv</i>: Die Schnittstelle ist inaktiv.
<p>Richtung des Datenverkehrs</p>	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Wählen Sie die Richtung des Datenverkehrs aus, deren Werte für das Auslösen einer Aktion beobachtet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>RX</i> (Standardwert): Der eingehende Datenverkehr wird überwacht. • <i>TX</i>: Der ausgehende Datenverkehr wird überwacht.
<p>Bedingung des Schnittstellenverkehrs</p>	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Wählen Sie aus, ob der Wert für Datenverkehr <i>Größer</i> (Standardwert) oder <i>Kleiner</i> dem in <i>Übertragener Datenverkehr</i> angegebenen Wert sein muss, um die Aktion auszulösen.</p>
<p>Übertragener Datenverkehr</p>	<p>Nur für Ereignistyp <i>Schnittstellenverkehr</i></p> <p>Geben Sie den gewünschten Wert für den Datenverkehr, mit dem verglichen werden soll, in kBytes ein.</p> <p>Standardwert ist 0.</p>
<p>Ziel-IP-Adresse</p>	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, deren Erreichbarkeit überprüft werden soll.</p>
<p>Quell-IP-Adresse</p>	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die IP-Adresse ein, die als Absendeadresse für den Ping-Test verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse der Schnittstelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Spezifisch</i>: Geben Sie die gewünschte IP-Adresse in das Eingabefeld ein.
Status	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Wählen Sie aus, ob Ziel-IP-Adresse <i>Erreichbar</i> (Standardwert) oder <i>Nicht erreichbar</i> sein muss, um die Aktion auszulösen.</p>
Intervall	<p>Nur für Ereignistyp <i>Ping-Test</i></p> <p>Geben Sie die Zeit in Sekunden ein, nach der erneut ein Ping gesendet werden soll.</p> <p>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>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>

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 Bedingungeinstellungen einen Wochentag aus.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Perioden</i> (Standardwert): Wählen Sie in Bedingungeinstellungen einen bestimmten Turnus aus. • <i>Tag des Monats</i>: Wählen Sie in Bedingungeinstellungen einen bestimmten Tag im Monat aus. <p>Mögliche Werte für Bedingungeinstellungen bei Bedingungstyp = <i>Wochentag</i>:</p> <p><i>Montag</i> (Standardwert) ... <i>Sonntag</i>.</p> <p>Mögliche Werte für Bedingungeinstellungen 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 Bedingungeinstellungen bei Bedingungstyp = <i>Tag des Monats</i>:</p> <p>1... 31.</p>
Startzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.
Stoppzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine Stoppzeit eingeben oder Stoppzeit = Startzeit setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.

18.5.2 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.

18.5.2.1 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: 80%;" type="text" value="60"/> Sekunden

OK
Abbrechen

Abb. 175: 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.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Zertifikatverwaltung</i>: Ein Zertifikat soll erneuert, gelöscht oder eingetragen werden. • <i>5 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5-GHz-Frequenzbands wird durchgeführt. • <i>5,8 GHz-WLAN-Bandscan</i>: Nur für Geräte mit Wireless LAN. Ein Scan des 5,8-GHz-Frequenzbands wird durchgeführt. • <i>WLC: Neuer Neighbor-Scanvorgang</i>: Nur für Geräte mit WLAN Controller. In einem durch den WLAN Controller kontrollierten WLAN-Netz wird ein Neighbor Scan ausgelöst. • <i>WLC: VSS-Status</i>: Nur für Geräte mit WLAN Controller. Der Status eines Drahtlosnetzwerkes wird verändert.
Ereignisliste	Wählen Sie die gewünschte Ereignisliste aus, die in Lokale Dienste->Scheduling->Auslöser angelegt ist.
Bedingung für Ereignisliste	<p>Wählen Sie für die gewählte Ereignisliste aus, wieviele der konfigurierten Ereignisse eintreten müssen, damit die Aktion ausgelöst wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Die Aktion wird ausgelöst, wenn alle Ereignisse eintreten. • <i>Eins</i>: Die Aktion wird ausgelöst, wenn ein Ereignis eintritt. • <i>Keiner</i>: Die Aktion wird ausgelöst, wenn keines der Ereignisse eintritt. • <i>Eins nicht</i>: Die Aktion wird ausgelöst, wenn eines der Ereignisse nicht eintritt.
Neustart des Geräts nach	<p>Nur bei Befehlstyp = <i>Neustart</i></p> <p>Geben Sie die Zeitspanne in Sekunden an, die nach dem Eintreten des Ereignisses gewartet werden soll, bis das Gerät neu gestartet wird.</p> <p>Standardwert ist <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 zu-</p>

Feld	Beschreibung
	<p>nächst 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. • <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</p>

Feld	Beschreibung
	<p>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></p> <p>Wählen Sie den Status aus, den das Drahtlosnetzwerk erhalten soll.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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 Teldat-Server</i> (Standardwert): Die aktuelle Software wird vom Teldat-Server geladen. • <i>HTTP-Server</i>: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen. • <i>HTTPS-Server</i>: Die aktuelle Software wird von einem HTTPS-Server geladen, den Sie über die <i>Server-URL</i> festlegen. • <i>TFTP-Server</i>: Die aktuelle Software wird von einem TFTP-Server geladen, den Sie über die <i>Server-URL</i> festlegen.
Server-URL	<p>Bei Befehlstyp = <i>Softwareaktualisierung</i> wenn Quelle nicht <i>Aktuelle Software vom Teldat-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>

Feld	Beschreibung
	<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>FTTP</i>
CSV-Dateiformat	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Datei im CSV-Format übertragen werden soll.</p> <p>Das CSV-Format kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel</p>

Feld	Beschreibung
	<p>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, Konfiguration umbenennen oder Konfiguration kopieren</i></p> <p>Geben Sie beim Importieren, Umbenennen oder Kopieren einen Namen für die Konfigurationsdatei ein, unter dem sie lokal auf dem Gerät gespeichert werden soll.</p>
Dateiname in Flash	<p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration exportieren</i></p> <p>Wählen Sie die Datei aus, die exportiert werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration umbenennen</i></p> <p>Wählen Sie die Datei aus, die umbenannt werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration löschen</i></p> <p>Wählen Sie die Datei aus, die gelöscht werden soll.</p> <p>Bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration kopieren</i></p> <p>Wählen Sie die Datei aus, die kopiert werden soll.</p>
Konfiguration enthält Zertifikate/Schlüssel	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren oder Konfiguration</i></p>

Feld	Beschreibung
	<p><i>exportieren</i></p> <p>Wählen Sie aus, ob in der Konfiguration enthaltene Zertifikate und Schlüssel importiert oder exportiert werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Konfiguration verschlüsseln	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i> oder <i>Konfiguration exportieren</i></p> <p>Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Nach Ausführung neu starten	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i></p> <p>Wählen Sie aus, ob Ihr Gerät nach der gewünschten Aktion neu gestartet werden soll.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Versionsprüfung	<p>Nur bei Befehlstyp = <i>Konfigurationsmanagement</i> und Aktion = <i>Konfiguration importieren</i></p> <p>Wählen Sie aus, ob beim Import einer Konfigurationsdatei 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 Schnitt-

Feld	Beschreibung
	<p>stelle, über die der Ping versendet wird, wird automatisch als Absendeadresse eingetragen.</p> <ul style="list-style-type: none"> • <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>Standardwert ist 1 Sekunde.</p>
Versuche	<p>Nur bei Befehlstyp = <i>Ping-Test</i></p> <p>Geben Sie die Anzahl der Ping-Tests ein, die durchgeführt werden soll, bis Ziel-IP-Adresse als unerreichbar gilt.</p> <p>Standardwert ist 3.</p>
Serveradresse	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie die URL des Servers ein, von dem eine Zertifikatsdatei geholt werden soll.</p>
Lokale Zertifikatsbeschreibung	<p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Geben Sie eine Beschreibung für das Zertifikat ein, unter der es im Gerät gespeichert werden soll.</p> <p>Bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat löschen</i></p> <p>Wählen Sie das Zertifikat aus, das gelöscht werden soll.</p>
Kennwort für geschütztes Zertifikat	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>Zertifikat importieren</i></p> <p>Wählen Sie aus, ob Sie ein geschütztes Zertifikat verwenden möchten, das ein Passwort benötigt, und geben Sie dieses in das Eingabefeld ein.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
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. <i>http://scep.teldat.de:8080/scep/scep.dll</i></p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
Subjektname	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie einen Subjektnamen mit Attributen ein.</p> <p>Beispiel: <i>"CN=VPNServer, DC=mydomain, DC=com, c=DE"</i></p>
CA-Name	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Geben Sie den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z.</p>

Feld	Beschreibung
	<p>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>
Autospeichermodus	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Wählen Sie, ob Ihr Gerät intern automatisch die verschiedenen Schritte des Registrierungsprozesses speichert. Dies ist dann von Nutzen, wenn die Registrierung nicht sofort abgeschlossen werden kann. Falls der Status nicht gespeichert wurde, kann die unvollständige Registrierung nicht abgeschlossen werden. Sobald die Registrierung abgeschlossen ist und das Zertifikat vom CA-Server heruntergeladen wurde, wird es automatisch in der Konfiguration Ihres Geräts gespeichert.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CRL verwenden	<p>Nur bei Befehlstyp = <i>Zertifikatverwaltung</i> und Aktion = <i>SCEP</i></p> <p>Legen Sie hier fest, inwiefern Sperrlisten (CRLs) in die Validierung von Zertifikaten, die vom Besitzer dieses Zertifikats gestellt wurden, einbezogen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auto</i> (Standardwert): Falls im CA-Zertifikat ein Eintrag für einen Zertifikatssperrlisten-Verteilungspunkt (CDP, CRL Distribution Point) vorhanden ist, soll dieser zusätzlich zu den global im Gerät konfigurierten Sperrlisten ausgewertet werden.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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>5,8 GHz-WLAN-Bandscan</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>
Status festlegen	<p>Nur bei Befehlstyp = <i>WLC: VSS-Status</i></p> <p>Wählen Sie den Status aus, in den das ausgewählte Drahtlosnetzwerk versetzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert) • <i>Deaktivieren</i>

18.5.3 Optionen

Im Menü **Lokale Dienste->Scheduling->Optionen** konfigurieren Sie das Schedule-Intervall.

The image shows a software interface with three tabs: 'Auslöser', 'Aktionen', and 'Optionen'. The 'Optionen' tab is selected. Below the tabs is a dialog box titled 'Scheduling-Optionen'. Inside the dialog, there is a field for 'Schedule-Intervall' with the value '0' and the unit 'sec'. To the right of this field is a checked checkbox labeled 'Aktiviert'. At the bottom of the dialog, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 176: **Lokale Dienste->Scheduling->Optionen**

Das Menü **Lokale Dienste->Scheduling->Optionen** besteht aus folgenden Feldern:

Felder im Menü Scheduling-Optionen

Feld	Beschreibung
Schedule-Intervall	<p>Wählen Sie aus, ob das Schedule-Intervall aktiviert werden soll.</p> <p>Geben Sie die Zeitspanne in Sekunden ein, nach der das System jeweils prüft, ob konfigurierte Ereignisse eingetreten sind.</p> <p>Möglich sind Werte zwischen 0 und 65535.</p> <p>Empfohlen wird der Wert 300 (5 Minuten Genauigkeit). Werte kleiner als 60 haben in der Regel keinen Sinn und benötigen unnötig Systemressourcen.</p>

18.6 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.

Bei Geräten der **bintec WI**-Serie können Sie die Temperatur überwachen lassen.




Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

18.6.1 Hosts

Im Menü **Lokale Dienste->Überwachung->Hosts** wird eine Liste aller überwachten Hosts angezeigt.

18.6.1.1 Bearbeiten oder Neu

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

Hosts Schnittstellen Temperatur Ping-Generator

Hostparameter					
Gruppen-ID	Neue ID ▾				
Trigger					
Überwachte IP-Adresse	Standard-Gateway ▾				
Quell-IP-Adresse	Automatisch ▾				
Intervall	10 <input type="text"/> Sekunden				
Erfolgreiche Versuche	3 <input type="text"/>				
Fehlgeschlagene Versuche	3 <input type="text"/>				
Auszuführende Aktion	<table border="1"> <thead> <tr> <th>Aktion</th> <th>Schnittstelle</th> </tr> </thead> <tbody> <tr> <td>Deaktivieren ▾</td> <td>Eine auswählen ▾</td> </tr> </tbody> </table> <p style="text-align: center;">Hinzufügen</p>	Aktion	Schnittstelle	Deaktivieren ▾	Eine auswählen ▾
Aktion	Schnittstelle				
Deaktivieren ▾	Eine auswählen ▾				
OK Abbrechen					

Abb. 177: 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>


Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Standard-Gateway</i> (Standardwert): Das Standard-Gateway wird überwacht. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse des zu überwachenden Hosts ein.
Quell-IP-Adresse	<p>Wählen Sie aus, wie die IP-Adresse ermittelt werden soll, die Ihr Gerät als Quelladresse des Pakets verwendet, das an den zu überwachenden Host gesendet wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i>: Geben Sie in das nebenstehende Eingabefeld die IP-Adresse ein.
Intervall	<p>Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Standardwert ist 10.</p> <p>Innerhalb einer Gruppe wird das kleinste Intervall der Gruppenmitglieder verwendet.</p>
Erfolgreiche Versuche	<p>Geben Sie ein, wieviele Pings beantwortet werden müssen, damit der Host als erreichbar angesehen wird.</p> <p>Mit dieser Einstellung können Sie zum Beispiel festlegen, wann ein Host als wieder erreichbar gilt und statt eines Backup-Geräts erneut verwendet wird.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>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>

Feld	Beschreibung
	Standardwert ist 3.
Auszuführende Aktion	<p>Wählen Sie aus, welche Aktion ausgeführt werden soll. Für die meisten Aktionen wählen Sie eine Schnittstelle, auf die sich die Aktion bezieht.</p> <p>Auswählbar sind alle physikalischen und virtuellen Schnittstellen.</p> <p>Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (<i>Aktivieren</i>), deaktiviert (<i>Deaktivieren</i>, Standardwert) oder zurückgesetzt (<i>Zurücksetzen</i>) werden soll oder ob die Verbindung erneut aufgebaut (<i>Erneut wählen</i>) werden soll.</p> <p>Mit Aktion = Überwachen können Sie die IP-Adresse überwachen, die unter Überwachte IP-Adresse angegeben ist. Diese Information kann für andere Funktionen, wie die IP-Adresse zur Nachverfolgung, genutzt werden.</p>

18.6.2 Schnittstellen

Im Menü **Lokale Dienste->Überwachung->Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.

18.6.2.1 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
Temperatur
Ping-Generator

Basisparameter	
Überwachte Schnittstelle	Eine auswählen ▾
Trigger	Schnittstelle wird aktiviert. ▾
Schnittstellenaktion	Aktivieren ▾
Schnittstelle	Eine auswählen ▾
OK Abbrechen	

Abb. 178: **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> .

18.6.3 Temperatur

Die Geräte der **WI**-Serie sind mit einem Temperatur-Sensor ausgestattet. Dieser befindet sich auf der Hauptplatine unterhalb der ersten WLAN-Karte.

Der Sensor misst die aktuelle Temperatur. Sein Messbereich erstreckt sich von -55 °C bis +125 °C bei einer Genauigkeit von unter 1 °C.


Zusätzlich wird die erreichte Minimal- und Maximaltemperatur aufgezeichnet zusammen mit dem Zeitpunkt, an dem die jeweilige Temperatur erreicht wurde. Bei einem Neustart

des Geräts werden die Werte zurückgesetzt und neu aufgezeichnet.

Standardmäßig sind untere und obere Grenzwerte für die Temperatur festgelegt, die bei Verletzung eine Alarm-Variable setzen und eine Syslog-Meldung erzeugen. Die Aktualisierung erfolgt alle 10 Sekunden.

Im Menü **Lokale Dienste->Überwachung->Temperatur** werden die Temperaturgrenzwerte konfiguriert. Sie können eine Grenzwertverletzung an eine Aktion koppeln.

18.6.3.1 Bearbeiten oder Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um neue Grenzwerte und Aktionen zu konfigurieren.

Hosts Schnittstellen Temperatur Ping-Generator

Basisparameter	
Trigger	Temperatur über °C
Aktion	Aktivieren
Schnittstelle	Relais
OK Abbrechen	

Abb. 179: Lokale Dienste->Überwachung->Temperatur ->Neu

Felder im Menü Basisparameter


Feld	Beschreibung
Trigger	<p>Geben Sie die Temperatur ein, die nicht über- bzw. unterschritten werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Temperatur über</i> • <i>Temperatur unter</i>
Aktion	<p>Wählen Sie die gewünschte Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktivieren</i> (Standardwert) • <i>Deaktivieren</i>
Schnittstelle	<p>Wählen Sie aus, über welche Schnittstelle die Aktion ausgeführt</p>


Feld	Beschreibung
	<p>werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Relais</i> (Standardwert): Die Grenzwertverletzung wird mit dem Relais gekoppelt (siehe Menü Physikalische Schnittstellen->Relais->Relaiskonfiguration). • <Schnittstelle>: Bei Temperaturüberschreitung wird die gewählte Schnittstelle abgeschaltet.

18.6.4 Ping-Generator

Im Menü **Lokale Dienste->Überwachung->Ping-Generator** wird eine Liste aller konfigurierten Pings angezeigt, die automatisch generiert werden.

18.6.4.1 Bearbeiten oder Neu

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



Basisparameter	
Ziel-IP-Adresse	<input type="text"/>
Quell-IP-Adresse	Spezifisch <input type="text"/>
Intervall	10 <input type="text"/> Sekunden
Versuche	3 <input type="text"/>

Abb. 180: **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.

Feld	Beschreibung
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>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>Standardwert ist 3.</p>

18.7 Teldat Discovery

18.7.1 Gerätesuche

Das Teldat Discovery Protokoll dient zur Erkennung und Konfiguration von Teldat Access-Points, die sich im gleichen kabelgebundenen Netz befinden wie Ihr Gerät. Nachdem ein Access-Point erkannt wurde, können bestimmte Basisparameter (Knotenname, IP-Adresse, Netzmaske und Geräte-Adresse) auf dem Access-Point konfiguriert werden (vorausgesetzt Sie kennen das Administrator-Passwort).



Hinweis

Eventuell vorhandene Teldat Access-Points werden mittels eines Multicasts ermittelt. Daher ist es unerheblich ob und welche IP-Adresse der Access-Point hat.

Beachten Sie, dass erkannte Teldat Access-Points nicht im Flash gespeichert werden, d. h. die Erkennung muss nach einem Neustart Ihres Geräts wiederholt werden.

Im Menü **Lokale Dienste->Teldat Discovery->Gerätesuche** wird unter **Ergebnisse** eine Liste aller erkannten Access-Points im Netzwerk angezeigt. Im Feld **Schnittstelle** wählen Sie die Schnittstelle Ihres Geräts aus, über das die Access-Point Erkennung durchgeführt werden soll. Mit der Option *-Alle-* werden alle Schnittstellen abgefragt.

Unter Ermittlungsstatus wird der aktuelle Erkennungsstatus für jede einzelne Schnittstelle angezeigt. Hierbei bedeutet *Keiner*, dass keine Erkennung aktiv ist. *Suchen* wird angezeigt, wenn aktuell eine Erkennung durchgeführt wird.

Ihr Gerät kann über diese Erkennungsfunktion ebenfalls von anderen Access Points mit Discovery-Funktion erkannt und konfiguriert werden. Dieses konfigurieren Sie im Untermenü **Optionen**.

18.7.1.1 Finden


Wählen Sie die Schaltfläche **Finden**, um die Teldat Access-Point-Erkennung zu starten.

Gerätesuche Optionen

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden		Übernehmen		
Ermittlungsstatus				
Schnittstelle			Status	
br0			Suchen	
Funkwerk Discovery starten				
Schnittstelle	-Alle- <input type="button" value="v"/>			
Ergebnisse				
Schnittstelle	Knotenname	IP-Adresse/Maske	MAC-Adresse	Letztes Schreibergebnis
br0	wi3040	192.168.0.252 / 255.255.255.0	00:01:cd:06:1a:b4	Kein Fehler
br0	w1002n	10.0.0.233 / 255.255.255.0	00:01:cd:0e:8f:04	Kein Fehler

Finden

Abb. 181: **Lokale Dienste->Teldat Discovery->Gerätesuche**

Wurden Access-Points im Netzwerk erkannt, erscheinen diese in der Liste. Über die -Schaltfläche gelangen Sie in das Konfigurationsmenü für den jeweiligen Access-Point.

Gerätesuche
Optionen

Basisparameter	
Schnittstelle	br0
MAC-Adresse	00:01:c:d:06:1a:b4
Knotenname	<input type="text" value="wi3040"/>
IP-Adresse	<input type="text" value="192.168.0.252"/>
Netzmaske	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
Authentifizierungspasswort	<input type="text"/>
Letztes Schreibergebnis	Kein Fehler

OK
Abbrechen

Abb. 182: Lokale Dienste->Teldat Discovery->Gerätesuche->

Dieses Menü Lokale Dienste->Teldat Discovery->Gerätesuche-> besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	Der Wert dieses Feldes kann nur gelesen werden. Zeigt die Schnittstelle Ihres Geräts an, an welchem die Erkennung durchgeführt wird.
MAC-Adresse	Der Wert dieses Feldes kann nur gelesen werden. Zeigt die MAC-Adresse des erkannten Access-Points an.
Knotenname	Sie können den Namen des erkannten Access-Points ändern.
IP-Adresse	Sie können die IP-Adresse des erkannten Access-Points ändern.
Netzmaske	Sie können die dazugehörige Netzmaske ändern.
Gateway	Sie können die Gateway-Adresse des erkannten Access-Points ändern.
Authentifizierungspasswort	Geben Sie das Administrator-Passwort des Access-Points ein. Ohne Passwort kann die Einstell-Operation nicht durchgeführt werden.

Feld	Beschreibung
Letztes Schreibergebnis	<p>Der Wert dieses Feldes kann nur gelesen werden.</p> <p>Zeigt das Ergebnis der letzten Einstell-Operation an.</p> <p>Mögliche Werte sind:</p> <ul style="list-style-type: none"> • <i>Kein Fehler</i>: Der Access-Point hat eine erfolgreiche Operation gemeldet oder es ist noch keine Konfigurationsänderung mit OK durchgeführt worden. • <i>Timeout</i>: Der Access-Point hat nicht geantwortet. • <i>Zugriff verweigert</i>: Der Access-Point hat einen Autorisierungsfehler gemeldet. Bitte überprüfen Sie das Authentifizierungspasswort. • <i>Ungültige IP-Parameter</i>: Es besteht ein Problem mit den vorgesehenen IP-Parametern (IP-Adresse, Netzmaske oder Gateway-Adresse). • <i>Destination Unreachable</i>: Der Access-Point kann aus internen Gründen nicht erreicht werden (z. B. die Schnittstelle, an die der Access-Point angeschlossen ist, ist außer Betrieb). Zum Access-Point kann keine Einstellanforderung gesandt werden. • <i>Anderer Fehler</i>: Der Access-Point antwortet auf die Einstellanforderung mit einem unerwarteten oder unspezifischen Fehler. • <i>Interner Fehler</i>: Ein internes Problem Ihres Geräts hat die Einstelloperation verhindert.

18.7.2 Optionen

In diesem Menü können Sie die Erlaubnis erteilen, dass auch Ihr Gerät von anderen Teldat-Geräten mittels Teldat Discovery Protokoll gefunden und über dieses konfiguriert werden kann.



Abb. 183: Lokale Dienste->Teldat Discovery->Optionen

Das Menü **Lokale Dienste->Teldat Discovery->Optionen** besteht aus folgenden Feldern:

Felder im Menü Discovery Server Optionen

Feld	Beschreibung
Discovery Server freigeben	<p>Wählen Sie aus, ob Ihr Gerät im Netzwerk von anderen Teldat-Geräten erkannt und konfiguriert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

18.8 Hotspot-Gateway

Die **Hotspot Solution** ermöglicht die Bereitstellung von öffentlichen Internetzugängen (mittels WLAN oder kabelgebundenem Ethernet). Die Lösung ist geeignet zum Aufbau kleinerer und größerer Hotspot-Lösungen für Cafes, Hotels, Unternehmen, Wohnheime, Campingplätze usw.

Die **Hotspot Solution** besteht aus einem vor Ort installierten Teldat Gateway (mit eigenem WLAN Access Point oder zusätzlich angeschlossenem WLAN-Gerät oder kabelgebundenem LAN) und aus dem Hotspot Server, der zentral in einem Rechenzentrum steht. Über ein Administrations-Terminal (z. B. dem Rezeptions-PC im Hotel) wird das Betreiber-Konto auf dem Server verwaltet, wie z. B. Erfassung von Registrierungen, Erzeugung von Tickets, statistische Auswertung usw.

Ablauf der Anmeldeprozedur am Hotspot Server

- Wenn sich ein neuer Benutzer mit dem Hotspot verbindet, bekommt er über DHCP automatisch eine IP-Adresse zugewiesen.
- Sobald er versucht, eine beliebige Internetseite mit seinem Browser zu öffnen, wird der Benutzer auf die Start/Login-Seite umgeleitet.
- Nachdem der Benutzer die Anmeldedaten (Benutzer/Passwort) eingegeben hat, werden diese als RADIUS-Anmeldung an den zentralen RADIUS-Server (Hotspot Server) geschickt.
- Nach erfolgreicher Anmeldung gibt das Gateway den Internetzugang frei.
- Das Gateway sendet für jeden Benutzer regelmäßig Zusatzinformationen an den RADIUS-Server, um Accounting-Daten zu erfassen.
- Nach Ablauf des Tickets wird der Benutzer automatisch abgemeldet und wieder auf die Start/Login-Seite umgeleitet.

Voraussetzungen

Um einen Hotspot betreiben zu können, benötigt der Kunde:

- ein Teldat Gerät als Hotspot-Gateway mit einem aktiven Internetzugang und konfigurierten Hotspot Server Einträgen für Login und Accounting (siehe Menü **Systemverwaltung** -> **Remote Authentifizierung** -> **RADIUS** -> **Neu mit Gruppenbeschreibung** *Standard-gruppe 0*)
- Teldat Hotspot Hosting (Artikelnummer 5510000198 bzw. 5510000197)
- Zugangsdaten
- Dokumentation
- Software-Lizenzierung

Beachten Sie bitte, dass Sie die Lizenz zuerst freischalten müssen.

- Gehen Sie auf www.teldat.de zu **Service/Support** -> **Services** -> **Online Services**.

- Tragen Sie die erforderlichen Daten ein (beachten Sie dazu die Erläuterung auf dem Lizenzblatt) und folgen Sie den Anweisungen der Online-Lizenzierung.

- Sie erhalten daraufhin die Login-Daten des Hotspot Servers.



Hinweis

Die Freischaltung kann etwa 2-3 Werktage in Anspruch nehmen.

Zugangsdaten zur Konfiguration des Gateways

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Wird von Teldat GmbH festgelegt
Domain	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Network	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Walled Garden Server URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt
Terms & Condition URL	Wird kundenindividuell vom Kunden/Fachhändler festgelegt

Zugangsdaten zur Konfiguration des Hotspot Servers

Admin URL	https://hotspot.teldat.de/
Username	Wird durch Teldat individuell festgelegt
Password	Wird durch Teldat individuell festgelegt



Hinweis

Beachten Sie auch den WLAN Hotspot Workshop der Ihnen auf www.teldat.de zum Download zur Verfügung steht.

18.8.1 Hotspot-Gateway

Im Menü **Hotspot-Gateway** konfigurieren Sie das vor Ort installierte Teldat Gateway für die **Hotspot Solution**.

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller konfigurierter Hotspot Netzwerke angezeigt.



Abb. 184: Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway

Mit der Option **Aktiviert** können Sie den entsprechenden Eintrag aktivieren oder deaktivieren.

18.8.1.1 Bearbeiten oder Neu

Im Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->** konfigurieren Sie die Hotspot Netzwerke. Wählen Sie die Schaltfläche **Neu**, um weitere Hotspot Netzwerke einzurichten.

Hotspot-Gateway Optionen

Basisparameter	
Schnittstelle	LAN_EN1-0
Domäne am Hotspot-Server	
Walled Garden	<input type="checkbox"/> Aktiviert
Sprache für Anmeldefenster	English

Erweiterte Einstellungen


Tickettyp	Benutzername/Passwort
Zulässiger Hotspot-Client	Alle
Anmeldefenster	<input checked="" type="checkbox"/> Aktiv
Pop-Up-Fenster für Statusanzeige	<input checked="" type="checkbox"/> Aktiviert
Standard-Timeout bei Inaktivität	<input type="text" value="600"/> Sekunden

OK Abbrechen

Abb. 185: Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway-> 

Das Menü **Lokale Dienste->Hotspot-Gateway->Hotspot-Gateway->**  besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Schnittstelle	<p>Wählen Sie die Schnittstelle aus, an der das Hotspot LAN oder WLAN angeschlossen ist. Bei Betrieb über LAN tragen Sie hier die Ethernet-Schnittstelle ein (z. B. die en1-0). Bei Betrieb über WLAN muss die WLAN-Schnittstelle ausgewählt werden, an der der Access Point angeschlossen ist.</p>
	<p> Achtung</p> <p>Die Konfiguration Ihres Gerätes ist aus Sicherheitsgründen nicht über eine Schnittstelle möglich, die für den Hotspot konfiguriert ist. Wählen Sie hier daher sorgfältig die Schnittstelle aus, die Sie für den Hotspot nutzen wollen!</p> <p>Wenn Sie hier die Schnittstelle auswählen, über die die aktuelle Konfigurationssitzung stattfindet, geht die aktuelle Verbindung verloren. Sie müssen sich dann über eine erreichbare, nicht für den Hotspot konfigurierte Schnittstelle</p>

Feld	Beschreibung
	zur weiteren Konfiguration Ihres Geräts erneut anmelden.
Domäne am Hotspot-Server	Geben Sie den Domännennamen ein, der bei der Einrichtung des Hotspot Servers für diesen Kunden verwendet wurde. Ein Domänenname wird benötigt, damit der Hotspot Server die verschiedenen Mandanten (Kunden) unterscheiden kann.
Walled Garden	<p>Aktivieren Sie diese Funktion, wenn Sie einen abgegrenzten und kostenfreien Bereich von Webseiten (Intranet) definieren wollen.</p> <p>Standardmäßig ist die Funktion deaktiviert.</p>
Walled Network / Netzmaske	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Geben Sie die Netzadresse des Walled Network und die entsprechende Netzmaske des Intranet-Servers ein.</p> <p>Für den aus Walled Network / Netzmaske resultierenden Adressraum benötigen die Clients keine Authentifizierung.</p> <p>Beispiel: Geben Sie 192.168.0.0 / 255.255.255.0 ein, sind alle IP-Adressen von 192.168.0.0 bis 19.168.0.255 frei. Geben Sie 192.168.0.1 / 255.255.255.255 ein, ist nur die IP-Adresse 192.168.0.1 frei.</p>
Walled Garden URL	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Geben Sie die Walled Garden URL des Intranet-Servers ein. Frei zugängliche Webseiten müssen über diese Adresse erreichbar sein.</p>
Geschäftsbedingungen	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Tragen Sie in das Eingabefeld Geschäftsbedingungen die Adresse der AGB's auf dem Intranet-Server bzw. auf einem öffentlichen Server ein, z. B. http://www.webserver.de/agb.htm. Die Seite muss im Adressraum des Walled Garden-Networks liegen.</p>
Zusätzliche, freizugängliche Domännennamen	<p>Nur wenn Walled Garden aktiviert ist.</p> <p>Fügen Sie mit Hinzufügen weitere URLs oder IP-Adressen hin-</p>

Feld	Beschreibung
	zu. Die Webseiten sind über diese zusätzlichen frei zugänglichen Adressen erreichbar.
Sprache für Anmeldefenster	<p>Hier können Sie die Sprache für die Start/Login-Seite auswählen.</p> <p>Folgende Sprachen werden unterstützt: <i>English, Deutsch, Italiano, Français, Español, Português</i> und <i>Netherlands</i>.</p> <p>Die Sprache kann auf der Start/Login-Seite selbst jederzeit umgeschaltet werden.</p>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
Tickettyp	<p>Wählen Sie den Tickettyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Voucher</i>: Nur der Benutzername muss eingegeben werden. Definieren Sie im Eingabefeld ein Standardpasswort. • <i>Benutzername/Passwort</i> (Standardwert): Benutzername und Passwort müssen eingegeben werden.
Zulässiger Hotspot-Client	<p>Hier legen Sie fest, welche Art von Benutzern sich am Hotspot anmelden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i>: Alle Clients werden zugelassen. • <i>DHCP-Client</i>: Verhindert die Anmeldung von Benutzern, die keine IP-Adresse mittels DHCP erhalten haben.
Anmeldefenster	<p>Aktivieren oder deaktivieren Sie das Anmeldefenster.</p> <p>Das Anmeldefenster auf der HTML-Startseite besteht aus zwei Frames.</p> <p>Wenn die Funktion aktiviert ist, wird auf der linken Seite das Anmelde-Formular angezeigt.</p> <p>Wenn die Funktion deaktiviert ist, wird nur die Webseite mit In-</p>

Feld	Beschreibung
	formationen, Werbung und/oder Links zu frei zugänglichen Webseiten angezeigt. Standardmäßig ist die Funktion aktiv.
Pop-Up-Fenster für Statusanzeige	Legen Sie fest, ob das Gerät Pop-Up-Fenster zur Statusanzeige verwendet. Standardmäßig ist die Funktion aktiv.
Standard-Timeout bei Inaktivität	Aktivieren oder deaktivieren Sie den Standard-Timeout bei Inaktivität Wenn ein Hotspot-Benutzer für einen einstellbaren Zeitraum keinen Datenverkehr verursacht, wird er vom Hotspot abgemeldet. Standardmäßig ist die Funktion aktiv. Standardwert ist 600 Sekunden.

18.8.2 Optionen

Im Menü **Lokale Dienste->Hotspot-Gateway->Optionen** werden allgemeine Einstellungen für den Hotspot vorgenommen.

Abb. 186: Lokale Dienste->Hotspot-Gateway->Optionen

Das Menü **Lokale Dienste->Hotspot-Gateway->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Host für mehrere Standorte	Wenn für einen Kunden auf dem Hotspot Server mehrere Standorte (Filialen) eingerichtet wurden, geben Sie hier den Wert des NAS-Identifiers (RADIUS-Server Parameter) ein, der für diesen Standort auf dem Hotspot Server eingetragen wurde.

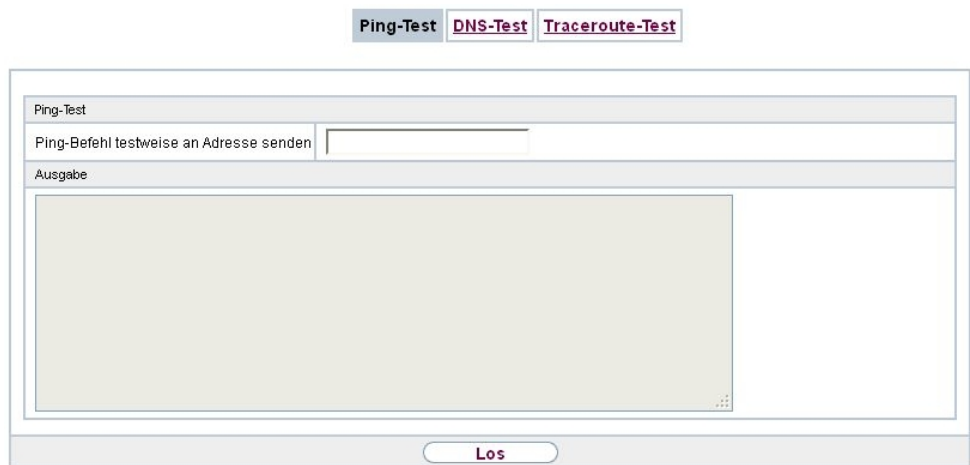
Kapitel 19 Wartung

Im diesem Menü werden Ihnen zahlreiche Funktionen zur Wartung Ihres Geräts zur Verfügung gestellt. So finden Sie zunächst eine Menü zum Testen der Erreichbarkeit innerhalb des Netzwerks. Sie haben die Möglichkeit Ihre Systemkonfigurationsdateien zu verwalten. Falls aktuellere Systemsoftware zur Verfügung steht, kann die Installation über dieses Menü vorgenommen werden. Falls Sie weitere Sprachen der Konfigurationsoberfläche benötigen, können Sie diese importieren. Auch ein System-Neustart kann in diesem Menü ausgelöst werden.

19.1 Diagnose

Im Menü **Wartung**->**Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

19.1.1 Ping-Test

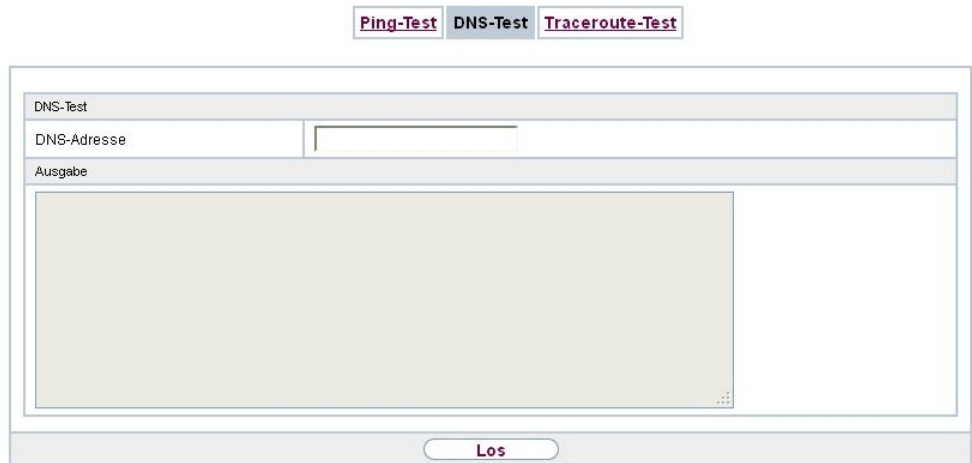


The screenshot shows a web-based interface for network diagnostics. At the top, there are three buttons: "Ping-Test" (highlighted in blue), "DNS-Test", and "Traceroute-Test". Below these is a form titled "Ping-Test". It contains a label "Ping-Befehl testweise an Adresse senden" followed by an empty text input field. Below the input field is a label "Ausgabe" followed by a large, empty rectangular area for displaying test results. At the bottom of the form is a button labeled "Los".

Abb. 187: **Wartung**->**Diagnose**->**Ping-Test**

Mit dem Ping-Test können Sie überprüfen, ob ein bestimmter Host im LAN oder eine Internetadresse erreichbar sind. Das **Ausgabe**-Feld zeigt die Meldungen des Ping-Tests an. Durch Eingabe der IP-Adresse, die getestet werden soll, in **Ping-Befehl testweise an Adresse senden** und Klicken auf die **Los**-Schaltfläche wird der Ping-Test gestartet.

19.1.2 DNS-Test



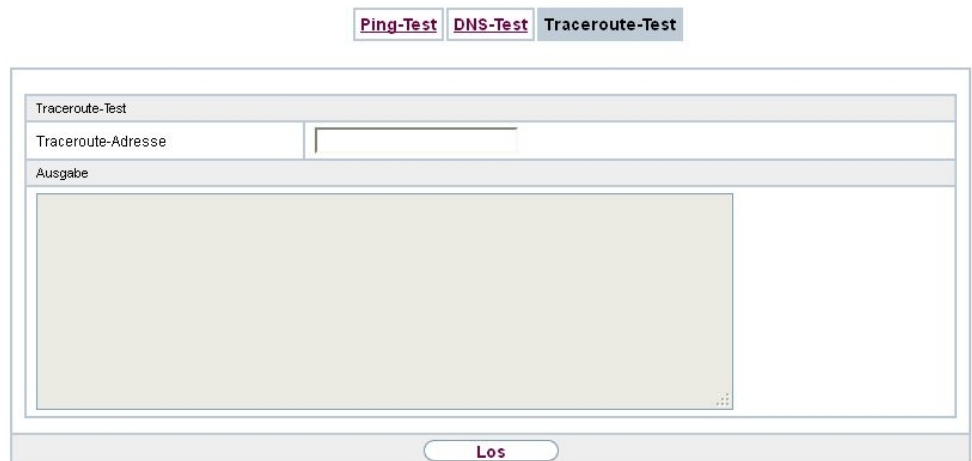
The screenshot shows a web interface for a network management tool. At the top, there are three tabs: "Ping-Test", "DNS-Test", and "Traceroute-Test". The "DNS-Test" tab is selected. Below the tabs, there is a form with the following sections:

- DNS-Test**: A header section.
- DNS-Adresse**: A text input field for entering a domain name.
- Ausgabe**: A large, empty text area for displaying the test results.
- Los**: A button to execute the test.

Abb. 188: **Wartung->Diagnose->DNS-Test**

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domänennamens, der getestet werden soll, in **DNS-Adresse** und Klicken auf die **Los**-Schaltfläche wird der DNS-Test gestartet.

19.1.3 Traceroute-Test



The screenshot shows a web interface for a network management tool. At the top, there are three tabs: "Ping-Test", "DNS-Test", and "Traceroute-Test". The "Traceroute-Test" tab is selected. Below the tabs, there is a form with the following sections:

- Traceroute-Test**: A header section.
- Traceroute-Adresse**: A text input field for entering a domain name.
- Ausgabe**: A large, empty text area for displaying the test results.
- Los**: A button to execute the test.

Abb. 189: **Wartung->Diagnose->Traceroute-Test**

Mit dem Traceroute-Test können Sie die Route zu einer bestimmten Adresse (IP-Adresse oder Domänenname) anzeigen lassen, sofern diese erreichbar ist. Das **Ausgabe**-Feld zeigt die Meldungen des Traceroute-Tests an. Durch Eingabe der Adresse, die getestet werden soll, in **Traceroute-Adresse** und Klicken auf die **Los**-Schaltfläche wird der Traceroute-Test gestartet.

19.2 Software & Konfiguration

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **GUIs** verwalten.

19.2.1 Optionen

Ihr Gerät ist mit der zum Zeitpunkt der Fertigung verfügbaren Version der Systemsoftware ausgestattet, von der es aktuell ggf. neuere Versionen gibt. Daher müssen Sie gegebenenfalls ein Software-Update durchführen.

Jede neue Systemsoftware beinhaltet neue Funktionen, bessere Leistung und bei Bedarf Fehlerkorrekturen der vorhergehenden Version. Die aktuelle Systemsoftware finden Sie unter www.teldat.de. 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 Teldat GmbH eine explizite Empfehlung dazu ausspricht.

Flash

Ihr Gerät speichert seine Konfiguration in Konfigurationsdateien im Flash EEPROM (electrically erasable programmable read-only memory). Auch wenn Ihr Gerät ausgeschaltet ist, bleiben die Daten im Flash gespeichert.

RAM

Im Arbeitsspeicher (RAM) befindet sich die aktuelle Konfiguration und alle Änderungen, die Sie während des Betriebes auf Ihrem Gerät einstellen. Der Inhalt des RAM geht verloren, wenn Ihr Gerät ausgeschaltet wird. Wenn Sie Ihre Konfiguration ändern und diese Änderungen auch beim nächsten Start Ihres Geräts beibehalten wollen, müssen Sie die geänderte Konfiguration im Flash speichern: Schaltfläche **Konfiguration speichern** über dem Navigationsbereich des **GUIs**. Dadurch wird die Konfiguration in eine Datei mit dem Namen *boot* im Flash gespeichert. Beim Starten Ihres Geräts wird standardmäßig die Konfigurationsdatei *boot* verwendet.

Aktionen

Die Dateien im Flash-Speicher können kopiert, verschoben, gelöscht und neu angelegt werden. Es ist auch möglich, Konfigurationsdateien zwischen Ihrem Gerät und einem Host per HTTP zu transferieren.

Format von Konfigurationsdateien

Das Dateiformat der Konfigurationsdatei erlaubt eine Verschlüsselung und stellt die Kompatibilität beim Zurückspielen der Konfiguration auf das Gateway in unterschiedliche Versionen der Systemsoftware sicher. Es handelt sich um ein CSV-Format; es kann problemlos gelesen und modifiziert werden. Außerdem können Sie z. B. mithilfe von Microsoft Excel die entsprechenden Dateien in übersichtlicher Form einsehen. Sicherungsdateien der Konfiguration können vom Administrator verschlüsselt abgelegt werden. Bei Versand der Konfiguration per E-Mail (z. B. für Supportzwecke) können vertrauliche Konfigurationsdaten bei Bedarf komplett geschützt werden. So können Sie mit den Aktionen "Konfiguration exportieren", "Konfiguration mit Statusinformationen exportieren" und "Konfiguration laden" Dateien sichern bzw. einspielen. Wenn Sie mit der Aktion "Konfiguration exportieren" oder "Konfiguration mit Statusinformationen exportieren" eine Konfigurationsdatei sichern wollen, können Sie bestimmen, ob die Konfigurationsdatei unverschlüsselt oder verschlüsselt gespeichert werden soll.



Achtung

Sollten Sie über die SNMP-Shell mit dem Kommando `put` eine Konfigurationsdatei in einem alten Format gesichert haben, kann ein Wiedereinspielen auf das Gerät nicht garantiert werden. Daher wird das alte Format nicht mehr empfohlen.

Optionen

Aktuell Installierte Software	
BOSS	V.9.1 Rev. 2 IPSec from 2012/03/23 00:00:00
Systemlogik	1.0
ADSL-Logik	2.1.4.7.0.2
Optionen zu Software und Konfiguration	
Aktion	Keine Aktion <input type="button" value="v"/>

Abb. 190: **Wartung->Software &Konfiguration ->Optionen**

Das Menü **Wartung->Software &Konfiguration ->Optionen** besteht aus folgenden Feldern:

Felder im Menü Aktuell Installierte Software

Feld	Beschreibung
BOSS	Zeigt die aktuelle Softwareversion an, die auf Ihrem Gerät geladen ist.
Systemlogik	Zeigt die aktuelle Systemlogik an, die auf Ihrem Gerät geladen ist.
ADSL-Logik	Zeigt die aktuelle Version der ADSL-Logik an, die auf Ihrem Gerät geladen ist.

Felder im Menü Optionen zu Software und Konfiguration

Feld	Beschreibung
Aktion	<p>Wählen Sie die Aktion aus, die Sie ausführen möchten.</p> <p>Nach Durchführung der jeweiligen Aufgabe erhalten Sie ein Fenster, in dem Sie auf die weiteren nötigen Schritte hingewiesen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine Aktion</i> (Standardwert): • <i>Konfiguration exportieren</i>: Die Konfigurationsdatei Aktueller Dateiname im Flash wird zu Ihrem lokalen Host transferiert. Wenn Sie die Los-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Konfiguration importieren</i>: Wählen Sie in Dateiname eine Konfigurationsdatei aus, die sie importieren wollen. Hinweis: Durch Klicken auf Los wird die Datei zunächst unter dem Namen <i>boot</i> in den Flash-Speicher des Geräts geladen. Zum Aktivieren müssen Sie das Gerät neu starten. Hinweis: Die Datei, die importiert werden soll, muss das CSV-Format haben! • <i>Konfiguration kopieren</i>: Die Konfigurationsdatei im Feld Name der Quelldatei wird als Name der Zieldatei gespeichert. • <i>Konfiguration löschen</i>: Die Konfiguration im Feld Datei auswählen wird gelöscht. • <i>Konfiguration umbenennen</i>: Die Konfigurationsdatei im Feld Datei auswählen wird zu Neuer Dateiname umbenannt. • <i>Sicherung wiederherstellen</i>: Nur, wenn unter Konfiguration speichern mit der Einstellung <i>Konfiguration speichern und vorhergehende Boot-Konfiguration sichern</i> die aktuelle Konfiguration als Boot-Konfiguration gespeichert und zusätzlich die vorhergehende Boot-Konfiguration archiviert wurde. Sie können die archivierte Boot-Konfiguration wieder einspielen. • <i>Software/Firmware löschen</i>: Die Datei im Feld Datei auswählen wird gelöscht. • <i>Sprache importieren</i>: Sie können weitere Sprachversionen des GUI auf Ihr Gerät einspielen. Die Dateien können Sie aus dem Download-Bereich von www.teldat.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> (Wird nur angezeigt, wenn eine SD-Karte gesteckt ist.): Wählen Sie in Dateiname die Datei <i>vms_wavfiles.zip</i> aus, die Sie importieren wollen. • <i>Konfiguration mit Statusinformationen exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie auf die Los-Schaltfläche klicken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten

Feld	Beschreibung
	Dateinamen eingeben können.
Aktueller Dateiname im Flash	Für Aktion = <i>Konfiguration exportieren</i> Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.
Zertifikate und Schlüssel einschließen	Für Aktion = <i>Konfiguration exportieren</i> Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Verschlüsselung der Konfiguration	Nur für Aktion = <i>Konfiguration exportieren, Konfiguration importieren, Konfiguration mit Statusinformationen exportieren</i> Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv. Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Passwort eingeben.
Dateiname	Nur für Aktion = <i>Konfiguration importieren, Sprache importieren, Systemsoftware aktualisieren</i> Geben Sie den Dateipfad und Namen der Datei ein oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.
Name der Quelldatei	Nur für Aktion = <i>Konfiguration kopieren</i> Wählen Sie die Quelldatei aus, die kopiert werden soll.
Name der Zieldatei	Nur für Aktion = <i>Konfiguration kopieren</i> Geben Sie den Namen der Kopie ein.
Datei auswählen	Nur für Aktion = <i>Konfiguration löschen, Konfigurati-</i>

Feld	Beschreibung
	<p><i>on umbenennen</i> oder <i>Software/Firmware löschen</i></p> <p>Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.</p>
Neuer Dateiname	<p>Nur für Aktion = <i>Konfiguration umbenennen</i></p> <p>Geben Sie den neuen Namen der Konfigurationsdatei ein.</p>
Quelle	<p>Nur für Aktion = <i>Systemsoftware aktualisieren</i></p> <p>Wählen Sie die Quelle der Aktualisierung aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Lokale Datei</i> (Standardwert): Die Systemsoftware-Datei ist lokal auf Ihrem PC gespeichert. • <i>HTTP-Server</i>: Die Datei ist auf dem entfernten Server gespeichert, der in der URL angegeben wird. • <i>Aktuelle Software vom Teldat-Server</i>: Die Datei liegt auf dem offiziellen Teldat-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>

19.3 Neustart

19.3.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **GUI** neu aufrufen und sich wieder anmelden.

Beobachten Sie dazu die LEDs an Ihrem Gerät. Für die Bedeutung der LEDs lesen Sie bitte in dem Handbuch-Kapitel **Technische Daten**.

**Hinweis**

Stellen Sie vor einem Neustart sicher, dass Sie Ihre Konfigurationsänderungen durch Klicken auf die Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.



Abb. 191: **Wartung->Neustart->Systemneustart**

Wenn Sie Ihr Gerät neu starten wollen, klicken Sie auf die **OK**-Schaltfläche. Der Neustart wird ausgeführt.

Kapitel 20 Externe Berichterstellung

In diesem Menü legen Sie fest, welche Systemprotokoll-Nachrichten auf welchem Rechner gespeichert werden und ob der Systemadministrator bei bestimmten Ereignissen eine Email erhalten soll. Informationen über den IP-Datenverkehr können - bezogen auf die einzelnen Schnittstellen - ebenfalls gespeichert werden. Darüber hinaus können im Fehlerfall SNMP-Traps an bestimmte Hosts versandt werden. Außerdem können Sie Ihr Gerät für die Überwachung mit dem Activity Monitor vorbereiten.

20.1 Systemprotokoll

Ereignisse in den verschiedenen Subsystemen Ihres Geräts (z. B. PPP) werden in Form von Systemprotokoll-Nachrichten (Syslog) protokolliert. Je nach eingestelltem Level (acht Stufen von *Notfall* über *Informationen* bis *Debug*) werden dabei mehr oder weniger Meldungen sichtbar.

Zusätzlich zu den intern auf Ihrem Gerät protokollierten Daten können und sollten alle Informationen zur Speicherung und Weiterverarbeitung zusätzlich an einen oder mehrere externe Rechner weitergeleitet werden, z. B. an den Rechner des Systemadministrators. Auf Ihrem Gerät intern gespeicherte Systemprotokoll-Nachrichten gehen bei einem Neustart verloren.



Warnung

Achten Sie darauf, die Systemprotokoll-Nachrichten nur an einen sicheren Rechner weiterzuleiten. Kontrollieren Sie die Daten regelmäßig und achten Sie darauf, dass jederzeit ausreichend freie Kapazität auf der Festplatte des Rechners zur Verfügung steht.

Syslog-Daemon

Die Erfassung der Systemprotokoll-Nachrichten wird von allen Unix-Betriebssystemen unterstützt. Für Windows-Rechner ist in den **DIME Tools** ein Syslog-Daemon enthalten, der die Daten aufzeichnen und je nach Inhalt auf verschiedene Dateien verteilen kann (abrufbar im Download-Bereich unter www.teldat.de).

20.1.1 Syslog-Server

Konfigurieren Sie Ihr Gerät als Syslog-Server, sodass die definierten Systemmeldungen an geeignete Hosts im LAN geschickt werden können.

In diesem Menü definieren Sie, welche Meldungen mit welchen Bedingungen zu welchem Host geschickt werden.

Im Menü **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** wird eine Liste aller konfigurierten Systemprotokoll-Server angezeigt.

20.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.

Syslog-Server

Basisparameter	
IP-Adresse	<input type="text"/>
Level	Informationen <input type="button" value="v"/>
Facility	local0 <input type="button" value="v"/>
Zeitstempel	<input checked="" type="radio"/> Keiner <input type="radio"/> Zeit <input type="radio"/> Datum & Uhrzeit
Protokoll	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
Nachrichtentyp	<input type="radio"/> System <input type="radio"/> Accounting <input checked="" type="radio"/> System & Accounting
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 192: **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** -> **Neu**

Das Menü **Externe Berichterstellung** -> **Systemprotokoll** -> **Syslog-Server** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, zu dem Systemprotokoll-Nachrichten weitergeleitet werden sollen.
Level	Wählen Sie die Priorität der Systemprotokoll-Nachrichten aus, die zum Host geschickt werden sollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität)

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Informationen</i> (Standardwert) • <i>Debug</i> (niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden an den Host gesendet, d. h. dass beim Syslog-Level <i>Debug</i> sämtliche erzeugten Meldungen an den Host weitergeleitet werden.</p>
Facility	<p>Geben Sie die Syslog Facility auf dem Host an.</p> <p>Dieses ist nur erforderlich, wenn der Log Host ein Unix-Rechner ist.</p> <p>Mögliche Werte: <i>local0</i> - 7 (Standardwert)</p> <p><i>local0</i>.</p>
Zeitstempel	<p>Wählen Sie das Format des Zeitstempels im Systemprotokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Keine Systemzeitangabe. • <i>Zeit</i>: Systemzeit ohne Datum. • <i>Datum & Uhrzeit</i>: Systemzeit mit Datum.
Protokoll	<p>Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>UDP</i> (Standardwert) • <i>TCP</i>
Nachrichtentyp	<p>Wählen Sie den Nachrichtentyp aus.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System & Accounting</i> (Standardwert) • <i>System</i> • <i>Accounting</i>

20.2 IP-Accounting

In modernen Netzwerken werden häufig aus kommerziellen Gründen Informationen über Art und Menge der Datenpakete gesammelt, die über die Netzwerkverbindungen übertragen und empfangen werden. Für Internet Service Provider, die ihre Kunden nach Datenvolumen abrechnen, ist das von entscheidender Bedeutung.

Aber auch nicht-kommerzielle Zwecke sprechen für ein detailliertes Netzwerk-Accounting. Wenn Sie z. B. einen Server verwalten, der verschiedene Arten von Netzwerkdiensten zur Verfügung stellt, ist es nützlich für Sie zu wissen, wieviel Daten von den einzelnen Diensten erzeugt werden.

Ihr Gerät enthält die Funktion IP-Accounting, die Ihnen die Sammlung vielerlei nützlicher Informationen über den IP-Netzwerkverkehr (jede einzelne IP-Session) ermöglicht.

20.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

The screenshot shows a web interface with two tabs: 'Schnittstellen' (selected) and 'Optionen'. Below the tabs is a control bar with 'Ansicht' set to '20 pro Seite', 'Filtern in' set to 'Keiner', and a search field containing 'gleich'. A 'Los' button is also present. The main area contains a table with two rows of interface configurations. The first row is for interface 'en1-4' and the second for 'en1-0'. Each row has a checkbox in the 'IP-Accounting' column, both of which are currently unchecked. Above the table, there are links for 'Alle auswählen' and 'Alle deaktivieren'. At the bottom of the table, it says 'Seite: 1, Objekte: 1 - 2'. Below the table are 'OK' and 'Abbrechen' buttons.

Nr.	Schnittstelle	IP-Accounting
1	en1-4	<input type="checkbox"/>
2	en1-0	<input type="checkbox"/>

Abb. 193: Externe Berichterstellung -> IP-Accounting -> Schnittstellen

Im Menü **Externe Berichterstellung -> IP-Accounting -> Schnittstellen** wird eine Liste aller auf Ihrem Gerät konfigurierten Schnittstellen angezeigt. Für jeden Eintrag kann durch Setzen eines Hakens die Funktion IP-Accounting aktiviert werden. In der Spalte **IP-**

Accounting müssen Sie nicht jeden Eintrag einzeln anklicken. Über die Optionen **Alle auswählen** oder **Alle deaktivieren** können Sie die Funktion IP-Accounting für alle Schnittstellen gleichzeitig aktivieren bzw. deaktivieren.

20.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

The screenshot shows a dialog box titled 'Optionen' with a tab labeled 'Schnittstellen'. Inside the dialog, there is a text input field labeled 'Protokollformat' containing the text 'INET: %d %t %a %c %i:%r%f-> %l:%R/%F %p %o %P %O [%s]'. At the bottom of the dialog, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 194: Externe Berichterstellung ->IP-Accounting->Optionen

Im Menü **Externe Berichterstellung ->IP-Accounting->Optionen** können Sie das **Protokollformat** der IP-Accounting-Meldungen festlegen. Die Meldungen können Zeichenketten in beliebiger Reihenfolge, durch umgekehrten Schrägstrich abgetrennte Sequenzen, z. B. `\t` oder `\n` oder definierte Tags enthalten.

Mögliche Format-Tags:

Format-Tags für IP-Accounting Meldungen

Feld	Beschreibung
%d	Datum des Sitzungsbeginns im Format DD.MM.YY
%t	Uhrzeit des Sitzungsbeginns im Format HH:MM:SS
%a	Dauer der Sitzung in Sekunden
%c	Protokoll
%i	Quell-IP-Adresse
%r	Quellport
%f	Quell-Schnittstellen-Index
%l	Ziel-IP-Adresse
%R	Zielport
%F	Ziel-Schnittstellen-Index
%p	Ausgegangene Pakete
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts

Feld	Beschreibung
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen:

```
INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

20.3 Benachrichtigungsdienst

Bisher war es schon möglich Syslog-Meldungen vom Router an einen beliebigen Syslog-Host übertragen zu lassen. Mit dem Benachrichtigungsdienst werden dem Administrator je nach Konfiguration E-Mails gesendet, sobald relevante Syslog-Meldungen auftreten.

20.3.1 Benachrichtigungsempfänger

Im Menü **Benachrichtigungsempfänger** wird eine Liste der Syslog-Meldungen angezeigt.

20.3.1.1 Neu

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

Benachrichtigungsempfänger Benachrichtigungseinstellungen

Benachrichtigungsempfänger hinzufügen/bearbeiten	
Benachrichtigungsdienst	E-Mail
Empfänger	<input type="text"/>
Nachrichtenkomprimierung	<input checked="" type="checkbox"/> Aktiviert
Betreff	<input type="text"/>
Ereignis	Systemmeldung enthält Zeichenfolge ▼
Enthaltene Zeichenfolge	<input type="text"/> (Wildcards zulässig)
Schweregrad	Notfall ▼
Überwachte Subsysteme	<div style="border: 1px solid gray; padding: 2px;"> Subsystem <input type="text"/> <input type="button" value="Hinzufügen"/> </div>
Timeout für Nachrichten	<input type="text" value="60"/>
Anzahl Nachrichten	<input type="text" value="1"/>

Abb. 195: Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungsempfänger -> Neu

Das Menü **Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungs-**

empfänger->Neu besteht aus folgenden Feldern:

Felder im Menü **Benachrichtigungsempfänger hinzufügen/bearbeiten**

Feld	Beschreibung
Benachrichtigungsdienst	<p>Zeigt den Benachrichtigungsdienst an. Für Geräte der Serien RS120wu, RS230au+ und RS230bu+ können Sie den Benachrichtigungsdienst auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • E-Mail • SMS
Empfänger	<p>Geben Sie die E-Mail-Adresse bzw. die Mobilfunknummer des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.</p>
Nachrichtenkomprimierung	<p>Wählen Sie aus, ob der Text der Benachrichtigungsmail verkürzt werden soll. Die Mail enthält dann die Syslog-Meldung nur einmal und zusätzlich die Anzahl der entsprechenden Ereignisse.</p> <p>Aktivieren oder deaktivieren Sie das Feld.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Betreff	<p>Sie können einen Betreff eingeben.</p>
Ereignis	<p>Diese Funktion ist nur bei Geräten mit Wireless LAN Controller verfügbar.</p> <p>Wählen Sie das Ereignis, das eine E-Mail-Benachrichtigung auslösen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Systemmeldung enthält Zeichenfolge</i> (Standardwert): Eine Syslog-Meldung enthält eine bestimmte Zeichenfolge. • <i>Neuer Neighbor-AP gefunden</i>: Ein neuer benachbarter AP wurde gefunden. • <i>Neuer Rogue-AP gefunden</i>: Ein neuer Rough AP wurde gefunden, d.h. ein AP, der eine SSID des eigenen Netzes verwendet, aber kein Bestandteil dieses Netzes ist. • <i>Neuer Slave-AP (WTP) gefunden</i>: Eine neuer unkonfiguriertes AP hat sich beim WLAN Controller gemeldet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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, Informationen, Debug</i></p>
Überwachte Subsysteme	<p>Wählen Sie die Subsysteme aus, die überwacht werden sollen.</p> <p>Fügen Sie mit Hinzufügen neue Subsysteme hinzu.</p>
Timeout für Nachrichten	<p>Geben Sie ein, wie lange der Router nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Benachrichtigungsmails erzwungen wird.</p> <p>Zur Verfügung stehen Werte von 0 bis 86400. Ein Wert von 0 deaktiviert den Timeout. Standardwert ist 60.</p>
Anzahl Nachrichten	<p>Geben Sie die Anzahl der Syslog-Meldungen ein, die erreicht sein muss, ehe eine Benachrichtigungsmail für diesen Fall gesendet werden kann. Wenn Timeout konfiguriert ist, wird die Mail bei dessen Ablauf gesendet, auch wenn die Anzahl an Meldungen noch nicht erreicht ist.</p> <p>Zur Verfügung stehen Werte von 0 bis 99, Standardwert ist 1.</p>

20.3.2 Benachrichtigungseinstellungen

Benachrichtigungsempfänger
Benachrichtigungseinstellungen

Basisparameter	
Benachrichtigungsdienst	<input checked="" type="checkbox"/> Aktiviert
Maximale Nachrichtenzahl pro Minute	6 <small>▼</small>
E-Mail-Parameter	
E-Mail-Adresse	<input type="text"/>
SMTP-Server	<input type="text"/>
SMTP-Authentifizierung	<input checked="" type="radio"/> Keine <input type="radio"/> ESMTP <input type="radio"/> SMTP after POP

Abb. 196: Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungseinstellungen

Das Menü **Externe Berichterstellung -> Benachrichtigungsdienst -> Benachrichtigungseinstellungen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	Wählen Sie aus, ob der Benachrichtigungsdienst aktiviert werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Maximale E-Mails pro Minute	Begrenzen Sie die Anzahl der ausgehenden Mails pro Minute. Zur Verfügung stehen Werte von 1 bis 15, der Standardwert ist 6.

Felder im Menü E-Mail-Parameter

Feld	Beschreibung
E-Mail-Adresse des Senders	Geben Sie die Mailadresse ein, die in das Absenderfeld der E-Mail eingetragen werden soll.
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailservers ein, der zum Versenden der Mails verwendet werden soll.

Feld	Beschreibung
	Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Authentifizierung	<p>Authentifizierung, die der SMTP-Server erwartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Der Server akzeptiert und versendet Mails ohne weitere Authentifizierung. • <i>ESMTP</i>: Der Server akzeptiert Mails nur, wenn sich der Router mit einer richtigen Benutzer/Passwort-Kombination einloggt. • <i>SMTP after POP</i>: Der Server verlangt, dass vor dem Versenden einer Mail Mails per POP3 von der sendenden IP aus mit dem richtigen POP3-Benutzernamen/Passwort abgerufen werden.
Benutzername	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie den Benutzernamen für den POP3 bzw. SMTP Server an.</p>
Passwort	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie das Passwort dieses Benutzers an.</p>
POP3-Server	<p>Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i></p> <p>Geben Sie die Adresse des Servers ein, von dem die Mails abgerufen werden sollen.</p>
POP3-Timeout	<p>Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i></p> <p>Geben Sie ein, wie lange der Router nach dem POP3-Abruf maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird.</p> <p>Standardwert ist 600 Sekunden.</p>

Felder im Menü SMS Parameter (nur bei RS120wu, RS230au+ und RS230bu+)

Feld	Beschreibung
SMS-Gerät	Sie können sich über Systemmeldungen per SMS informieren

Feld	Beschreibung
	lassen. Wählen Sie das Gerät aus, das zum Versenden der SMS verwendet werden soll.
Maximale SMS pro Tag	<p>Begrenzen Sie hier die Anzahl der an einem Tag versendeten SMS.</p> <p>Die Aktivierung von <i>Uneingeschränkt</i> erlaubt eine beliebige Anzahl an versendeten SMS.</p> <p>Der Standardwert beträgt 10 SMS pro Tag.</p> <p>Hinweis: Die Eingabe des Wertes 0 ist gleichbedeutend mit der Aktivierung von <i>Uneingeschränkt</i>.</p>

20.4 SNMP

SNMP (Simple Network Management Protocol) ist ein Protokoll in der IP-Protokollfamilie für den Transport von Managementinformationen über Netzwerkkomponenten.

Zu den Bestandteilen eines jeden SNMP-Managementsystems zählt u. a. eine MIB. Über SNMP sind verschiedene Netzwerkkomponenten von einem System aus zu konfigurieren, zu kontrollieren und zu überwachen. Mit Ihrem Gerät haben Sie ein solches SNMP-Werkzeug erhalten, den Konfigurationsmanager. Da SNMP ein genormtes Protokoll ist, können Sie aber auch beliebige andere SNMP-Manager wie z. B. HPOpenView verwenden.

Weitergehende Informationen zu den SNMP-Versionen finden Sie in den entsprechenden RFCs und Drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

20.4.1 SNMP-Trap-Optionen

Zur Überwachung des Systems wird im Fehlerfall unaufgefordert eine Nachricht gesendet, ein sogenanntes Trap-Paket.

Im Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Optionen** können Sie das Senden von Traps konfigurieren.

SNMP-Trap-Optionen SNMP-Trap-Hosts

Basisparameter	
SNMP Trap Broadcasting	<input checked="" type="checkbox"/> Aktiviert
SNMP-Trap-UDP-Port	162
SNMP-Trap-Community	snmp-Trap

OK Abbrechen

Abb. 197: Externe Berichterstellung ->SNMP->SNMP-Trap-Optionen

Das Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
SNMP Trap Broadcasting	<p>Wählen Sie aus, ob die Übertragung von SNMP-Traps aktiviert werden soll.</p> <p>Ihr Gerät sendet SNMP-Traps dann an die Broadcast-Adresse des LANs.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
SNMP-Trap-UDP-Port	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p> <p>Geben Sie die Nummer des UDP-Ports ein, zu dem Ihr Gerät SNMP-Traps senden soll.</p> <p>Möglich ist jeder ganzzahlige Wert.</p> <p>Standardwert ist <i>162</i>.</p>
SNMP-Trap-Community	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p> <p>Geben Sie eine SNMP-Kennung ein. Diese muss vom SNMP-Manager mit jeder SNMP-Anforderung übergeben werden, damit sie von Ihrem Gerät akzeptiert wird.</p> <p>Möglich ist eine Zeichenkette mit <i>0</i> bis <i>255</i> Zeichen.</p> <p>Standardwert ist <i>SNMP-Trap</i>.</p>

20.4.2 SNMP-Trap-Hosts

In diesem Menü geben Sie an, an welche IP-Adressen Ihr Gerät die SNMP-Traps schicken soll.

Im Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Hosts** wird eine Liste aller konfigurierten SNMP-Trap-Hosts angezeigt.

20.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

Abb. 198: **Externe Berichterstellung ->SNMP->SNMP-Trap-Hosts->Neu**

Das Menü **Externe Berichterstellung ->SNMP->SNMP-Trap-Hosts->Neu** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

20.5 Activity Monitor

Im diesem Menü finden Sie die Einstellungen, die nötig sind, um Ihr Gerät mit dem Windows-Tool **Activity Monitor** (Bestandteil von **BRICKware** for Windows) überwachen zu können.

Zweck

Mit dem **Activity Monitor** können Windows-Nutzer die Aktivitäten ihres Geräts überwachen. Wichtige Informationen über den Status von physikalischen Schnittstellen (z. B. ISDN-Leitung) und virtuellen Schnittstellen sind leicht mit einem einzigen Tool erreichbar. Ein permanenter Überblick über die Auslastung der Schnittstellen Ihres Geräts ist damit

möglich.

Funktionsweise

Ein Status-Daemon sammelt Informationen über Ihr Gerät und überträgt sie in Form von UDP-Paketen zur Broadcast-Adresse der ersten LAN-Schnittstelle (Standardeinstellung) oder zu einer explizit eingetragenen IP-Adresse. Ein Paket pro Zeitintervall, das individuell einstellbar ist auf Werte von 1 - 60 Sekunden, wird gesendet. Bis zu 100 physikalische und virtuelle Schnittstellen können überwacht werden, soweit die Paketgröße von 4096 Bytes nicht überschritten wird. Der **Activity Monitor** auf Ihrem PC empfängt die Pakete und kann die enthaltenen Informationen je nach Konfiguration auf verschiedene Arten darstellen.

Um den **Activity Monitor** zu aktivieren, müssen Sie:

- das/die zu überwachende(n) Gerät(e) entsprechend konfigurieren
- die Windows-Anwendung auf Ihrem PC starten und konfigurieren (**BRICKware** for Windows, können Sie vom Download-Bereich auf www.teldat.de auf Ihren PC herunterladen und von da aus in Ihr Gerät einspielen).

20.5.1 Optionen

Optionen

Basisparameter	
Überwachte Schnittstellen	<input checked="" type="radio"/> Keine <input type="radio"/> Physikalisch <input type="radio"/> Physikalisch/WAN/VPN
Informationen senden an	Alle IP-Adressen (Broadcast) ▾
Aktualisierungsintervall	5 Sekunden
UDP-Zielport	2107
Passwort	••••••••
<input type="button" value="OK"/> <input type="button" value="Abbrechen"/>	

Abb. 199: Externe Berichterstellung ->Activity Monitor->Optionen

Das Menü **Externe Berichterstellung ->Activity Monitor->Optionen** besteht aus folgenden Feldern:

Felder im Menü Basisparameter

Feld	Beschreibung
Überwachte Schnittstellen	Wählen Sie die Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden soll.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Deaktiviert das Senden von Informationen an den Activity Monitor. • <i>Physikalisch</i>: Nur Informationen über physikalische Schnittstellen werden gesendet. • <i>Physikalisch/WAN/VPN</i>: Informationen über physikalische und virtuelle Schnittstellen werden gesendet.
Informationen senden an	<p>Wählen Sie aus, an wen Ihr Gerät die UDP Pakete schicken soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle IP-Adressen (Broadcast)</i> (Standardwert): Mit dem Standardwert <i>255.255.255.255</i> wird die Broadcast-Adresse der ersten LAN-Schnittstelle verwendet. • <i>Einzelner Host</i>: Die UDP-Pakete werden an die im nebenstehenden Eingabefeld eingetragene IP-Adresse geschickt.
Aktualisierungsintervall	<p>Geben Sie das Aktualisierungsintervall (in Sekunden) ein.</p> <p>Mögliche Werte sind <i>0</i> bis <i>60</i></p> <p>Standardwert ist <i>5</i>.</p>
UDP-Zielport	<p>Geben Sie die Port-Nummer für die Windows-Anwendung Activity Monitor ein.</p> <p>Standardwert ist <i>2107</i> (registriert durch IANA - Internet Assigned Numbers Authority).</p>
Passwort	<p>Geben Sie das Passwort für den Activity Monitor ein.</p>

Kapitel 21 Monitoring

Dieses Menü enthält Informationen, die das Auffinden von Problemen in Ihrem Netzwerk und das Überwachen von Aktivitäten, z. B. an der WAN-Schnittstelle Ihres Geräts, ermöglichen.

21.1 Internes Protokoll

21.1.1 Systemmeldungen

Im Menü **Monitoring->Internes Protokoll->Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die konfigurierten Werte der Felder **Maximale Anzahl der Syslog-Protokolleinträge** und **Maximales Nachrichtenlevel von Systemprotokolleinträgen**. Diese Werte können im Menü **Systemverwaltung->Globale Einstellungen->System** verändert werden.

Systemmeldungen

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden <input type="button" value="Übernehmen"/>					
Maximale Anzahl der Syslog-Protokolleinträge					50
Maximales Nachrichtenlevel von Systemprotokolleinträgen					Informationen
Ansicht <input type="text" value="20"/> pro Seite <input type="button" value="«"/> <input type="button" value="»"/> Filtern in <input type="text" value="Keiner"/> <input type="button" value="gleich"/> <input type="button" value="Los"/>					
Nr.	Datum	Zeit	Level	Subsystem	Nachricht
1	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
2	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
3	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
4	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
5	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas5Ghz not found
6	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas5Ghz
7	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanVSSTable
8	2005-10-07	20:35:21	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanIFTable
9	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
10	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
11	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
12	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
13	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas5Ghz not found
14	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas5Ghz
15	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanVSSTable
16	2005-10-07	20:06:23	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/loopobj.cpp-817: ERROR LoopObj:LoopObj name=wlanIFTable
17	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas58Ghz
18	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-457: Error Attribut gui_wlanGlobal.gui_wlanHas58Ghz not found
19	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-182: failed to add attrib for gui_wlanHas58Ghz
20	2005-10-07	20:04:58	Alarm	Konfiguration	NCI Alert: ./.J.J./nci/app/easp/easobj.cpp-625: Attrib not found gui_wlanHas5Ghz
Seite: 1, Objekte: 1 - 20, Summe der Objekte: 43					

Abb. 200: Monitoring->Internes Protokoll->Systemmeldungen

Werte in der Liste Systemmeldungen

Feld	Beschreibung
Nr.	Zeigt die laufende Nummer der System-Meldung an.
Datum	Zeigt das Datum der Aufzeichnung an.
Zeit	Zeigt die Uhrzeit der Aufzeichnung an.
Level	Zeigt die hierarchische Einstufung der Meldung an.
Subsystem	Zeigt an, welches Subsystem Ihres Geräts die Meldung generiert hat.
Nachricht	Zeigt den Meldungstext an.

21.2 IPsec

21.2.1 IPSec-Tunnel



Im Menü **Monitoring->IPSec->IPSec-Tunnel** wird eine Liste aller konfigurierten IPSec-Tunnel angezeigt.




Abb. 201: **Monitoring->IPSec->IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt den Namen der IPSec-Verbindung an.
Entfernte IP-Adresse	Zeigt die IP-Adresse des entfernten IPSec-Peers an.
Entfernte Netzwerke	Zeigt die aktuell ausgehandelten Subnetze der Gegenstelle an.
Sicherheitsalgorithmus	Zeigt den Verschlüsselungsalgorithmus der IPSec-Verbindung an.
Status	Zeigt den Betriebszustand der IPSec-Verbindung an.
Aktion	Bietet die Möglichkeit den Status der IPSec-Verbindung wie angezeigt zu ändern.
Details	Öffnet ein detailliertes Statistik-Fenster.

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

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

IPSec-Tunnel		IPSec-Statistiken	
Automatisches Aktualisierungsintervall		60	Sekunden Übernehmen
Allgemein			
Beschreibung	Peer-1		
Lokale IP-Adresse	0.0.0.0		
Entfernte IP-Adresse	0.0.0.0		
Lokale ID			
Entfernte ID			
Aushandlungsmodus			
Authentifizierungsmethode			
MTU	1418		
Erreichbarkeitsprüfung			
Statistik	Eingehend	Ausgehend	
Pakete	0	0	
Bytes	0	0	
Fehler	0	0	
Nachrichten (0)			

Abb. 202: Monitoring->IPSec->IPSec-Tunnel-> 

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Zeigt die Beschreibung des Peers an.
Lokale IP-Adresse	Zeigt die WAN-IP-Adresse Ihres Geräts an.
Entfernte IP-Adresse	Zeigt die WAN-IP-Adresse des Verbindungspartners an.
Lokale ID	Zeigt die ID Ihres Geräts für diese IPSec-Verbindung an.
Entfernte ID	Zeigt die ID des Peers an.
Aushandlungsmodus	Zeigt den Aushandlungsmodus an.
Authentifizierungsmethode	Zeigt die Authentifizierungsmethode an.
MTU	Zeigt die aktuelle MTU (Maximum Transfer Unit) an.
Erreichbarkeitsprüfung	Zeigt die Methode an, wie überprüft wird, dass der Peer erreichbar ist.
NAT-Erkennung	Zeigt die NAT-Erkennungsmethode an.
Lokaler Port	Zeigt den lokalen Port an.
Entfernter Port	Zeigt den entfernten Port an.
Pakete	Zeigt die Anzahl der eingehenden und ausgehenden Pakete an.
Bytes	Zeigt die Anzahl der eingehenden und ausgehenden Bytes an.
Fehler	Zeigt die Anzahl der Fehler an.

Feld	Beschreibung
IKE (Phase-1) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IKE (Phase 1) SAs an.
IPSec (Phase-2) SAs (x) Rolle / Algorithmus / Verbleibende Lebensdauer / Status	Zeigt die Parameter der IPSec (Phase 2) SAs an.
Nachrichten	Zeigt die Systemmeldungen zu diesem IPSec-Tunnel an.

21.2.2 IPSec-Statistiken

Im Menü **Monitoring->IPSec->IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

IPSec-Tunnel
IPSec-Statistiken

Automatisches Aktualisierungsintervall <input type="text" value="60"/> Sekunden Übernehmen					
Lizenzen			In Verwendung	Maximal	
IPSec-Tunnel			0	110	
Peers	Aktiv	Aktivieren	Blockiert	Ruhend	Konfiguriert
Status	0	0	0	1	1
SAs			Hergestellt	Gesamt	
IKE (Phase-1)			0	0	
IPSec (Phase-2)			0	0	
Paketstatistiken			Eingehend	Ausgehend	
Gesamt			59	136	
Weitergeleitet			59	136	
Verworfen			0	0	
Verschlüsselt			0	0	
Fehler			0	0	

Abb. 203: **Monitoring->IPSec->IPSec-Statistiken**

Das Menü **Monitoring->IPSec->IPSec-Statistiken** besteht aus folgenden Feldern:

Feld im Menü Lizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (In Verwendung) und die Anzahl der maximal verwendbaren Lizenzen

Feld	Beschreibung
	(Maximal) an.

Feld im Menü Peers

Feld	Beschreibung
Status	<p>Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an.</p> <ul style="list-style-type: none"> • Aktiv: Aktuell aktive IPSec-Verbindungen. • Aktivieren: IPSec-Verbindungen, die sich aktuell in der Tunnelaufbau-Phase befinden. • Blockiert: IPSec-Verbindungen, die geblockt sind. • Ruhend: Aktuell inaktive IPSec-Verbindungen. • Konfiguriert: Konfigurierte IPSec-Verbindungen.

Felder im Menü SAs

Feld	Beschreibung
IKE (Phase-1)	Zeigt die Anzahl der aktiven Phase-1-SAs (Hergestellt) zur Gesamtzahl der Phase-1-SAs (Gesamt) an.
IPSec (Phase-2)	Zeigt die Anzahl der aktiven Phase-2-SAs (Hergestellt) zur Gesamtzahl der Phase-2-SAs (Gesamt) an.

Felder im Menü Paketstatistiken

Feld	Beschreibung
Gesamt	Zeigt die Anzahl aller verarbeiteten eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an.
Weitergeleitet	Zeigt die Anzahl der eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an, die im Klartext weitergeleitet wurden.
Verworfen	Zeigt die Anzahl der verworfenen eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an.
Verschlüsselt	Zeigt die Anzahl der durch IPSec geschützten eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an.
Fehler	Zeigt die Anzahl der eingehenden (Eingehend) bzw. ausgehenden (Ausgehend) Pakete an, bei deren Behandlung es zu Fehlern gekommen ist.

21.3 Schnittstellen

21.3.1 Statistik

Im Menü **Monitoring->Schnittstellen->Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

Über die Filterleiste können Sie auswählen, ob **Gesamttransfer** oder **Transferdurchsatz** angezeigt werden soll. In der Anzeige **Transferdurchsatz** werden die Werte pro Sekunde angezeigt.

Statistik

Nr.	Beschreibung	Typ	Tx-Pakete	Tx-Bytes	Tx-Fehler	Rx-Pakete	Rx-Bytes	Rx-Fehler	Status	Nicht geändert seit	Aktion
1	en1-4	Ethernet	0	0	0	0	0	0	⊘	6d 22h 42m 24s	⬆️⬇️🔍
2	en1-0	Ethernet	3.87K	3.75M	0	2.80K	483.09K	0	⬆️⬇️	1d 0h 57m 51s	⬆️⬇️🔍
3	Peer-1	Tunnel	0	0	0	0	0	0	⊘	0d 0h 4m 25s	⬆️⬇️🔍

Seite: 1, Objekte: 1 - 3


Abb. 204: **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

Feld	Beschreibung
	zu ändern.

Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

Statistik

Anzeigen	Gesamttransfer	<input checked="" type="checkbox"/> Automatisches Aktualisierungsintervall	300	Sekunden	Übernehmen
Beschreibung	en1-0				
MAC-Adresse	00:a0f9:21:ef:16				
IP-Adresse / Netzmaske	0.0.0.0 / 0.0.0.0				
NAT	Deaktiviert				
Tx-Pakete	5.658				
Tx-Bytes	5.840.808				
Rx-Pakete	252.517				
Rx-Bytes	147.957.968				
TCP-Verbindungen					
Status	Lokale Adresse	Lokaler Port	Remote-Adresse	Entfernter Port	

Abb. 205: **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.

Feld	Beschreibung
Remote-Adresse	Zeigt die IP-Adresse an, zu der eine aktive TCP-Verbindung besteht.
Entfernter Port	Zeigt den Port an, zu dem eine aktive TCP-Verbindung besteht.

21.4 WLAN

21.4.1 WLANx

Im Menü **Monitoring->WLAN->WLAN** werden die aktuellen Werte und Aktivitäten der WLAN-Schnittstelle angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1		
VSS	WDS	Bridge-Links
Client Links	Client-Verwaltung	
Automatisches Aktualisierungsintervall	300	Sekunden
Übernehmen		
WLAN1 Statistik		
Mbit/s	Tx-Pakete	Rx-Pakete
802.11 a/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
5.5	0	0
2	0	0
1	0	0
802.11n		
144,4	0	0
139	0	0
115,6	0	0
86,7	0	0
72,2	0	0
65	0	0
57,8	0	0
43,3	0	0
28,9	0	0
21,7	0	0
14,4	0	0
7,2	0	0
Gesamt	0	0
Erweitert		

Abb. 206: 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](#) [WDS](#) [Bridge-Links](#) [Client Links](#) [Client-Verwaltung](#)

Automatisches Aktualisierungsintervall Sekunden

#	Beschreibung	Wert
1	Unicast MSDUs erfolgreich übertragen	0
2	Erfolgreich übertragene Multicast-MSDUs	0
3	Übertragene MPDUs	0
4	Erfolgreich empfangene Multicast-MSDUs	0
5	Unicast MPDUs erfolgreich erhalten	0
6	MSDUs, die nicht übertragen werden konnten	0
7	Frame-Übertragungen ohne ACK	0
8	Doppelte empfangene MSDUs	0
9	CTS Frames als Antwort auf RTS empfangen	0
10	Nicht entschlüsselbare MPDUs erhalten	0
11	RTS Frames ohne CTS	0
12	Fehlerhafte Erhaltene Pakete	0

Abb. 207: 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.
Frame-Übertragungen ohne ACK	Zeigt die Anzahl der gesendeten Frames an, für die kein Acknowledgement-Frame empfangen wurde.
Doppelte empfangene MSDUs	Zeigt die Anzahl von doppelt empfangenen MSDUs an.

Beschreibung	Bedeutung
CTS Frames als Antwort auf RTS empfangen	Zeigt die Anzahl der empfangenen CTS (Clear to send)-Frames an, die als Antwort auf RTS (Request to send) empfangen wurden.
Nicht entschlüsselbare MPDUs erhalten	Zeigt die Anzahl der empfangenen MPDUs an, die nicht entschlüsselt werden konnten. Ein Grund dafür könnte sein, dass kein passender Schlüssel eingetragen wurde.
RTS Frames ohne CTS	Zeigt die Anzahl der RTS-Frames an, für die kein CTS empfangen wurde.
Fehlerhafte Erhaltene Pakete	Zeigt die Anzahl der Frames an, die unvollständig oder fehlerhaft empfangen wurden.

21.4.2 VSS

Im Menü **Monitoring->WLAN->VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.

WLAN1 VSS WDS Bridge-Links Client Links Client-Verwaltung

Automatisches Aktualisierungsintervall	300	Sekunden	Übernehmen					
Client-Node-Tabelle								
MAC-Adresse	IP-Adresse	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s	
Funkwerk-ec (vss1-0)								
00:0d:f0:67:55:f3	0.0.0.0	0 Tag(e) 0:1:57	1	3	-99(0,0,0)	-98	1	


Abb. 208: **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.

Feld	Beschreibung
Datenrate Mbit/s	<p>Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an.</p> <p>Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s.</p> <p>Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.</p>

VSS - Details für Verbundene Clients

Im Menü **Monitoring->WLAN->VSS-><Verbundener Client>->**  werden die aktuellen Werte und Aktivitäten eines verbundenen Clients angezeigt. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1 VSS WDS Bridge-Links Client Links Client-Verwaltung						
Automatisches Aktualisierungsintervall		60	Sekunden		Übernehmen	
Client-MAC-Adresse	IP-Adresse	Uptime	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	SNR dB	Datenrate Mbit/s
00:01:cd:06:1a:b4	10.0.0.234	0 Tag(e) 0:0:27	-88(-90,-88,-88)	-87	-1	12
Rate		Tx-Pakete	Rx-Pakete			
802.11 a/b/g						
54		0	0			
48		0	0			
36		0	0			
24		0	518			
18		0	89.27k			
12		0	8.39k			
11		4	0			
9		0	0			
6		0	519			
5.5		0	0			
2		2	0			
1		0	75			
802.11n						
300		0	0			
270		0	0			
240		0	0			
180		0	0			
150		0	0			
135		0	0			
120		0	0			
90		0	0			
60		0	701			
45		0	0			
30		0	0			
15		0	0			
Gesamt		6	215.36k			
Zurück						

Abb. 209: **Monitoring->WLAN->VSS-><Verbundener Client>->** 

Werte in der Liste <Verbundener Client>

Feld	Beschreibung
Client-MAC-Adresse	Zeigt die MAC-Adresse des assoziierten Clients.
IP-Adresse	Zeigt die IP-Adresse des Clients.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client angemeldet ist.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen

Feld	Beschreibung
	Indikator für die Qualität der Verbindung im Funk dar. Werte: <ul style="list-style-type: none"> • > 25 dB exzellent • 15 – 25 dB gut • 2 – 15 dB grenzwertig • 0 – 2 dB schlecht.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der von diesem Client empfangenen Daten in Mbit/s an. Folgende Übertragungsraten sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s Falls das 5-GHz-Frequenzband genutzt wird, wird die Anzeige von 11, 5.5, 2 und 1 Mbit/s bei IEEE 802.11b unterdrückt.
Rate	Zeigt die möglichen Datenraten auf dem Funkmodul an.
Tx-Pakete	Zeigt die Anzahl der gesendeten Pakete für die jeweilige Datenrate an.
Rx-Pakete	Zeigt die Anzahl der erhaltenen Pakete für die jeweilige Datenrate an.

21.4.3 WDS

Im Menü **Monitoring->WLAN->WDS** werden die aktuellen Werte und Aktivitäten der konfigurierten WDS-Links angezeigt.


WLAN	VSS	WDS	Bridge-Links	Client Links	Client-Verwaltung				
Automatisches Aktualisierungsintervall		300	Sekunden		Übernehmen				
WDS-Tabelle									
WDS-Beschreibung	Entfernte MAC	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s		
wds1-0	00:00:00:00:00:00	0d 0h 0m 5s	0	0	0(0,0,0)	0	0		

Abb. 210: **Monitoring->WLAN->WDS**

Werte in der Liste WDS


Feld	Beschreibung
WDS-Beschreibung	Zeigt den Namen des WDS Links an.
Entfernte MAC	Zeigt die MAC-Adresse des WDS-Link-Partners an.

Feld	Beschreibung
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige WDS-Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem WDS-Link empfangenen Daten in Mbit/s an.


Über die Verknüpfung **Test** kann ggf. ein Link-Test ausgelöst werden. Der Test ist nur für Teldat-Geräte verfügbar und nur, wenn der WDS-Link aktiv ist.

Der Link-Test liefert alle Daten, die zur Beurteilung der Qualität des WDS-Links benötigt werden. Der Link-Test dient auch als Unterstützung beim Ausrichten der Antennen. Diese Option wird nur angezeigt, wenn Link state auf *Aktiviert* steht.

WDS Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den WDS-Links. Dabei werden die Werte für den Drahtlos-Modus 802.11n separat aufgeführt.

WLAN1		VSS	WDS	Bridge-Links	Client Links	Client-Verwaltung	
Automatisches Aktualisierungsintervall		300	Sekunden		Übernehmen		
WDS-Beschreibung	Entfernte MAC	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s
wds1-0	00:00:00:00:00:00	0d 16h 2m 15s	0	0	0(0,0,0)	0	0
Rate		Tx-Pakete		Rx-Pakete			
802.11 a/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			
5.5		0		0			
2		0		0			
1		0		0			
802.11n							
144,4		0		0			
139		0		0			
115,6		0		0			
86,7		0		0			
72,2		0		0			
65		0		0			
57,8		0		0			
43,3		0		0			
28,9		0		0			
21,7		0		0			
14,4		0		0			
7,2		0		0			
Gesamt		0		0			
Zurück							

Abb. 211: Monitoring->WLAN->WDS-> 

Werte in der Liste WDS

Feld	Beschreibung
WDS-Beschreibung	Zeigt den Namen des WDS Links an.
Entfernte MAC	Zeigt die MAC-Adresse des WDS-Link-Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige WDS-Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm (RSSI1, RSSI2, RSSI3)	Zeigt die Empfangsstärke des Signals in dBm an.

Feld	Beschreibung
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem WDS-Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.

21.4.4 Bridge-Links

Im Menü **Monitoring->WLAN->Bridge-Links** werden die aktuellen Werte und Aktivitäten der Bridge-Links angezeigt.

WLAN1 VSS WDS **Bridge-Links** Client Links Client-Verwaltung

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

Bridge-Link-Tabelle								
Bridge-Link-Beschreibung	Entfernte MAC	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s	
wds1-0	00:00:00:00:00:00	0d 16h 7m 1s	0	0	0(0,0,0)	0	0	

Abb. 212: **Monitoring->WLAN->Bridge-Links**

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Bridge-Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.

Über die Verknüpfung **Test** kann ggf. ein Link-Test ausgelöst werden.

Der Link test liefert alle Daten, die zur Beurteilung der Qualität des Bridge-Links benötigt

werden. Der Link test dient auch als Unterstützung beim Ausrichten der Antennen. Diese Option wird nur angezeigt, wenn Link state auf *Aktiviert* steht.

Bridge-Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Bridge-Links.

WLAN1 VSS WDS Bridge-Links Client Links Client-Verwaltung							
Automatisches Aktualisierungsintervall		300	Sekunden		Übernehmen		
Bridge-Link-Beschreibung	Entfernte MAC	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s
wds1-0	00:00:00:00:00:00	0d 16h 12m 59s	0	0	0(0,0,0)	0	0
Rate		Tx-Pakete		Rx-Pakete			
802.11 a/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			
5.5		0		0			
2		0		0			
1		0		0			
802.11n							
144,4		0		0			
139		0		0			
115,6		0		0			
86,7		0		0			
72,2		0		0			
65		0		0			
57,8		0		0			
43,3		0		0			
28,9		0		0			
21,7		0		0			
14,4		0		0			
7,2		0		0			
Gesamt		0		0			
Zurück							

Abb. 213: Monitoring->WLAN->Bridge-Links->

Werte in der Liste Bridge-Links

Feld	Beschreibung
Bridge-Link-Beschreibung	Zeigt den Namen des Bridge-Links an.

Feld	Beschreibung
Entfernte MAC	Zeigt die MAC-Adresse des Bridge-Link-Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Bridge-Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Bridge-Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.

21.4.5 Client Links

Im Menü **Monitoring->WLAN->Client Links** werden die aktuellen Werte und Aktivitäten der Client Links angezeigt.

WLAN1
VSS
WDS
Bridge-Links
Client Links
Client-Verwaltung

Automatisches Aktualisierungsintervall Sekunden Übernehmen

Client Links							
Beschreibung des Client Links	AP-MAC-Adresse	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm (RSSI1, RSSI2, RSSI3)	Rauschen dBm	Datenrate Mbit/s
WLAN1 ()							
sta1-0		0d 0h 0m 22s	0	0	0(0,0,0)	0	0

Abb. 214: Monitoring->WLAN->Client Links

Werte in der Liste Client Links

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des Client Links an.
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm	Zeigt die Empfangsstärke des Signals in dBm an.

Feld	Beschreibung
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.

Client Link Details

Über das -Symbol öffnen Sie eine Übersicht über weitere Details zu den Client Links.

WLAN1
VSS
WDS
Bridge-Links
Client Links
Client-Verwaltung

Automatisches Aktualisierungsintervall <input type="text" value="300"/> Sekunden		Übernehmen			
AP-MAC-Adresse	Uptime	Signal dBm(RSSI1, RSSI2, RSSI3)	Rauschen dBm	SNR dB	Datenrate Mbit/s
	0d 0h 1m 12s	0(0,0,0)	0	0	0
Rate	Tx-Pakete	Rx-Pakete			
802.11 a/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			
5.5	0	0			
2	0	0			
1	0	0			
802.11n					
144,4	0	0			
139	0	0			
115,6	0	0			
86,7	0	0			
72,2	0	0			
65	0	0			
57,8	0	0			
43,3	0	0			
28,9	0	0			
21,7	0	0			
14,4	0	0			
7,2	0	0			
Gesamt	0	0			

Zurück

Abb. 215: Monitoring->WLAN->Client Links->

Werte in der Liste Client Links

Feld	Beschreibung
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.

Feld	Beschreibung
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Signal dBm	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Zeigt die Qualität des Signals in dB an.
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrate der auf diesem Client Link empfangenen Daten in Mbit/s an.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.

21.4.6 Lastverteilung

Im Menü **Monitoring->WLAN+Lastverteilung** wird eine Übersicht des **Lastverteilung** 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.

WLAN1 VSS WDS Bridge-Links Client Links Client-Verwaltung


Ansicht: 20 pro Seite << >> Filtern in: Keiner gleich Los						
VSS-Beschreibung ^	Netzwerkname (SSID)	MAC-Adresse	Aktive Clients	2,4/5-GHz-Übergang	Abgewiesene Clients soft/hard	
vss7-10	default	00:a0:f9:0b:cfe0	0	0	0/0	
Seite: 1, Objekte: 1 - 1						

Abb. 216: **Monitoring->WLAN+Lastverteilung**

Werte in der Liste Lastverteilung

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	Zeigt die Anzahl der abgewiesenen Clients, nachdem die abso-

Feld	Beschreibung
soft/hard	lute Anzahl an zulässigen Clients erreicht wurde.

21.5 Bridges

21.5.1 br<x>

Im Menü **Monitoring->Bridges-> br<x>** werden die aktuellen Werte der konfigurierten Bridges angezeigt.

br0

Automatisches Aktualisierungsintervall Sekunden Übernehmen

MAC-Adresse	Port
00:a0:f9:0b:08:98	en1-0

Abb. 217: **Monitoring->Bridges**

Werte in der Liste **br<x>**

Feld	Beschreibung
MAC-Adresse	Zeigt die MAC-Adressen der assoziierten Bridges an.
Port	Zeigt den Port an, auf dem die Bridge aktiv ist.

21.6 Hotspot-Gateway

21.6.1 Hotspot-Gateway

Im Menü **Monitoring->Hotspot-Gateway->Hotspot-Gateway** wird eine Liste aller verbundenen Hotspot-Benutzer angezeigt.

Hotspot-Gateway

Automatisches Aktualisierungsintervall Sekunden Übernehmen

Authentifizierter Hotspot-Benutzer

Benutzername	IP-Adresse	Physische Adresse	Anmeldung	Schnittstelle

Abb. 218: **Monitoring->Hotspot-Gateway->Hotspot-Gateway**

Werte in der Liste Hotspot-Gateway

Feld	Beschreibung
Benutzername	Zeigt den Namen des Benutzers an.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Physische Adresse	Zeigt die Physische Adresse des Benutzers an.
Anmeldung	Zeigt den Zeitpunkt der Anmeldung an.
Schnittstelle	Zeigt die verwendete Schnittstelle an.

21.7 QoS

Im Menü **Monitoring->QoS** werden Statistiken für die Schnittstellen angezeigt, für die QoS konfiguriert wurde.

21.7.1 QoS

Im Menü **Monitoring->QoS->QoS** wird eine Liste aller Schnittstellen angezeigt, für die QoS konfiguriert wurde.

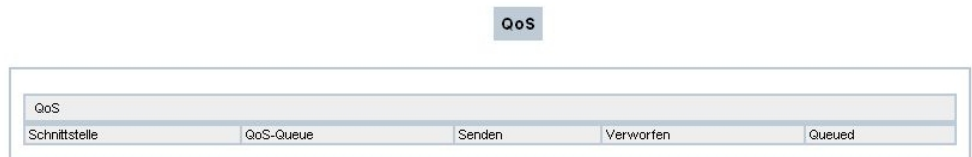


Abb. 219: **Monitoring->QoS->QoS**

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.

21.8 PIM

21.8.1 Allgemeine Statusangaben

Im Menü **Monitoring->PIM->Allgemeine Statusangaben** wird der Status aller konfigurier-ten PIM Komponenten angezeigt.

Abb. 220: **Monitoring->PIM->Allgemeine Statusangaben**

Werte in der Liste Allgemeine Statusangaben

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: <i>Alle, PIM-Schnittstellen, PIM-Nachbarn und Zuordnung Multicast-Gruppen zu RPs</i>

Werte in der Liste PIM-Schnittstellen

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der PIM-Schnittstelle an.
IP-Adresse	Zeigt die primäre IP-Adresse der PIM-Schnittstelle an.
Designated Router (DR)	Zeigt die primäre IP-Adresse des Designated Routers auf dieser

Feld	Beschreibung
	PIM-Schnittstelle an.

Werte in der Liste PIM-Nachbarn

Feld	Beschreibung
Schnittstelle	Zeigt die Schnittstelle an, über die der PIM Neighbor erreicht wird.
Generation ID	Zeigt die ID des Nachbar-Gateways an.
IP-Adresse	Zeigt die primäre IP-Adresse des PIM Neighbors an.
Uptime	Zeigt an, wie lange der letzte PIM Neighbor ein Nachbar des lokalen Routers ist.
Expiry Timer	Zeigt an, wann der PIM Neighbor nicht mehr als Nachbar eingetragen ist. Wird der Wert 0 angezeigt, bleibt der PIM Neighbor immer als Nachbar eingetragen.

Werte in der Liste Zuordnung Multicast-Gruppen zu RPs

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Präfixlänge der Multicast-Gruppe	Zeigt die dazugehörige Netzmaske an.
IP-Adresse des Rendezvous Points	Zeigt die IP-Adresse des Rendezvous Points an.

21.8.2 Nicht-schnittstellen-spezifischer Status

Das Menü **Monitoring->PIM->Nicht-schnittstellen-spezifischer Status** enthält Status-Angaben für alle PIM-Schnittstellen.

Allgemeine Statusangaben
Nicht-schnittstellen-spezifischer Status
Schnittstellenspezifische Zustände

Ansicht: Alle

(*,*,RP) Status

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

IP-Adresse des Rendezvous Point Upstream Join State Upstream Nachbar-IP-Adresse Uptime Upstream Join Timer

Seite: 1

(*,G) Status

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

Multicast-Gruppen-Adresse Upstream Nachbar-IP-Adresse Reverse-Path-Forwarding (RPF) Upstream Join State Uptime Upstream Join Timer

Seite: 1

(S,G) Status

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

Multicast-Gruppen-Adresse Quell-IP-Adresse Upstream Nachbar-IP-Adresse Upstream Join State Uptime Upstream Join Timer Shortest Path Tree

Seite: 1

(S,G,RPT) Status

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

Multicast-Gruppen-Adresse Quell-IP-Adresse Reverse-Path-Forwarding (RPF) Uptime Upstream Override Timer

Seite: 1

Abb. 221: Monitoring->PIM->Nicht-schnittstellen-spezifischer Status

Werte in der Liste Nicht-schnittstellen-spezifischer Status

Feld	Beschreibung
Ansicht	<p>Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus.</p> <p>Zur Auswahl stehen: <i>Alle</i>, <i>(*,*,RP) Status</i>, <i>(*,G) Status</i>, <i>(S,G) Status</i> und <i>(S,G,RPT) Status</i></p>

Werte in der Liste (*,*,RP) Status

Feld	Beschreibung
IP-Adresse des Rendezvous Point	Zeigt die IP-Adresse des Rendezvous Point (RP) der Gruppe an.
Upstream Join State	Der Upstream (*,*,RP) Join/Prune Status gibt den Status der Upstream (*,*,RP) State Machine in der PIM-SM Spezifikation wieder.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Upstream Neighbors, oder unknown(0), wenn die Upstream Neighbor IP-Adresse nicht bekannt ist oder es sich nicht um einen PIM Neighbor handelt.
Uptime	Zeigt den Zeitraum an, wie lange der RP besteht.
Upstream Join Timer	Der Join/Prune Timer wird verwendet, um periodisch

Feld	Beschreibung
	Join(*,*,RP) Nachrichten zu senden, und um Prune(*,*,RP) Nachrichten von Peers auf einer Upstream LAN Schnittstelle zu korrigieren.

Werte in der Liste (*,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse an.
Upstream Nachbar-IP-Adresse	Zeit die primäre IP-Adresse des Neighbors auf pimStarGRPFIIndex an, zu der der lokale Router periodisch (*,G) Join Nachrichten schickt. Der InetAddressTyp ist durch das Objekt pimStarGUpstreamNeighborType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF(*,G) genannt.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der Next Hop nicht bekannt ist.
Upstream Join State	Zeigt an, ob der lokale Router dem RP Tree der Gruppe beitreten soll. Dieses entspricht dem Status der Upstream (*,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (*,G) Join Nachricht auf pimStarGRPFIIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Upstream Join Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimSGAddressType definiert.
Upstream Nachbar-IP-Adresse	Zeigt die primäre IP-Adresse des Neighbors auf pimSGRPFIIndex an, zu dem der Router periodisch (S,G) Join Nachrichten schickt. Der Wert ist 0, wenn der RPF Next Hop nicht bekannt oder kein PIM Neighbor ist. InetAddressType wird im Objekt pimSGAddressType definiert. Diese Adresse wird in der PIM-SM Spezifikation RPF(S,G) genannt.
Upstream Join State	Zeigt an, ob der lokale Router den Shortest-Path-Tree für die

Feld	Beschreibung
	Quelle und die Gruppe, die durch diesen Eintrag dargestellt wird, beitreten soll. Dieses entspricht dem Status der Upstream (S,G) State Machine in der PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Join Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste periodische (S,G) Join Nachricht auf pimSGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Upstream Join Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.
Shortest Path Tree	Zeigt an, ob das Shortest Path Tree Bit gesetzt ist, d.h. ob das Forwarding über den Shortest Path Tree stattfinden soll.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Reverse-Path-Forwarding (RPF)	Zeigt den Adresstyp des RPF Next Hop zum RP an, oder unknown(0), wenn der RPF Next Hop nicht bekannt ist.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Upstream Override Timer	Zeigt die verbleibende Zeit an, bis der lokale Router die nächste Triggered (S,G,rpt) Join Nachricht auf pimStarGRPFIfIndex sendet. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Upstream Override Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.

21.8.3 Schnittstellenspezifische Zustände

Das Menü **Monitoring->PIM->Schnittstellenspezifische Zustände** enthält schnittstellenspezifische Status-Angaben.

Allgemeine Statusangaben	Nicht-schnittstellen-spezifischer Status	Schnittstellenspezifische Zustände
Ansicht: -Alle-		
(*,G,I) Status		
Ansicht: 20	pro Seite: << >>	Filtern in: Keiner
		gleich
Multicast-Gruppen-Adresse	Schnittstelle	Join/Prune-Status
		Uptime
		Expiry Timer
		Assert-Status
		IP-Adresse des Assert Winner
Seite: 1		
(S,G,I) Status		
Ansicht: 20	pro Seite: << >>	Filtern in: Keiner
		gleich
Multicast-Gruppen-Adresse	Quell-IP-Adresse	Schnittstelle
		Join/Prune-Status
		Uptime
		Expiry Timer
		Assert-Status
		IP-Adresse des Assert Winner
Seite: 1		
(S,G,Rpt,I) Status		
Ansicht: 20	pro Seite: << >>	Filtern in: Keiner
		gleich
Multicast-Gruppen-Adresse	Quell-IP-Adresse	Schnittstelle
		Uptime
		Join/Prune-Status
		Expiry Timer
Seite: 1		

Abb. 222: Monitoring->PIM->Schnittstellenspezifische Zustände

Werte in der Liste Schnittstellenspezifische Zustände

Feld	Beschreibung
Ansicht	Wählen Sie in dem Dropdown-Menü die gewünschte Ansicht aus. Zur Auswahl stehen: <i>Alle</i> , <i>(* ,G ,I) Status</i> , <i>(S ,G ,I) Status</i> und <i>(S ,G ,RPT) Status</i>

Werte in der Liste (*,G,I) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-Gruppenadresse dieses Eintrags an. InetAddressType wird im Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (*,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden. Dieses entspricht dem Status der Downstream Per-Interface (*,G) State Machine in the PIM-SM Spezifikation.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (*,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (*,G) Join Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFF'h steht für unendlich.

Feld	Beschreibung
Assert-Status	Zeigt den (*,G) Assert State für diese Schnittstelle. Dieser entspricht dem Status der Per-Interface (*,G) Assert State Machine in der PIM-SM Spezifikation. Wenn pimStarGPimMode 'bidir' ist, muss dieses Objekt 'holInfo' lauten.
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner an, wenn pimStarGIAssertState 'iAmAssertLoser' lautet. InetAddressType wird durch das Objekt pimStarGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Join/Prune-Status	Zeigt den Status an, der sich aus den (S,G) Join/Prune Nachrichten ergibt, die auf dieser Schnittstelle empfangen wurden. Dieser entspricht dem Status der Downstream Per-Interface (S,G) State Machine in der PIM-SM und PIM-DM Spezifikation.
Uptime	Zeigt die Zeit an, die verbleibt, bevor der lokale Router auf eine (S,G) Prune Nachricht reagiert, die auf dieser Schnittstelle empfangen wird. Der Router wartet diese Zeit, um zu prüfen, ob ein anderer Downstream Router die Prune Nachricht korrigiert. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Prune-Pending Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G) Join State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G) Join Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation (S,G) Prune Timer genannt.
Assert-Status	Zeigt den (S,G) Assert State für diese Schnittstelle an. Dieser entspricht dem Status der Per-Interface (S,G) Assert State Machine in der PIM-SM Spezifikation Siehe "I-D.ietf-pim-sm-v2-new section 4.6.1"
IP-Adresse des Assert Winner	Zeigt die Adresse des Assert Winner, wenn pimSGIAssertState 'iAmAssertLoser lautet. InetAddressType wird durch das Objekt pimSGIAssertWinnerAddressType definiert.

Werte in der Liste (S,G,RPT) Status

Feld	Beschreibung
Multicast-Gruppen-Adresse	Zeigt die Multicast-IP-Adresse an. InetAddressType wird durch das Objekt pimSGAddressType definiert.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse an. InetAddressType wird durch das Objekt pimStarGAddressType definiert.
Schnittstelle	Zeigt den Namen der Schnittstelle an.
Uptime	Zeigt die Zeitdauer an, seit der Eintrag vom lokalen Router erzeugt wurde.
Join/Prune-Status	Zeigt an, ob der lokale Router die Quelle des RP Tree abschneiden soll. Dieses entspricht in der PIM-SM Spezifikation dem Status der Upstream (S,G,rpt) State Machine für Triggered Messages.
Expiry Timer	Zeigt die verbleibende Zeit an, bis der (S,G,rpt) Prune State für diese Schnittstelle ungültig wird. Dieser Timer wird in der PIM-SM Spezifikation (S,G,rpt) Prune Expiry Timer genannt. Er hat den Wert 0, wenn der Timer deaktiviert ist. Der Wert 'FFFFFFFF'h steht für unendlich. Dieser Timer wird in der PIM-DM Spezifikation(S,G) Prune Timer genannt.

Glossar

2G	Siehe GSM.
3DES	Siehe DES.
3G	Siehe UMTS.
4G	Siehe LTE.
802.11	Die Norm 802.11 beschreibt Wireless LAN (WLAN). Es existieren verschiedene Erweiterungen: 802.11a: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 5 GHz, 802.11b: Brutto-Datentransferrate: 11 Mbit/s, Frequenzband: 2,4 GHz, 802.11g: Brutto-Datentransferrate: 54 Mbit/s, Frequenzband: 2,4 GHz, 802.11n: Brutto-Datentransferrate: 600 Mbit/s, Frequenzband: 2,4 GHz (optional: 5 GHz)
Access Client	Der Client Mode ist eine Betriebsart eines Wireless Access Points (AP), bei dem sich dieser gegenüber dem übergeordneten AP wie ein Wireless Adapter verhält. Mit einem im Client Mode betriebenen AP können einzelne Rechner oder ganze Subnetze an übergeordnete Netze angebunden werden.
Access Point	Ein Access Point (AP) ist ein Gerät zur drahtlosen Verbindung von Clients (Computern). Der AP dient somit zum Aufbau eines Funknetzwerks (WLAN) sowie der Verbindung dieses WLANs mit einem kabelgebundenen Ethernet-Netzwerk (Bridging).
Accounting	Beim Accounting werden Verbindungsdaten aufgezeichnet, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.
Activity Monitor	Mithilfe des Activity Monitors kann der Status physikalischer und virtueller Geräteschnittstellen überwacht werden.
Ad-Hoc-Netzwerk	In einem Ad-Hoc-Netzwerk verbinden sich einzelne Clients über einen Wireless Adapter zu einem unabhängiges Wireless LAN. Ad-Hoc-Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer-Basis. Der Ad-Hoc-Modus wird auch als IBSS-Modus (Independent Basic Service Set) bezeichnet und ist in kleinsten Netzen sinnvoll, z. B. bei der Vernetzung zweier Notebooks ohne Access Point.
ADSL	Asymmetric Digital Subscriber Line. Siehe DSL.

AES	Advanced Encryption Standard (AES, Rijndael) ist ein Verschlüsselungsverfahren (siehe Cipher). AES verwendet eine feste Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit. AES ist ein sehr schneller und sicherer Algorithmus.
Aggressive Mode	Beim Aufbau einer IPSec-Verbindung wird der Aggressive Mode zur Realisierung eines Phase-1-Austausches verwendet. Der Aggressive Mode bietet keinen Schutz der Identität für aushandelnde Knoten, da sie ihre Identitäten übertragen müssen, bevor sie einen sicheren Kanal aufbauen können. Siehe auch Main Mode.
AH	Der Authentication Header (AH) wird bei IPSec verwendet, um die Authentizität und Integrität der übertragenen Pakete sicherzustellen sowie den Sender zu authentisieren.
Anlagenanschluss	Beim Anlagenanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer TK-Anlage. Man erhält eine Anlagenanschluss-Rufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Anlagenanschluss-Rufnummer: 1234, Rufnummernblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...) Siehe auch Mehrgeräteanschluss.
Anlagenanschluss-Rufnummer	Siehe Anlagenanschluss.
Annex A	Annex A ist eine DSL-Variante, die in Verbindung mit analogen Telefonanschlüssen (POTS) auftritt, z. B. in Frankreich.
Annex B	Annex B ist eine DSL-Variante, die in Verbindung mit ISDN auftritt, z. B. in Deutschland.
Annex J	Annex J ist eine DSL-Variante zur reinen Datenübertragung, ohne Sprachinformationen (entbundelter Anschluss). Annex J ist eine Ergänzung zur Spezifikation G.992. Diese DSL-Anschlüsse benötigen keinen Splitter und haben eine höhere Reichweite und eine schnellere Übertragungsgeschwindigkeit.
Annex L	Annex L ist eine Erweiterung von Annex A. Die Reichweite ist zulasten der Datenübertragungsrate vergrößert.
Annex M	Annex M ist eine Erweiterung von Annex A. Der Upstream ist zulasten des Downstreams vergrößert.

ANSI T1.413	ANSI T1.413 ist eine ADSL-Variante.
ARP	Das Address Resolution Protocol (ARP) liefert zu IPv4-Adressen die zugehörigen MAC-Adressen. Die notwendigen Informationen werden zwischen den Netzwerkknoten ausgetauscht, im Cache des Geräts gespeichert und nach Ablauf der ARP Lifetime wieder gelöscht. Für IPv6 wird diese Funktionalität durch das Neighbor Discovery Protocol (NDP) bereitgestellt.
ATM	Asynchronous Transfer Mode (ATM) ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete – Zellen oder Slots genannt – mit fester Länge kodiert und über asynchrones Zeitmultiplexing übertragen wird.
Authentifikation	Überprüfung der Identität des Nutzers (Authentisierung).
Autorisierung	Auf Basis seiner Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
AUX	AUX ist ein Signaleingang für externe Geräte, z. B. Analog- oder GSM-Modems.
B-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.
Backbone Area	Als Backbone wird der Kernbereich eines Netzwerks bezeichnet, der alle Teilnetze (Areas) miteinander verbindet.
Basisanschluss	Der Basisanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Basic Rate Interface (BRI). Ein Basisanschluss bietet zwei Nutzkanäle (B-Kanäle) mit je 64 kbit/s und einen Steuerkanal (D-Kanal) mit 16 kbit/s. Für den Basisanschluss existieren zwei Betriebsarten: Anlagenanschluss und Mehrgeräteanschluss. Für größere Installationen wird der Primärmultiplexanschluss verwendet.
Beacon	Zum Aufbau eines Wireless LAN im Infrastruktur-Modus versendet der zentrale Access Point Beacons. Diese Mitteilungen enthalten den Netzwerknamen (SSID), eine Liste der unterstützten Übertragungsraten und die Art der Verschlüsselung.
Bit	Ein Binary Digit (Bit) ist die kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.
Black / White List	Einträge in der Black List werden blockiert, Einträge in der White List werden durchgelassen. (Beispiel: Alle Telefonnummern, die mit 01234 beginnen, werden in der Black List blockiert. Die Telefonnum-

mer 01234987 kann trotzdem in der White List freigegeben werden.)

Blowfish	Blowfish ist ein Verschlüsselungsverfahren (siehe Cipher). Blowfish verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 32 und 448 Bit gewählt werden.
BootP	Das Bootstrap Protocol (BootP) dient zur automatischen Vergabe einer IP-Adresse.
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Siehe Basisanschluss.
Bridge	Eine Bridge ist eine Netzwerkkomponente zum Verbinden gleichartiger Netze auf Schicht 2 des OSI-Modells. Datenpakete werden anhand von MAC-Adressen übertragen. Durch Bridges wird das Netzwerk aufgeteilt und entlastet.
Broadcast	Bei einem Broadcast werden Datenpakete von einem Punkt an alle Teilnehmer eines Netzes übertragen, z. B. falls der Empfänger noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP und DHCP. Die Kommunikation erfolgt über Broadcast-Adressen: MAC-Netzwerke: FF:FF:FF:FF:FF:FF, IPv4-Netzwerke: 255.255.255.255, IPv6-Netzwerke: ff00::/8
BRRP	BRRP ist eine Implementierung des Virtual Router Redundancy Protocol (VRRP). Ziel des Verfahrens ist es den Ausfall des Standardgateways zu kompensieren. Mehrere Router werden zu einem virtuellen Router zusammengefasst. Fällt einer dieser Router aus, können die Restlichen diesen ersetzen.
CA	Certificate Authority. Siehe Zertifikat.
Cache	Informationen zur Namensauflösung werden vom Gerät im sogenannten Cache zwischengespeichert. Siehe auch ARP.
Called Party's Number	Rufnummer des angerufenen Teilnehmers.
Calling Party's Number	Rufnummer des Anrufers.
CAPI	Das Common ISDN Application Programming Interface (CAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch TAPI.

CAPWAP	Das Control And Provisioning of Wireless Access Points Protocol (CAPWAP) dient zur Überwachung von Wireless Access Points (Slaves) durch einen WLAN-Controller (Master). Es verwendet die UDP-Ports 5246 zur Kontrolle und 5247 zur Datenübertragung.
CAST	CAST ist ein Verschlüsselungsverfahren (siehe Cipher). CAST verwendet eine fixe Blocklänge von 64 Bit. Die Schlüssellänge kann zwischen 40 und 128 Bit gewählt werden. Alternative Bezeichnungen sind CAST-128 oder CAST5.
CHAP	Das Challenge Handshake Authentication Protocol (CHAP) ist ein Authentifizierungsprotokoll für PPP-Verbindungen. Neben dem Standard-CHAP existieren noch die Varianten MS-CHAPv1 und MS-CHAPv2 der Firma Microsoft. Man wählt sich über PPP in ein Netzwerk ein und authentifiziert sich mit Benutzername und Passwort. Benutzername und Passwort werden verschlüsselt übertragen. Siehe auch PAP.
Cipher	Eine Blockchiffre (Block Cipher) ist ein Verschlüsselungsalgorithmus. In diesem Verschlüsselungsverfahren wird ein Datenblock mit fester Größe (normalerweise 64 Bit) mithilfe eines sogenannten Schlüssels zu einem Block derselben Größe umgeschrieben. Je länger der Schlüssel ist, umso sicherer ist der Algorithmus.
Client	Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.
CoS	Der Begriff Class of Service (CoS) hat je nach Anwendungsgebiet verschiedene Bedeutungen. In der Telekommunikation wird unter CoS die dem Benutzer zugewiesene Berechtigungsklasse verstanden. Die Berechtigungsklasse legt die Rechte des Benutzers fest, wie z. B. Amtsberechtigung, nutzbare Leistungsmerkmale, Zugriff auf Anwendungen, ... In der Netzwerktechnologie versteht man unter CoS die Klassifizierung bestimmter Dienste gemäß IEEE 802.1p. CoS ermöglicht eine gezielte Priorisierung, während mit Quality of Service (QoS) explizite Bandbreitengarantien oder -beschränkungen eingerichtet werden. Die Einteilung der Datenpakete erfolgt mittels eines DSCP-Werts (Differentiated Services Code Point).
CRC	Cyclic Redundancy Check (CRC) ist ein Verfahren, um Fehler in der Datenübertragung zu erkennen.
CRL	Siehe Zertifikat.
D-Kanal	Siehe Basisanschluss und Primärmultiplexanschluss.

Daemon	Als Daemon bezeichnet man ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt.
Datagramm	Ein Datagramm ist eine in sich geschlossene Dateneinheit mit Nutz- und Steuerdaten. Es steht allgemein für die Begriffe Datenframe, Datenpaket und Datensegment.
Datenkompression	Die Datenkompression ist ein Verfahren, um die übertragene Datenmenge zu verringern. Siehe STAC und MPPC.
Dead Peer Detection	In IPsec werden mithilfe der Dead Peer Detection nicht mehr erreichbare IKE-Peers aufgespürt.
Default Gateway	An das Default Gateway (Standardrouter) wird sämtlicher Datenverkehr gesendet, der nicht für das eigene Netzwerk bestimmt ist.
Default Route	Siehe Standardroute.
Diffie-Hellman	Diffie-Hellman ist ein Public-Key-Algorithmus zur Aushandlung und Etablierung von Schlüsseln. Da Daten weder verschlüsselt noch signiert werden, ist das Verfahren nur sicher, falls sich die Verbindungspartner über andere Mechanismen, wie RSA oder DSA, authentifizieren.
Denial-Of-Service Attack	Bei einem Denial-of-Service-Angriff (DoS) wird eine Netzwerkkomponente mit Anfragen überflutet, sodass diese völlig überlastet wird. Das System oder ein bestimmter Dienst ist in Folge dessen nicht mehr funktionsfähig.
DES	Data Encryption Standard (DES) ist ein Verschlüsselungsverfahren (siehe Cipher). DES verwendet eine feste Blocklänge von 64 Bit. Die Schlüssellänge beträgt 56 Bit. Triple-DES oder 3DES basiert auf der dreimaligen Anwendung von DES (drei verschiedene unabhängige Schlüssel).
DFÜ	DFÜ steht für Datenfernübertragung.
DHCP	Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die dynamische Zuweisung von IP-Adressen. Ein DHCP-Server vergibt an jeden Client im Netzwerk eine IP-Adresse aus einem definierten Adress-Pool. Die Clients müssen dazu entsprechend konfiguriert sein.
DIME	Desktop Internetworking Management Environment (DIME) wird zur Konfiguration und Überwachung von Gateways verwendet.
DNS	Mithilfe des Domain Name System (DNS) wird der Domänenname

	(z. B. www.example.org) in eine IP-Adresse konvertiert (Namensauflösung).
Domäne	Ein Domäne ist ein zusammenhängender Teilbereich des DNS (z. B. example.org).
Downstream	Das Gateway erhält die Daten von einem übergeordneten Netz und reicht sie an sein angeschlossenes Netzwerk weiter.
DSA	Mithilfe des Digital Signature Algorithm (DSA) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über Signaturen können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. DSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch RSA. DSA ist schneller in der Schlüsselerzeugung aber langsamer in der Schlüsselverarbeitung als RSA.
DSCP	Datenpakete können mit einem Differentiated Services Codepoint (DSCP) ausgezeichnet werden. DSCP-Werte teilen Datenpakete in Klassen ein, sodass wichtige Pakete schneller durch das Netzwerk geleitet werden können. Siehe auch QoS.
DSL-Modem	Siehe Modem.
DSS1	Digital Subscriber Signalling System No. 1 (DSS1) ist ein Signalisierungsprotokoll für den D-Kanal des ISDN. Es ist auch bekannt als Euro-ISDN.
DTIM	Eine Delivery Traffic Indication Message informiert die Clients über auf dem Access Point vorhandene Multicast- bzw. Broadcast-Daten.
Durchwahl (VoIP)	Beim Durchwahl-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Point-Anschluss (Punkt-zu-Punkt) bezeichnet wird. Dieser dient zum Anschluss einer IP-TK-Anlage. Man erhält eine Basisrufnummer und einen Rufnummernblock. Die einzelnen Rufnummern im Rufnummernblock werden als Durchwahlausnahmen bezeichnet. (Beispiel: Basisrufnummer: 1234, Rufnummernblock: 1 - 99, Rufnummern der einzelnen Teilnehmer: 1234-1, 1234-2, 1234-3, ...)
Durchwahlausnahme	Siehe Anlagenanschluss und Durchwahl (VoIP).
Durchwahlbereich	Siehe Rufnummernblock bei Anlagenanschluss und Durchwahl (VoIP).
Durchwahlnummer	Siehe Anlagenanschluss und Durchwahl (VoIP).

Dynamische IP-Adresse	Im Gegensatz zu einer statischen IP-Adresse wird die dynamische IP-Adresse temporär per DHCP zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
DynDNS	Mithilfe eines DynDNS-Providers kann ein Domänenname auch mit einer dynamisch wechselnden IP-Adresse verknüpft werden.
Einzelrufnummer (VoIP)	Beim Einzelrufnummer-Anschluss handelt es sich um einen VoIP-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von VoIP-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Durchwahl (VoIP).
Encapsulation	Encapsulation (Einschließen) von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete in einem Netzwerk zu übertragen. Siehe auch VPN.
Encryption	Encryption bezeichnet die Verschlüsselung von Daten, z. B. mithilfe von MPPE.
ESP	Encapsulating Security Payload (ESP) ist ein Protokoll für IPSec. Es verwendet die Protokollnummer 50 und unterstützt Datenverschlüsselung sowie Authentifizierung.
Ethernet	Ethernet ist eine Spezifikation für kabelgebundene Datennetze. Ethernet arbeitet auf der ersten und zweiten Schicht des OSI-Modells.
Euro-ISDN	In Europa standardisiertes ISDN, basierend auf dem Signalisierungsprotokoll DSS1.
Eurofile-Transfer	EuroFile Transfer (EFT) ist ein Protokoll für den Austausch von Dateien über ISDN.
Filter	Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Treffen diese Kriterien für ein Datenpaket zu, kann das Datenpaket einer bestimmten Aktion (weiterleiten, ablehnen, ...) unterworfen werden. Dadurch entsteht eine Filterregel.
Filterregel	Eine Regel, die definiert, welche Datenpakete vom Gateway übertragen bzw. nicht übertragen werden sollen.
Firmware	Die Firmware (Systemsoftware) ist ein fest ins Gerät eingebetteter Programmcode. Mit dessen Hilfe werden die Funktionen des Geräts

bereitgestellt.

Fragmentierung	Falls die Gesamtlänge des Datenpakets größer als die Maximum Transmission Unit (MTU) der Netzwerkschnittstelle ist, muss das Datenpaket durch IP-Fragmentierung auf mehrere physikalische Datenblöcke aufgeteilt werden. Der umgekehrte Prozess wird Reassembly genannt.
Frame	Ein Datenframe ist eine Informationseinheit (Protocol Data Unit) auf der Sicherungsschicht des OSI-Modells
Frame Relay	Frame Relay ist eine Datenübertragungstechnik und Weiterentwicklung von X.25 (kleinere Pakete, weniger Fehlerprüfung). Frame Relay wird überwiegend für GSM-Netze verwendet.
FTP	Das File Transfer Protocol (FTP) regelt die Dateiübertragung in IP-Netzwerken. Es regelt den Austausch zwischen FTP-Server und Client.
Full-Duplex	Daten können bei Full-Duplex über eine Leitung gleichzeitig gesendet und empfangen werden.
G.991.1	Datenübertragungsempfehlung für HDSL.
G.991.2	Datenübertragungsempfehlung für SHDSL.
G.992.1	Datenübertragungsempfehlung für ADSL (G.DMT). Es existieren zwei länderspezifische Ausprägungen G.992.1 Annex A und G.992.1 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.2	Datenübertragungsempfehlung für ADSL (G.LITE / ADSL-Lite). Es existieren zwei Varianten G.992.2 Annex A und G.992.2 Annex B. Datentransferraten: 12 Mbit/s (Downstream), 1,3 Mbit/s (Upstream)
G.992.3	Datenübertragungsempfehlung für xDSL2. Es existieren drei Varianten: G.992.3 Annex A/B (G.DMT bis ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.3 Annex L (RE-ADSL2) mit Datenübertragungsraten von 5 Mbit/s im Downstream und 0,8 Mbit/s im Upstream und G.992.3 Annex M (ADSL2) mit Datenübertragungsraten von 12 Mbit/s im Downstream und 2,5 Mbit/s im Upstream.
G.992.4	Datenübertragungsempfehlung für ADSL2 mit Annex A/B. Datenübertragungsraten: 12 Mbit/s (Downstream), 1,0 Mbit/s (Upstream)
G.992.5	Datenübertragungsempfehlung für xDSL2+. Es existieren drei Vari-

anten: G.992.5 Annex A/B (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream, G.992.5 Annex L (RE-ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 1,0 Mbit/s im Upstream und G.992.5 Annex M (ADSL2+) mit Datenübertragungsraten von 25 Mbit/s im Downstream und 3,5 Mbit/s im Upstream.

G.993.1	Datenübertragungsempfehlung für VDSL. Datenübertragungsraten: 52 Mbit/s (Downstream), 16 Mbit/s (Upstream)
G.993.2	Datenübertragungsempfehlung für VDSL2. Datenübertragungsraten: 200 Mbit/s (Downstream), 200 Mbit/s (Upstream)
G.DMT	Siehe F.992.1.
G.Lite	Siehe F.992.2.
G.SHDSL	Siehe G.991.2.
Gateway	Das Gateway ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze.
GPRS	General Packet Radio Service (GPRS) ist die Bezeichnung für den paketorientierten Dienst zur Datenübertragung in GSM-Netzen.
GRE	Generic Routing Encapsulation (GRE) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. GRE verwendet die Protokollnummer 47.
GSM	Das Global System for Mobile Communications (GSM), auch als 2G bezeichnet, ist ein Mobilfunkstandard. Dieser erreicht zusammen mit GPRS eine spezifizierte max. Datenübertragungsrate von 171,2 kbit/s.
Half-Duplex	Daten können bei Half-Duplex über eine Leitung nur nacheinander gesendet und empfangen werden.
Hash	Zur Sicherstellung der Datenintegrität muss die Information vor unautorisierter Manipulation während der Übertragung geschützt werden. Um dies zu gewährleisten, muss jede empfangene Kommunikation mit der ursprünglich gesendeten Information übereinstimmen. Deshalb werden mathematische Streuwertfunktionen (Hashfunktionen) zur Berechnung von Prüfsummen (Hashwerten) verwendet. Diese werden verschlüsselt und mit der Nachricht als digitale Signatur versendet. Der Empfänger prüft wiederum die Signatur, bevor er das Paket öffnet. Falls sich die Signatur und damit der

	<p>Inhalt des Datenpakets geändert hat, wird das Paket verworfen. Die am häufigsten verwendeten Hash-Algorithmen sind Message Digest Version 5 (MD5) und Secure Hash Algorithm (SHA1).</p>
HDSL	<p>High Data Rate Digital Subscriber Line. Siehe DSL.</p>
Heartbeat	<p>Mithilfe von Heartbeat-Meldungen signalisieren die Teilnehmer eines Netzwerks ihre Empfangsbereitschaft.</p>
Hop	<p>Als Hop bezeichnet man die Verbindung von einem Netzwerkknoten zum nächsten.</p>
Host	<p>Ein Host ist ein Rechnersystem, das seine Dienste im Netzwerk zur Verfügung stellt.</p>
Host-Name	<p>Domänenname eines Host. Siehe DNS.</p>
Hostroute	<p>Eine Hostroute bezeichnet die Route zu einem einzelnen Host.</p>
Hotspot	<p>Ein Hotspot ist ein öffentlicher Internetzugangspunkt über WLAN oder kabelgebundenes Ethernet.</p>
HSDPA	<p>High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ oder UMTS-Broadband) ist ein Datenübertragungsverfahren des Mobilfunkstandards UMTS.</p>
HTTP	<p>Das HyperText Transfer Protocol (HTTP) ist ein Protokoll zur Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. Es verwendet standardmäßig den Port 80.</p>
HTTPS	<p>Das HyperText Transfer Protocol Secure (HTTPS) ist ein Protokoll zur abhörsicheren Übertragung von HTML-Seiten (Web-Seiten) zwischen Server und Client. HTTPS ist schematisch identisch zu HTTP. Für die zusätzliche Verschlüsselung der Daten wird SSL / TLS verwendet. Der Standard-Port für HTTPS-Verbindungen ist 443.</p>
Hyperchannel	<p>Beim Hyperchannel haben mehrere Teilnehmer Zugriff auf das Übertragungsmedium. Ein Teilnehmer kann seine Informationen nur übertragen, wenn kein anderer Teilnehmer das Medium belegt. Ein Hyperchannel-Netzwerk dient hauptsächlich für Kurzstreckenbetrieb mit höchsten Datenraten.</p>
ICMP	<p>Das Internet Control Message Protocol (ICMP) dient dem Austausch von Informations- und Fehlermeldungen über IPv4. Für IPv6 existiert die Version ICMPv6.</p>

IGMP	Das Internet Group Management Protocol (IGMP) dient in IPv4-Netzen zur Organisation von Multicast-Gruppen.
IKE	Das Internet-Key-Exchange-Protokoll (IKE) dient der automatischen Schlüsselverwaltung bei IPSec-Verbindungen. Der IKE-Prozess verläuft in zwei Phasen. Während Phase 1 authentifizieren sich die IKE-Teilnehmer gegenseitig und etablieren einen sicheren Kanal. In Phase 2 handeln die beiden IPSec-Teilnehmer die SAs aus. Es existieren zwei Versionen des IKE-Mechanismus.
Infrastruktur-Netzwerk	In einem Infrastruktur-Netz bilden die einzelnen Endgeräte (Clients) über einen zentralen Knotenpunkt (Access Point) ein Wireless LAN. Dieser zentrale Access Point kann dabei auch ein Vermittler in weitere Netze sein.
IP	Das Internet Protocol (IP) ist ein Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es arbeitet auf der Vermittlungsschicht des OSI-Modells. Auf IP bauen die Protokolle TCP und UDP auf. Es existieren zwei Versionen Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6).
IP-Adresse	IP-Adressen werden zur Navigation in einem IP-Netzwerk verwendet, um Quelle und Ziel eindeutig zu bestimmen. IPv4-Adressen bestehen aus 32 Bits, IPv6-Adressen aus 128 Bits. Damit sind bei IPv4 232, also 4.294.967.296 Adressen darstellbar, bei IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 Adressen. Für IPv4 wird die Dezimaldarstellung (dotted decimal notation) verwendet, z. B. 192.168.0.250. Für IPv6 wird die Hexadezimaldarstellung verwendet, z. B. 2001:db8:85a3::8a2e:370:7344. Siehe auch Netzmaske.
IPCP	Das Internet Protocol Control Protocol (IPCP) dient, analog zu DHCP, zur Konfiguration eines Host mit IP-Adresse, Gateway und DNS-Server, falls eine PPP-Netzwerkverbindung verwendet wird. Mithilfe der Erweiterung Robust Header Compression over PPP kann der Header für eine schnellere Datenübertragung komprimiert werden. Analog wird in IPv6-Netzwerken die Funktionalität durch das Internet-Protocol-Version-6-Control-Protokoll (IPv6CP) bereitgestellt.
IPSec	IPSec (Internet Protocol Security) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. Die Protokollnummer für IPSec ist dabei vom verwendeten Protokoll abhängig. Der Authentication-Header (AH) verwendet die Protokollnummer 51, das Encapsulating-Security-Payload (ESP) die Nummer 50.

IPv6	Siehe IP.
ISDN	Integrated Services Digital Network (ISDN) ist ein Datenübertragungsstandard, der Telefonie, Telefax und Datenübertragung umfasst. Es existieren zwei ISDN-Anschluss-Varianten: Basisanschluss und Primärmultiplexanschluss.
ISDN-Adresse	Die ISDN-Adresse eines ISDN-Geräts setzt sich zusammen aus einer ISDN-Nummer gefolgt von weiteren Ziffern, die sich auf das spezifische Endgerät beziehen.
ISDN-Login	Über ISDN-Login ist das Gerät über SNMP fernkonfigurierbar. Es muss dazu einen konfigurierten ISDN- oder Mobilfunk-Anschluss besitzen.
ISDN-Nummer	Die ISDN-Nummer ist die Netzwerkadresse der ISDN-Schnittstelle.
ISDN-Router	Siehe Router.
ISP	Internet Service Provider (ISP) sind Anbieter technischer Leistungen zur Nutzung des Internets.
ITU	Die International Telecommunication Union (ITU) koordiniert den Aufbau und Betrieb von Telekommunikationsnetzen und Diensten.
Kanal	Ein Funkkanal ist ein für Wireless LAN genutztes Frequenzband. Geräte, die auf benachbarten Kanälen senden, stören sich gegenseitig.
Kanalbündelung	Bei der Kanalbündelung werden die B-Kanäle einer ISDN-Verbindung zusammengefasst, um den Datendurchsatz zu erhöhen.
Keepalive	Mit Keepalive-Paketen wird die Erreichbarkeit des Kommunikationspartners überprüft.
Keepalive	Keepalive ist ein Mechanismus zur Aufrechterhaltung der Netzwerkverbindung und zur Überprüfung der Erreichbarkeit der Kommunikationspartner. Dazu werden in der Regel spezifische Pakete ins Netzwerk gesendet.
Konfiguration	Alle Einstellungen des Geräts werden als Konfiguration bezeichnet. Diese Konfiguration ist intern in MIB-Tabellen gespeichert. Diese Informationen können extern gespeichert, von extern geladen oder gelöscht werden. Bearbeitet wird die Konfiguration über die HTTP(S)-Benutzeroberfläche, einen SNMP-Client oder angeschlossene Telefone.

L2TP	Das Layer 2 Tunneling Protocol (L2TP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über verschiedene Protokolle zu transportieren. L2TP verwendet standardmäßig die Protokollnummer 1701. Die Architektur eines L2TP-Netzwerks besteht aus einem L2TP-Access-Concentrator (LAC), der auch fest in den Client integriert sein kann, und dem L2TP-Network-Server (LNS). Der LAC stellt die Verbindungen zum LNS her und verwaltet diese. Die Autorisierung wird über einen Network-Access-Server (NAS), der im LAC oder LNS implementiert sein kann, geregelt. Der LNS ist für das Routing und die Kontrolle der vom LAC empfangenen Pakete zuständig. Die eigentlichen Nutzdaten werden unverschlüsselt ausgetauscht, während Kontrollnachrichten zur Aufrechterhaltung der Erreichbarkeit der Tunnelendpunkte abgesichert übertragen werden.
LAC	Siehe L2TP.
LAN	Ein Local Area Network (LAN) bezeichnet ein räumlich eng begrenztes Netzwerk und umspannt meist ein Gebäude oder einen Firmensitz.
Lastverteilung	Bei der Lastverteilung werden Daten über unterschiedliche Schnittstellen gesendet, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen. Im Unterschied zu Multilink funktioniert die Lastverteilung auch mit Accounts zu unterschiedlichen Providern.
Layer	Ein Layer bezeichnet eine Schicht im OSI-Modell.
LCP	Das Link Control Protocol (LCP) wird in PPP-Verbindungen verwendet, um die Einkapsulierung automatisch auszuhandeln, Grenzen für variierende Paketgrößen zu verarbeiten, den Verbindungspartner zu authentifizieren, einen defekten Link zu bestimmen, Verbindungsfehler zu erkennen und die Verbindung zu beenden.
LDAP	Das Lightweight Directory Access Protocol (LDAP) regelt die Kommunikation zwischen einem Client und dem Directory-Server. LDAP wird für den Austausch und die Aktualisierung von Verzeichnissen, z. B. ein Telefonbuch, verwendet.
Lease Time	Die Lease Time bezeichnet die Gültigkeitsdauer einer dynamischen IP-Adresse, die ein Client von einem DHCP-Server erhalten hat.
Leased Line	Siehe Standleitung.
LLC	Die Link Layer Control (LLC) regelt die Medienzuteilung auf MAC-Ebene.

LNS	Siehe L2TP.
Loopback	Bei einer Loopback-Schaltung sind Sender und Empfänger identisch.
LTE	Long Term Evolution (LTE), auch als 4G bezeichnet, ist ein Mobilfunkstandard mit einer standardisierten max. Datenübertragungsrate von 300 Mbit/s.
MAC-Adresse	Die Media-Access-Control-Adresse (MAC-Adresse) ist die Hardware-Adresse des Netzwerkadapters und dient zur Identifizierung des Geräts auf Hardware-Ebene.
Main Mode	Beim Aufbau einer IPSec-Verbindung wird der Main Mode zur Realisierung eines Phase-1-Austausches verwendet, indem ein sicherer Kanal eingerichtet wird. Siehe auch Aggressive Mode.
Man-in-the-Middle Attack	Im Man-in-the-middle-Angriff befindet sich der Angreifer physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kann somit den Datenverkehr einsehen und sogar manipulieren.
MD5	Message-Digest Algorithm 5 (MD5) ist eine Hashfunktion, die einen 128-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
Media Gateway	Ein Media Gateway wandelt den Netzwerktyp von digitalen Sprach-, Audio- oder Bildinformationen um. Beispielsweise können die Signale eines ISDN-Netzwerks auf ein IP-Netzwerk umgesetzt werden.
Mehrfachrufnummer (MSN)	MSNs (Multiple Subscriber Number) sind die einzelnen Rufnummern des ISDN-Mehrgeräteanschlusses.
Mehrgeräteanschluss	Beim Mehrgeräteanschluss handelt es sich um einen ISDN-Anschluss, der auch als Point-to-Multipoint-Anschluss (Punkt-zu-Mehrpunkt) bezeichnet wird. Dieser dient zum Anschluss von ISDN-Endgeräten. Man erhält Einzelrufnummern (MSNs). Siehe auch Anlagenanschluss.
Metrik	Die Metrik ist eine Maß für die Güte der Route. Die schnellste Route weist dabei die geringste Metrik (costs, »Kosten«) auf. Vereinfacht ist dies die Verbindung mit der kleinsten Anzahl an Knotenpunkten (Routern).
MIB	Die Management Information Base (MIB) beschreibt die Informationen, die über ein Netzwerk-Management-Protokoll (z. B. SNMP) abgefragt oder modifiziert werden können. Die MIB ist eine Datenbank, die alle Geräte und Funktionen im Netzwerk beschreibt.

MLP	Das Multicast Listener Discovery (MLD) dient in IPv6-Netzen zur Organisation von Multicast-Gruppen.
Modem	Ein Modem ist ein elektronisches Gerät, das digitale Signale in Frequenzsignale umwandelt, um Daten in einem Kabel- oder Mobilfunknetz zu verbreiten.
MPDU	Die MAC Protocol Data Unit (MPDU) bezeichnet ein per Funkmedium ausgetauschtes Informationspaket, inklusive Management-Frames und fragmentierten MSDUs.
MPPC	Microsoft Point-to-Point Compression (MPPC) ist ein Datenkompressionsverfahren.
MPPE	Microsoft Point-To-Point Encryption (MPPE) wird zur Verschlüsselung von Daten, die über PPP übertragen werden, eingesetzt. Es wurde von Microsoft und Cisco entwickelt und als RFC 3078 spezifiziert.
MS-CHAP	Das Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) ist ein Authentisierungsverfahren. MS-CHAPv1 ist für die Authentifizierung von DFÜ-Verbindungen gedacht und entspricht in weiten Teilen dem standardmäßigen CHAP. MS-CHAPv2 ist ein Authentisierungsverfahren für PPTP-Verbindungen (VPN).
MSDU	Eine MAC Service Data Unit (MSDU) ist ein Datenpaket, das auf LLC-Ebene ausgetauscht wird.
MSN	Siehe Mehrfachrufnummer.
MSS	Die Maximum Segment Size (MSS) definiert die maximale Anzahl an Bytes, die als Nutzdaten in einem TCP-Segment versendet werden können. Die MSS muss kleiner als die Maximum Transmission Unit (MTU) sein, um eine Fragmentierung der IP-Pakete zu vermeiden.
MSS Clamping	Bei MSS Clamping wird die Maximum Segment Size (MSS) reduziert, um Netzwerke mit verschiedenen Maximum Transmission Units (MTU) zu verbinden.
MTU	Die Maximum Transmission Unit (MTU) ist die größtmögliche über eine physikalische Leitung übertragbare Dateneinheit.
Multicast	Bei einem Multicast werden Datenpakete von einem Punkt an bestimmte Teilnehmer eines Netzes übertragen. In IPv4 wird dies über den Adress-Bereich 224.0.0.0 bis 239.255.255.255 und das Protokoll IGMP gesteuert, in IPv6 über ff00::/8-Adressen und ICMPv6.

Multilink	Bei Multilink werden mehrere Schnittstellen (PPP, PPPoE, ...) zu einer einzigen virtuellen Verbindung zusammengefasst, um die zur Verfügung stehende Gesamtbandbreite zu erhöhen.
NAPT	Network Address Port Translation (NAPT) ist eine andere Bezeichnung für PAT. Siehe PAT.
NAT	Mithilfe von Network Address Translation (NAT) werden die Quell- und Ziel-IP-Adressen eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch PAT.
NBNS	NetBIOS Name Service (NBSN) dient wie DNS der zentralen Namensauflösung. Siehe auch WINS und DNS.
Netzabschluss	Der Netzabschluss (Network Termination, NT) bezeichnet einen Anschluss bzw. eine Betriebsart. Am NT-Anschluss (Anschlussdose) wird einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt. Beim analogen Anschluss wird die Steckdose TAE genannt, beim ISDN-Basisanschluss NTBA und beim ISDN-Primärmultiplexanschluss NTPMGF. Im NT-Betrieb wird das Gateway am externen S0 der Telefonanlage angeschlossen und stellt für diese einen externen Amtsanschluss dar. Siehe auch TE.
Netzmaske	Die Netzmaske, auch Netzwerkmaske oder Subnetzmaske, definiert bei IPv4 in Verbindung mit der IP-Adresse das Netzwerk, indem sie die IP-Adresse in einen Netzwerk- und einen Geräteanteil aufteilt und somit bestimmt, welche Adressen geroutet werden müssen. Beispiel einer Netzmaske: 255.255.255.0. Bei IPv6 spricht man von der Präfixlänge.
Netzwerkadresse	Eine Netzadresse (Präfix) bezeichnet die Adresse des gesamten Netzwerks. Die Netzwerkmaske bzw. Präfixlänge unterteilt die IP-Adresse in die Netzadresse und Host-Adresse (Geräteadresse). Beispiel für eine Netzadresse: 192.168.0.250/24
Netzwerkroute	Die Netzwerkroute bezeichnet die Route zu einem bestimmten Netzwerk.
NT	Siehe Netzabschluss.
NTP	Das Network Time Protocol (NTP) dient zur Synchronisation der Uhrzeit.
OAM	OAM ist ein Dienst zur Überwachung von ATM-Verbindungen.
OSI-Modell	Das OSI-Modell gliedert den Ablauf der Kommunikation zwischen

physikalischem Medium und Anwenderebene in Schichten. Die Anforderungen jeder Schicht werden durch entsprechende Protokolle erfüllt.

OSPF	OSPF ist ein dynamisches Routing-Protokoll das meist in größeren Netzwerk-Installationen als eine Alternative zu RIP verwendet wird.
PAP	Das Password Authentication Protocol (PAP) ist ein Authentisierungsverfahren für Verbindungen über PPP. Im Gegensatz zu CHAP werden Benutzername und Passwort nicht verschlüsselt übertragen.
PAT	Mithilfe von Port and Address Translation (PAT) werden die Quell- und Ziel-IP-Adressen sowie die Quell- und Ziel-Ports eines Datenpakets durch andere ersetzt. Dadurch können unterschiedliche Netze miteinander verbunden werden. Siehe auch NAT.
Peer	Ein Peer ist der Endpunkt einer Kommunikation im Netzwerk.
Phase-1/2	Siehe IKE.
PIM	Das Protocol Independent Multicast (PIM) ermöglicht dynamisches Routing von Multicast-Paketen im Internet.
Ping	Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist. Daneben wird die Zeitspanne zwischen dem Aussenden eines Datenpakets (ICMP(v6)-Echo-Request-Paket) und dem Empfangen eines daraufhin unmittelbar zurückgeschickten Antwortpakets gemessen. Dadurch kann die Qualität der Verbindung ermittelt werden.
PKCS	Die Public-Key Cryptography Standards (PKCS) beinhalten Standards für Public-Key-Kryptografie. Die PKCS sind konzipiert für binäre und ASCII-Daten und sind kompatibel mit dem X.509-Standard. Die veröffentlichten Standards sind PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12, und #15. PKCS #10 beschreibt die Syntax für Zertifizierungsanfragen.
PKI	Mithilfe einer Public-Key-Infrastruktur (PKI) werden digitale Zertifikate für ein Verschlüsselungsverfahren ausgestellt, verteilt und geprüft.
PMTU	Die Path MTU (PMTU) beschreibt die maximale Paketgröße, die entlang der gesamten Verbindungsstrecke übertragen werden kann, ohne einer Fragmentierung zu unterliegen.
Point-to-Multipoint	Siehe Mehrgeräteanschluss und Einzelrufnummer (VoIP).

Point-to-Point	Siehe Anlagenanschluss und Durchwahl (VoIP).
Pool	Ein Address-Pool ist eine Ansammlung von IP-Adressen, die den angeschlossenen Clients z. B. per DHCP zugewiesen werden können.
POP3	Das Post Office Protocol Version 3 (POP3) ist ein Übertragungsprotokoll, um den E-Mail-Abruf von einem E-Mail-Server durch einen Client zu steuern.
Port	Anhand der Port-Nummer wird entschieden, an welchen Dienst (Telnet, FTP, ...) ein ankommendes Datenpaket weitergeleitet wird.
PPP	Das Point-to-Point Protocol (PPP) ist eine standardisierte Technologie, um eine direkte Verbindung zwischen den Netzwerkknoten über Wählleitungen einzurichten.
PPPoA	Das Point-to-Point-over-ATM Protocol (PPPoA) ermöglicht, PPP-Datenpakete direkt über ein ATM-Netzwerk zu transportieren.
PPPoE	Das Point-to-Point-over-Ethernet Protocol (PPPoE) ermöglicht, PPP-Datenpakete direkt über ein Ethernet-Netzwerk zu transportieren.
PPTP	Das Point-to-Point Tunneling Protocol (PPTP) ist ein Netzprotokoll zur Einkapselung anderer Protokolle, um sie so in Form eines Tunnels (VPN) über das Internet Protocol (IP) zu transportieren. PPTP verwendet die Protokollnummer 1723. Die PPTP-Architektur teilt sich in zwei logische Systeme. Den PPTP-Access-Concentrator (PAC) und den PPTP-Network-Server (PNS). Der PAC ist üblicherweise in den Windows Client integriert. Er stellt die Verbindung zum PNS her und verwaltet diese. Der PNS ist für das Routing und die Kontrolle der vom PNS empfangenen Pakete zuständig.
Präfix	Siehe Netzwerkadresse.
Präfixdelegation	In IPv6-Netzwerken wird die Präfixdelegation zur Zuteilung der Netzwerkadresse (Präfix) an den Router verwendet.
Präfixlänge	Siehe Netzmaske.
Preshared Key	Ein Preshared Key (PSK) ist ein Schlüssel für ein Verschlüsselungsverfahren. Der Schlüsselwert wurde zwischen den Teilnehmern vorher anderweitig ausgetauscht.
PRI	Siehe Primärmultiplexanschluss.

Primärmultiplexanschluss	Der Primärmultiplexanschluss ist ein Netzanschluss an das ISDN. Eine andere Bezeichnung für diese Anschlussart ist Primary Rate Interface (PRI) oder S2M-Anschluss. Ein Primärmultiplexanschluss bietet in Europa 30 und in den USA 23 Nutzkanäle (B-Kanäle) mit je 64 kbit/s, einen Steuerkanal (D-Kanal) mit 64 kbit/s und einen Synchronisationskanal mit 64 kbit/s in Europa und 8 kbit/s in den USA. Siehe auch Basisanschluss.
Proposal	Beim Aufbau einer IPSec-Verbindung werden vom Initiator der Verbindung Vorschläge (Proposals) bezüglich der zu verwendenden Authentifizierungs- und Verschlüsselungsverfahren.
Protokoll	Protokolle regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen des OSI-Modells. Protokolle steuern Adressierung, Codierung, Authentifizierung, Formatierung, usw. Beispiele: Ethernet, IP, TCP, HTTP
Proxy	Ein Proxy ist eine Netzwerkkomponente. Der Proxy ist ein Vermittler. Er leitet eine Anfrage der Quelle mit seiner eigenen IP-Adresse an das Ziel weiter.
PVID	Der Port VLAN Identifier (PVID) ist die Standard-VLAN-ID des jeweiligen Ports. Ein Paket, das ohne VLAN-Tag diesen Port erreicht, wird mit dieser ID versehen.
Q-SIG	Q-Interface Signalling Protocol (Q-SIG) ist ein ISDN-basiertes Signalisierungsprotokoll für die Vernetzung von Telefonanlagen.
QoS	Quality of Service (QoS) beschreibt die Qualität (Güte) des Kommunikationsdienstes. Diese wird anhand von Bandbreite, Verzögerung, Paketverlusten und Jitter definiert. Um zeitkritische Datenpakete für VoIP oder Videostreaming möglichst schnell zu übertragen, werden alle Datenpakete bei QoS in Gruppen sortiert und entsprechend ihrer Priorität im Netzwerk schneller oder langsamer weitergeleitet.
Queue	In einer Warteschlange (Queue) laufen die Datenpakete auf, bevor sie versendet werden.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen. Der RADIUS-Server authentifiziert den Client z. B. mittels der Überprüfung von Benutzername und Kennwort. Siehe auch TACACS+.
RE-ADSL2	Siehe G.992.5.

Real Time Jitter Control	Über die Real Time Jitter Control werden Datenpakete während eines Telefongesprächs bei Bedarf in der Größe reduziert, damit Sprachpakete nicht blockiert werden.
Regelkette	In einer Regelkette sind unterschiedliche Filterregeln zusammengefasst. Eine Filterregel wählt einen Teil des Datenverkehrs aufgrund bestimmter Merkmale, z. B. der Quell-IP-Adresse, aus und wendet auf diese Teilmenge eine Aktion an, z. B. blockieren.
Registrar	Der SIP-Server (Registrar) muss eingesetzt werden, falls die Teilnehmer eines VoIP-Gesprächs keine statischen IP-Adressen verwenden. Der SIP-Server registriert die IP-Adressen der Clients und sendet diese Informationen an den SIP-Proxy, der die Anrufe vermittelt. Meistens sind SIP-Proxy und SIP-Registrar identisch.
Repeater	Ein Repeater ist ein Gerät, das elektrische oder optische Signale verstärkt und somit die Reichweite des Netzwerks erhöht.
Reset	Ein Reset setzt das Gerät in einen unkonfigurierten Zustand zurück.
RFC	Ein Request For Comments (RFC) ist ein Dokument, das Standards und Richtlinien für das Internet beschreibt.
Rijndael	Siehe AES.
RIP	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll. Es ist auf kleine Netzwerke begrenzt. Siehe auch OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
RJ45	RJ45 bezeichnet einen Stecker bzw. eine Buchse mit maximal acht Adern zum Anschluss digitaler Endgeräte.
Roaming	Beim Roaming bewegt sich ein Client durch ein WLAN und meldet sich dabei an verschiedenen Access Points des gleichen Netzes an und wieder ab.
Router	Ein Router ist eine Netzwerkkomponente zum Verbinden verschiedenartiger Netze auf der Vermittlungsschicht des OSI-Modells. Datenpakete werden anhand von IP-Adressen übertragen. Über Routing-Tabellen werden die besten Wege (Routen) durch das Netzwerk festgelegt. Um die Routing-Tabellen auf dem Laufenden zu halten, tauschen die Router untereinander Informationen über Routing-Protokolle, z. B. OSPF oder RIP, aus.

Router Advertisement	Router Advertisements sind Nachrichten, die der Router ins Netzwerk sendet. Diese verkünden die Anwesenheit des Routers im Netz. Ferner werden mithilfe von Router Advertisements Präfixe verteilt, die Autokonfiguration organisiert und der Standardrouter festgelegt.
Routing	Routing bezeichnet das Festlegen von Wegen für die Nachrichtenübermittlung.
RSA	Mithilfe des RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Shamir, Adleman) werden digitale Signaturen erstellt und Datenpakete verschlüsselt. Über die Signatur können Veränderungen an den Informationen des Datenpakets nachgewiesen werden. RSA wird für Public-Key-Kryptographie (IPSec) verwendet. Siehe auch DSA. RSA ist langsamer in der Schlüsselerzeugung aber schneller in der Schlüsselverarbeitung als DSA.
RTP	Mit dem Real-Time Transport Protocol (RTP) werden Audio- und Video-Daten (Streams) über IP-basierte Netzwerke übertragen.
RTS Threshold	Sobald die Anzahl der Frames im Datenpaket über der RTS-Schwelle (RTS Threshold) liegt, wird vor dem Senden eines Datenpakets eine Verbindungsüberprüfung (RTS/CTS-Handshake) durchgeführt.
RTSP	Das Real-Time Streaming Protocol (RTSP) steuert die Übertragung von Audio- und Videodaten (Streams) über IP-basierte Netzwerke. Während das Real-Time Transport Protocol (RTP) zur Übertragung der Nutzdaten dient, besteht die Funktion von RTSP hauptsächlich in der Steuerung der Datenströme.
S2M-Anschluss	Siehe Primärmultiplexanschluss.
SA	Eine sogenannte Sicherheitsverbindungen (Security Associations, SA) enthält Informationen über die Maßnahmen zur Sicherung der Kommunikationsverbindung. Mindestens eine SA ist die Voraussetzung für den Aufbau einer gesicherten Verbindung. Eine SA enthält die IP-Adresse des Teilnehmers, das verwendete Authentifizierungsprotokoll, den verwendeten Verschlüsselungsalgorithmus, den Sicherheits-Parameter-Index (SPI), den Selektor und die Gültigkeitsdauer.
SAD	Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die SAD enthält Informationen über

jede Sicherheitsverbindung. Also welche Verschlüsselungsalgorithmen, Schlüssel, Protokolle, Sitzungsnummern oder Gültigkeitszeiträumen verwendet werden sollen. Für eine ausgehende Verbindung zeigt ein Eintrag der SPD auf einen Eintrag der SAD. Dadurch kann die SPD festlegen, welcher SA für ein bestimmtes Paket verwendet wird. Bei einer eingehenden Verbindung wird die SAD angesprochen, um festzulegen, wie das Paket verarbeitet wird.

SCEP	Das Simple Certificate Enrollment Protocol (SCEP) dient zur Verwaltung digitaler Zertifikate.
Scheduling	Unter Scheduling versteht man einen Aufgabenplan. Bestimmte Aktionen (z. B. Deaktivierung einer Schnittstelle) werden durch Ereignisse (z. B. Zeit oder Änderung einer MIB-Variablen) ausgelöst.
Serielle Schnittstelle	Die serielle Schnittstelle dient dem Datenaustausch zwischen Computern und Peripheriegeräten. Sie kann zur Konfiguration des Geräts oder zur Datenübertragung über eine IP-Infrastruktur verwendet werden (Serial over IP).
Server	Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden.
SFP	Small Form-factor Pluggable (SFP) ist eine Steckverbindung, die für extrem schnelles Ethernet entwickelt wurde.
SHA1	Secure-Hash-Algorithm Version 1 (SHA1) ist eine Hashfunktion, die einen 160-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
SHDSL	Symmetrical High-bit-rate Digital Subscriber Line. Siehe DSL.
Shell	Die Shell ist eine Eingabeschnittstelle (z. B. Kommandozeile oder grafische Benutzerschnittstelle) zwischen Computer und Benutzer.
Shorthold	Der Shorthold bezeichnet die definierte Zeit, nach der eine Netzwerkverbindung automatisch abgebaut wird, falls keine Daten mehr übertragen werden.
SIF	Bei einer Stateful Inspection Firewall (SIF) wird die Weiterleitung eines Datenpakets nicht nur durch Quell- und Zieladressen oder Port bestimmt, sondern auch mittels dynamischer Paketfilterung aufgrund des Zustands (Status) der Verbindung.
SIP	Das Session Initiation Protocol (SIP) ist ein Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei oder mehr Teilnehmern. Das Protokoll wird für IP-Telefonie (VoIP) verwendet.

SIP-Provider	Ein SIP-Provider übernimmt die Vermittlung zwischen einem SIP-Anschluss und anderen analogen, ISDN- und VoIP-Anschlüssen.
SNMP	Mithilfe des Simple Network Management Protocol (SNMP) werden verschiedene Netzwerkkomponenten (z. B. Router, Server, usw.) von einem zentralen System aus konfiguriert, kontrolliert und überwacht. Die änderbaren Einstellungen der Netzwerkkomponenten sind dabei in einer Datenbank gespeichert – der Management Information Base (MIB). SNMP verwendet UDP. Die Netzwerkkomponente empfängt dabei Anfragen (Requests) auf Port 161, während das verwaltende System Bestätigungsmeldungen (TRAPs) auf Port 162 entgegennimmt.
Spatial Streams	Spatial Streams sind Datenströme, die im Wireless LAN zur gleichen Zeit auf der gleichen Frequenz ausgesendet werden. Dies führt zu einer Vervielfachung der Übertragungsrates.
SPD	Alle Parameter, die während der Konfiguration von IPSec festgesetzt werden, sind in Form von Datenbanken im Router abgelegt. Dies sind die Security-Policy-Datenbank (SPD) sowie die Security-Association-Datenbank (SAD). Die Security-Policy-Datenbank führt die Formen des Datenverkehrs auf, die gesichert werden sollen. Dazu werden Faktoren wie Quell- und Zieladresse des Datenpakets verwendet.
SRTP	Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die mithilfe von AES verschlüsselte Variante des Real-Time Transport Protocol (RTP).
SSH	Secure Shell (SSH) ist ein Netzwerkprotokoll mit dem man eine verschlüsselte Verbindung zur Shell eines Geräts herstellen kann.
SSID	Der Service Set Identifier (SSID) definiert ein Funknetzwerk, das auf IEEE 802.11 basiert. Der SSID ist der Netzwerkname des Wireless LAN. Alle Access Points und Clients, die zum gleichen Netzwerk gehören, verwenden denselben SSID. Die SSID-Zeichenfolge kann bis zu 32 Zeichen lang sein und wird allen Paketen unverschlüsselt vorangestellt. Mithilfe der SSID ANY kontaktiert ein Client alle erreichbaren Access Points. Dem Anwender werden daraufhin alle verfügbaren WLANs angezeigt und er kann das passende Netz auswählen. Wenn ein Access Point für verschiedene Netze verwendet wird, erhält jedes Funknetzwerk eine eigene MSSID (Multi Service Set Identifier).
SSL	Secure Sockets Layer (SSL) ist ein Protokoll zur Datenverschlüsselung. Seit Version 3.1 wird die neue Bezeichnung Transport Layer

Security (TLS) verwendet. SSL wird hauptsächlich für HTTPS verwendet, um die Datenübertragung zwischen Web-Server und Web-Browser zu verschlüsseln.

STAC	Mithilfe von STAC wird die übertragene Datenmenge verringert (Datenkompression).
Standardroute	Die Standardroute (Default Route) wird verwendet, falls keine andere passende Route vorhanden ist.
Standardrouter	Siehe Default Gateway.
Standleitung	Eine Standleitung (Leased Line) ist eine permanente Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetz.
Statische IP-Adresse	Im Gegensatz zu einer dynamischen IP-Adresse wird die statische IP-Adresse fest vom Anwender zugeordnet. Netzwerkkomponenten wie Web-Server oder Drucker besitzen in der Regel statische IP-Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP-Adressen.
STUN-Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). Ein STUN-Server ermöglicht VoIP-Geräten hinter einem aktivierten NAT den Zugang zum Netzwerk.
Subadressierung	Neben der ISDN-Telefonnummer kann eine Subadresse beim Verbindungsaufbau übertragen werden. Diese Subadresse überträgt eine beliebige Zusatzinformation. Diese kann genutzt werden, um z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt anzusprechen oder bestimmte Programme auf einem PC aufzurufen.
Subnetz	Ein Teilnetz eines IP-Netzes wird als Subnetz bezeichnet. Ein Teilnetz wird wie ein normales Netzwerk über IP-Adresse und (Sub-)Netzmaske (IPv4) bzw. Präfixlänge (IPv6) definiert. Beispiel: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 mögliche IP-Adressen) ist ein Subnetz von 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 mögliche IP-Adressen).
Switch	Ein Switch ist eine Netzwerkkomponente, die einzelne Netzwerkkomponenten miteinander verbindet. Ein Switch kann einerseits als Bridge auf der Sicherungsschicht des OSI-Modells betrieben werden. Ein Switch besitzt aber im Gegensatz zur Bridge mehrere Ein- und Ausgänge. Andererseits kann der Switch als Gateway auf der Vermittlungsschicht des OSI-Modells betrieben werden. Das dem

	Switch vergleichbare Gerät der Bitübertragungsschicht wird als Hub bezeichnet.
SWYX	SwyxWare ist eine softwarebasierte Kommunikationslösung für VoIP.
Syslog	Das Syslog-Protokoll wird zur Übermittlung von Status-Meldungen in einem IP-Netzwerk verwendet. Verschiedene Netzwerkkomponenten können somit von einem zentralen System aus überwacht werden. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP-Port 514 gesendet.
T.38	T.38 oder Fax over IP (FoIP) bezeichnet die Faxübertragung über ein IP-Netzwerk.
TACACS+	Das Terminal Access Controller Access Control System Plus (TACACS+) ist ein Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern. Der TACACS+-Server authentifiziert den Client mittels der Überprüfung von z. B. Benutzername und Kennwort. Im Gegensatz zum UDP-basierten RADIUS-Protokoll verwendet TACACS+ TCP auf Port 49 und überträgt die gesamte Kommunikation verschlüsselt.
TAPI	Telephony Applications Programming Interface (TAPI) ist eine Programmierschnittstelle für ISDN. Diese ermöglicht es Anwendungsprogrammen, von einem PC aus auf ISDN-Hardware zuzugreifen. Siehe auch CAPI.
TCP	Beim Transmission Control Protocol (TCP) handelt es sich um ein verbindungsorientiertes Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungsorientierten Protokoll wird vor der Übertragung eine logische Verbindung aufgebaut und aufrechterhalten. Dies ermöglicht eine zuverlässige Übertragung der Daten. Allerdings werden ständig Kontrollinformationen neben dem eigentlichen Datenpaketen übertragen. Dies führt zu einem Anstieg des übertragenen Datenvolumens. Siehe auch UDP.
TCP-ACK-Paket	Ein ACK-Signal (Acknowledgement = Bestätigung) wird bei einer Datenübertragung verwendet, um den Erhalt oder die Verarbeitung von Daten oder Befehlen zu bestätigen. TCP verwendet ACK-Signale zur Kommunikation.
TE	Der Endgeräteanschluss (Terminal Equipment, TE) bezeichnet einen Anschluss bzw. eine Betriebsart. Der TE-Anschluss ist der Anschluss eines Endgeräts. Im TE-Betrieb wird das Gateway am internen S0 der Telefonanlage angeschlossen und stellt damit ein

	ISDN-Endgerät dar. Siehe auch NT.
Telnet	Telecommunication Network (Telnet) ist ein Netzwerkprotokoll. Es ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk, z. B. PCs, Routern, usw.
TFTP	Das Trivial File Transfer Protocol (TFTP) regelt die Übertragung von Dateien. Im Vergleich zu FTP fehlen eine Möglichkeit zur Dateianzeige, eine Rechtevergabe und eine Benutzerauthentifizierung.
Tiger 192	Tiger 192 ist eine Hashfunktion, die einen 192-Bit-Hashwert (Prüfsumme) erzeugt. Siehe auch Hash.
TLS	Siehe SSL.
TOS	Type of Service (TOS) ist eine Feld im Header von IP-Datenpaketen. Es legt die Priorität des Datenpakets fest. Siehe auch QoS.
Traceroute	Mithilfe von Traceroute wird ermittelt, über welche Router Datenpakete bis zum abgefragten Ziel-Host vermittelt werden.
Trigger	Unter Trigger versteht man einen Auslöseimpuls.
Triple DES	Siehe DES.
TTL	Die Time to live (TTL) ist die konfigurierte Gültigkeitsdauer eines Datenpakets. Beim Internet Protocol (IP) legt die TTL fest, wie viele Hops ein Datenpaket passieren darf. Der Maximalwert beträgt 255 Hops. Mit jedem Hop wird die TTL um 1 reduziert. Falls ein Datenpaket nach Ablauf seiner TTL noch nicht sein Ziel erreicht hat, wird es verworfen.
Twofish	Twofish ist ein Verschlüsselungsverfahren (siehe Cipher). Twofish verwendet eine fixe Blocklänge von 128 Bit. Die Schlüssellänge beträgt 128, 192 oder 256 Bit.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) ist eine DSL-Variante. Sie wurde als ANSI T1.413 entwickelt und als G.992.2 standardisiert. U-ADSL erlaubt die parallele Nutzung verschiedener Kommunikationstechniken, z. B. ISDN und POTS, und benötigt keinen Splitter.
Überprüfung der Rückroute	Falls bei einer Schnittstelle "Überprüfung der Rückroute" (Back Route Verify) aktiviert ist, werden über diese eingehende Datenpakete nur akzeptiert, wenn ausgehende Antwortpakete über die gleiche Schnittstelle geroutet würden.

UDP	Beim User Datagram Protocol (UDP) handelt es sich um ein verbindungsloses Protokoll. Es operiert auf der Transportschicht des OSI-Modells. Bei einem verbindungslosen Protokoll ist keine Kontrolle für die Auslieferung des Pakets integriert. Die Kontrolle muss in der Anwendungsschicht erfolgen. Im Gegenzug ist UDP schneller als verbindungsorientierte Protokolle.
ULA	Unique Local Addresses (ULA) sind IPv6-Adressen, die nicht geroutet werden. Sie können in privaten Netzen (z. B. einem LAN) verwendet werden. ULAs beginnen mit dem Präfix fd.
UMTS	Das Universal Mobile Telecommunications System (UMTS), auch als 3G bezeichnet, ist ein Mobilfunkstandard mit einer spezifizierten max. Datenübertragungsrate von 384 kbit/s bzw. 21 Mbit/s in Verbindung mit HSPA+.
Unicast	Bei Unicast werden Datenpakete von einem Sender zu einem einzigen Empfänger übertragen.
UPnP	Universal Plug and Play (UPnP) dient zur herstellerübergreifenden Ansteuerung von Geräten (Audio-Geräte, Router, Drucker, usw.) über ein IP-basiertes Netzwerk.
Upstream	Das Gateway leitet die Daten des eigenen Netzwerks weiter.
URL	Ein Uniform Resource Locator (URL) identifiziert den Speicherort einer Datei. Beispiel: http://www.example.org/index.htm (Web-Seite im Internet)
V.110	V.110 beschreibt ein Verfahren zur Anpassung von Bitströmen mit 0,6, 1,2, 2,4, 2,8, 7,2, 9,6, 12, 14,4, 19,2 und 38,4 kbit/s in den ISDN-Bitstrom von 64 kbit/s.
VDSL	Very High Speed Digital Subscriber Line. Siehe DSL.
VID	Siehe VLAN.
VLAN	Ein Netzwerk kann in eines oder mehrere logische Teilnetze – sogenannte Virtual-Local-Area-Networks (VLAN) – aufgespalten werden, indem die Netzwerkkomponenten das Datenpaket eines definieren Teilnetzes nicht mehr in andere Teilnetze weiterleiten. Jedem VLAN wird eine eindeutige Nummer zugeordnet. Diese Nummer wird VLAN ID (VID) genannt und den Datenpaketen im VLAN-Tag zugeordnet.
VoIP	Voice over IP (VoIP), auch IP-Telefonie genannt, bezeichnet die Übertragung von Sprache über ein IP-Netzwerk. Der Auf- und Ab-

	<p>bau der Telefonverbindung erfolgt dabei über Signalisierungsprotokolle, wie z. B. SIP.</p>
VPN	<p>Mithilfe eines virtuellen privaten Netzwerks (VPN) werden private Datenpakete durch ein öffentliches Netzwerk transportiert. Die Informationen werden dabei durch Einkapselung in neue Protokolle von den öffentlich zugänglichen Daten getrennt, um sie an den vorgesehenen Empfänger zu leiten. Man spricht in diesem Zusammenhang auch von einem Tunnel, der zwischen den privaten Netzen der beiden Verbindungsteilnehmer aufgebaut wird. VPN-Protokolle sind IP-Sec, PPTP, L2TP und GRE.</p>
VSS	<p>Das Virtual Service Set (VSS) bezeichnet ein Präfix von Wireless-LAN-Schnittstellen.</p>
Wählverbindung	<p>Eine Wählverbindung wird bei Bedarf durch die Wahl einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung (siehe Standleitung), die permanent aktiv ist.</p>
Walled Garden	<p>Bei Hotspots bezeichnet Walled Garden den Bereich des Internetangebots, der für die Benutzer unentgeltlich und ohne Anmeldung zur Verfügung steht.</p>
WAN	<p>Ein Wide Area Network (WAN) bezeichnet ein räumlich weit ausge dehntes Netzwerk. Die globalen WAN-Netze gewähren Zugriff auf das Internet.</p>
WDS	<p>Mithilfe des Wireless Distribution System (WDS) wird eine drahtlose Verbindung zwischen mehreren Access Points aufgebaut.</p>
Web-Server	<p>Ein Web-Server bietet HTML-Dokumente (Web-Seiten) an.</p>
WEP	<p>Wired Equivalent Privacy (WEP) ist ein Verschlüsselungsprotokoll für WLANs. Die Schlüssellänge beträgt 40 oder 104 Bit.</p>
WINS	<p>Der Windows Internet Name Service (WINS) ist eine Umsetzung des Netzwerkprotokolls NetBIOS over TCP/IP durch Microsoft. Wie DNS dient WINS der zentralen Namensauflösung. Siehe auch DNS.</p>
WLAN	<p>Wireless Local Area Network (Wireless LAN, WLAN) bezeichnet ein lokales Funknetz, das auf dem Standard 802.11 basiert.</p>
WMM	<p>Wi-Fi Multimedia (WMM) priorisiert die Datenpakete unterschiedlicher Anwendungen und verbessert damit die Übertragung von Sprach-, Musik- und Videodaten in WLAN-Netzwerken. Dazu stellt WMM Quality-of-Service-Merkmale (QoS) für IEEE 802.11-basierte Netzwerke bereit.</p>

WPA	Wi-Fi-Protected Access (WPA) ist ein Verschlüsselungsprotokoll für WLANs. WPA verwendet dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren.
WPA - Enterprise	WPA - Enterprise bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmer durch das Extensible Authentication Protocol (EAP). Nach erfolgreicher Authentisierung übermittelt der Server dem Client und dem Access Point einen gemeinsamen Schlüssel für die Datenübertragung im WLAN.
WPA - PSK	WPA - PSK bietet bei WPA 1 / 2 eine Authentifizierung der Teilnehmern über Preshared Keys. Dabei nutzen Access Point und Client die gleiche Zeichenfolge für die Schlüsselberechnung im WLAN. Diese Zeichenfolge muss von den Anwendern konfiguriert werden.
WPA 2	Wi-Fi Protected Access 2 (WPA 2) ist ein Verschlüsselungsprotokoll für WLANs. WPA 2 verwendet AES.
X.25	X.25 ist eine standardisierte Protokollfamilie für großräumige Netzwerke (WANs) über das Telefonnetz.
X.31	Der X.31-Standard beschreibt die Verbindung von ISDN- und X.25-Systemen. Es ist ein Standard zum Anbinden von Kartenterminals.
X.500	Der X.500-Standard beschreibt den Aufbau eines Verzeichnisdienstes. Siehe auch LDAP.
X.509	Der X.509-Standard beschreibt die Erstellung der Zertifikate für eine Public-Key-Infrastruktur (PKI).
X.75	X.75 ist eine standardisierte Protokollfamilie für ISDN-Netzwerke mit einer Übertragungsrate von 64 kbit/s.
XAuth	Mithilfe von XAUTH (Extended Authentication) wird IKE um weitere Authentifizierungsmechanismen ergänzt. Nach einer erfolgreichen IKE-Phase-1-Authentifizierung kann der Benutzer noch einmal separat identifiziert werden. Die Identifizierung erfolgt über Benutzername und Passwort, PAP, CHAP oder Hardware-basierte Systeme.
Zeitschlitz	Ein Zeitschlitz ist ein fest zugeordneter Zeitabschnitt innerhalb eines Übertragungsrahmens und entspricht meist einem Übertragungskanal.
Zertifikat	Ein Zertifikat identifiziert eine Person, eine Institution, ein Gerät oder eine Anwendung. Ein Public-Key-Zertifikat ist ein digitales Zertifikat und stellt eine Verbindung zwischen der Identität und einem öffentli-

chen Schlüssel her. Zertifikate mit öffentlichem Schlüssel werden von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt. Nicht mehr vertrauenswürdige Zertifikate können über Zertifikatsperrlisten (Certificate Revocation List, CRL) deaktiviert werden.

Index

- 230
- ISDN-Zeitserver 93
- Systemadministrator-Passwort 90
- #
- #1 #2, #3 130
- 2
- 2,4/5-GHz-Übergang 505
- A**
- Abfrage Intervall 298
- Abgewiesene Clients soft/hard 505
- ACCESS_ACCEPT 111
- ACCESS_REJECT 111
- ACCESS_REQUEST 111
- ACCOUNTING_START 111
- ACCOUNTING_STOP 111
- Activity Monitor 481
- Admin-Status 256
- Administrativer Status 331 , 404
- Administrativer Zugriff 103
- Adressbereich 393
- Adresse/Subnetz 393
- Adressen 392
- Adressliste 393
- Adressmodus 144
- Adresstyp 393
- ADSL-Logik 464
- Ähnliches Zertifikat überschreiben 430
- Airtime Fairness 160 , 213
- Aktion 184 , 184 , 193 , 193 , 231 , 280 , 386 , 430 , 447 , 464 , 486 , 490
- Aktionen 429
- aktiv 311
- Aktive Clients 505
- Aktive Clients 225
- Aktive IPSec-Tunnel 84
- Aktive Sitzungen (SIF, RTP, etc...) 84
- Aktives Funkmodulprofil 208
- Aktiviert 380
- Aktualisierung aktivieren 413
- Aktualisierungsintervall 415 , 482
- Aktualisierungspfad 415
- Aktualisierungstimer 292
- Aktuelle Ortszeit 92
- Aktuelle Geschwindigkeit / Aktueller Modus 136
- Aktueller Dateiname im Flash 464
- Alle Multicast-Gruppen 303
- Allgemein 297
- Allgemeine Statusangaben 508
- Allgemeiner Name 128
- Als DHCP-Server 403
- Als IPCP-Server 403
- Alternative Schnittstelle, um DNS-Server zu erhalten 401
- Andere Inaktivität 391
- Angegriffener Access Point 228
- Ankommende Rufnummer 344
- Anmeldefenster 458
- Anmeldung 507
- Ansicht 508 , 510 , 513
- Antwort 406
- Antwortintervall (Letztes Mitglied) 298
- Anzahl Nachrichten 475
- Anzahl der Spatial Streams 155 , 211
- Anzahl erlaubter Verbindungen 338
- AP-MAC-Adresse 184 , 503 , 504
- Arbeitsspeichernutzung 84
- ARP Lifetime 284
- ARP Processing 172 , 218
- Art des Datenverkehrs 244
- Art des Angriffs 228
- Assert-Status 513 , 514
- Assistenten 82
- Ausgehende Rufnummer 344
- Ausgehende Schnittstelle 270
- Ausgewählte Kanäle 162

- Ausgewählter Kanal 155
 - Aushandlungsmodus 487
 - Auslöser 424
 - Auswahl 394
 - Auswahl des Client-Bands 176 , 222
 - Auszuführende Aktion 443
 - Authentifizierung 317 , 322 , 376
 - Authentifizierung für PPP-Einwahl 121
 - Authentifizierungsmethode 331 , 347 , 487
 - Authentifizierungspasswort 451
 - Authentifizierungstyp 113 , 118
 - Autospeichermodus 130 , 430
- B**
- Bandbreite 155 , 211
 - Bandbreite angeben 389
 - Basierend auf Ethernet-Schnittstelle 144
 - Baudrate 138
 - Beacon Period 162 , 177 , 215
 - Bedingung des Schnittstellenverkehrs 425
 - Bedingung für Ereignisliste 430
 - Befehlsmodus 430
 - Befehlstyp 430
 - Benachbarte APs 226
 - Benachrichtigungsdienst 474 , 475 , 477
 - Benachrichtigungseinstellungen 477
 - Benachrichtigungsempfänger 474
 - Benutzer 361 , 372
 - Benutzerdefiniert 128
 - Benutzerdefinierter Kanalplan 165 , 215
 - Benutzername 314 , 320 , 373 , 413 , 477 , 507
 - Berichtsmethode 282
 - Berücksichtigen 251
 - Beschreibung 123 , 134 , 207 , 211 , 236 , 244 , 256 , 260 , 263 , 270 , 276 , 280 , 314 , 320 , 331 , 337 , 347 , 356 , 361 , 369 , 373 , 380 , 392 , 393 , 394 , 395 , 398 , 404 , 422 , 425 , 430 , 486 , 487 , 490 , 491 , 494
 - Beschreibung - Verbindungsinformation - Link 86
 - Beschreibung des Client Links 184
 - Beschreibung des Client Links 503
 - Beschreibung Entfernter Link 193
 - Betreff 475
 - Betreibermodus 113
 - Betriebsmodus 155 , 208 , 211
 - Blockieren nach Verbindungsfehler für 317 , 322 , 376
 - blockiert 311
 - Blockzeit 119 , 352
 - BOSS 464
 - BOSS-Version 84
 - Bridge-Link-Beschreibung 191 , 193 , 501 , 502
 - Bridge-Links 185 , 501
 - Bridges 506
 - Burst-Größe 270
 - Burst-Mode 160 , 213
 - Bytes 487
 - Bytezahl 140
- C**
- CA-Name 430
 - CA-Zertifikat 126
 - CA-Zertifikate 352
 - Cache 409
 - Cache-Größe 401
 - Cache-Treffer 410
 - Cache-Trefferrate (%) 410
 - CAPWAP-Verschlüsselung 207
 - Channel Sweep 165
 - Client Link 181
 - Client Links 503
 - Client-MAC-Adresse 497
 - Client-Modus 155
 - Code 395
 - Controller-Konfiguration 202
 - COS-Filter (802.1p/Layer 2) 260 , 276
 - CPU-Nutzung 84

- CRL verwenden 430
- CRLs 132
- CRLs senden 367
- CSV-Dateiformat 430
- CTS Frames als Antwort auf RTS empfangen 494
- D**
- Datei auswählen 464
- Dateikodierung 131 , 132
- Dateiname 430 , 464
- Dateiname auf Server 430
- Dateiname in Flash 430
- Datenbits 138
- Datenrate Mbit/s 495 , 497 , 498 , 500 , 501 , 502 , 503 , 504
- Datum 485
- Datum einstellen 92
- Datum und Uhrzeit 91
- Designated Router (DR) 508
- Designated-Router-Priorität 305
- Details 486
- DH-Gruppe 347
- DHCP Broadcast Flag 146
- DHCP Client an Schnittstelle 284
- DHCP-Hostname 146
- DHCP-Konfiguration 417
- DHCP-MAC-Adresse 146
- DHCP-Optionen 419
- DHCP-Relay-Einstellungen 422
- DHCP-Server 203 , 416
- Diagnose 460
- Dienst 245 , 256 , 260 , 276 , 386
- Dienste 394
- Dienstliste 395
- Discovery Server freigeben 453
- DNS 399
- DNS-Anfragen 410
- DNS-Aushandlung 317 , 322 , 377
- DNS-Hostname 406
- DNS-Server 325 , 363 , 403 , 407 , 417
- DNS-Test 461
- Domäne 407
- Domäne am Hotspot-Server 456
- Domänenname 401
- Domänenweiterleitung 407
- Doppelte empfangene MSDUs 494
- Drahtloser Modus 160 , 213
- Drahtlosnetzwerke (VSS) 169 , 217 , 225
- Dritter Zeitserver 93
- Drop-In 283
- Drop-In-Gruppen 283
- Dropping-Algorithmus 273
- DSA-Schlüsselstatus 107
- DSCP-/TOS-Wert 236
- DSCP/TOS-Filter (Layer 3) 260 , 276
- DTIM Period 162 , 177 , 215
- Dynamische
 - RADIUS-Authentifizierung 365
- Dynamische Black List 223
- DynDNS-Aktualisierung 412
- DynDNS-Client 412
- DynDNS-Provider 414
- E**
- E-Mail 128
- E-Mail-Adresse 477
- EAP-Vorabauthentifizierung 173 , 219
- Eigene IP-Adresse per ISDN/GSM übertragen 344
- Einstellungen Funkmodul 153
- Eintrag aktiv 113 , 118
- Empfangene DNS-Pakete 410
- Empfänger 475
- Entfernte GRE-IP-Adresse 380
- Entfernte IP-Adresse 370
- Entfernte MAC-Adresse 181 , 192 , 193
- Entfernte PPTP-IP-Adresse 322
- Entfernte IP-Adresse 486 , 487
- Entfernte MAC 498 , 500 , 501 , 502
- Entfernte Netzwerke 486
- Entfernte ID 487
- Entfernte IP 140
- Entfernter Hostname 369
- Entfernter Port 487 , 491

Entfernter Link aktiviert 193
 Enthaltene Zeichenfolge 475
 Ereignis 475
 Ereignisliste 425 , 430
 Ereignistyp 425
 Erfolgreich empfangene Multicast-MS-DUs 494
 Erfolgreich übertragene Multicast-MS-DUs 494
 Erfolgreich beantwortete Anfragen 410
 Erfolgreiche Versuche 443
 Erlaubte Adressen 177 , 223
 Erreichbarkeitsprüfung 115 , 352 , 358 , 487
 Erster Zeitserver 93
 Erweiterte Route 239
 Ethernet-Ports 135
 Expiry Timer 509 , 513 , 514 , 515
 Externe Berichterstellung 469
 Externer Dateiname 131 , 132

F

Facility 470
 Fehler 230 , 487 , 489
 Fehlerhafte Erhaltene Pakete 494
 Fehlgeschlagene Versuche 443
 Fehlversuche per Zeitraum 223
 Fernkonfiguration 191
 Fertig 230
 Filter 263
 Filterregeln 385 , 389
 Firewall 383
 Firewall Status 390
 Firmware-Wartung 230
 Fragmentation Threshold 162 , 165 , 215
 Frame-Übertragungen ohne ACK 494
 Frames ohne Tag verwerfen 150
 Frequenzband 155 , 211
 Funkmodulprofile 210

G

Garbage Collection Timer 292
 Gateway 239 , 419 , 451
 Gateway-IP-Adresse 235
 Generation ID 509
 Gerät 207
 Gerätesuche 449
 Gesamt 489
 Geschäftsbedingungen 456
 Gewichtung 270
 Globale Einstellungen 401
 Globale Einstellungen 86
 GRE 379
 GRE-Tunnel 380
 Größe der Zero Cookies 365
 Größe des Protokoll-Headers unterhalb Layer 3 267
 Gruppen 392 , 394 , 397
 Gruppen-ID 443
 Gruppenbeschreibung 113 , 251 , 253 , 284

H

Handshake 138
 Hashing-Algorithmen 107
 Hello Hold Time 305
 Hello-Intervall 305 , 371
 Hersteller auswählen 421
 High-Priority-Klasse 263
 Hinzuzufügende/zu bearbeitende MIB/SNMP-Variable 430
 Hold Down Timer 293
 Host 407
 Host für mehrere Standorte 459
 Hostname 413
 Hosts 442
 Hotspot-Gateway 453 , 455 , 506
 HTTP 104
 HTTPS 104 , 411
 HTTPS-Server 411
 HTTPS-TCP-Port 411

I

IEEE 802.11d-Konformität 155

- IGMP 297
 - IGMP Proxy 300
 - IGMP-Status 301
 - IKE (Phase-1) 489
 - IKE (Internet Key Exchange) 331
 - IKE (Phase-1) SAs 487
 - Image bereits vorhanden. 230
 - Immer aktiv 314 , 320 , 373
 - inaktiv 311
 - Indexvariablen 425 , 430
 - Informationen senden an 482
 - Initial Contact Message senden 365
 - Inter-Byte Gap 140
 - Internes Protokoll 484
 - Internet + Einwählen 311
 - Intervall 425 , 430 , 443 , 448
 - Intra-cell Repeating 172 , 218
 - IP Pools 324 , 362
 - IP-Accounting 472
 - IP-Adressbereich 203 , 325 , 363 , 417
 - IP-Adresse 406 , 422 , 451 , 470 , 481 , 495 , 497 , 507 , 508 , 509
 - IP-Adresse / Netzmaske 144
 - IP-Adresse des Rendezvous Point 510
 - IP-Adresse des Rendezvous Points 509
 - IP-Adresse des Assert Winner 513 , 514
 - IP-Adresse zur Nachverfolgung 254
 - IP-Adresse/Netzmaske 290 , 491
 - IP-Adressenvergabe 334
 - IP-Adressmodus 316 , 321 , 374
 - IP-Komprimierung 358
 - IP-Konfiguration 143
 - IP-Pool-Konfiguration 416
 - IP-Poolname 325 , 363 , 417 , 418
 - IP-Zuordnungspool 334
 - IP-Zuordnungspool (IPCP) 374
 - IP/MAC-Bindung 421
 - IPSec 328 , 485
 - IPSec (Phase-2) 489
 - IPSec aktivieren 364
 - IPSec (Phase-2) SAs 487
 - IPSec über TCP 365
 - IPSec-Debug-Level 364
 - IPSec-Peers 330
 - IPSec-Statistiken 488
 - IPSec-Tunnel 486 , 488
 - IPv4-Routing-Tabelle 239
 - ISDN-Login 104
- J**
- Join/Prune Hold Time 305
 - Join/Prune-Intervall 305
 - Join/Prune-Status 513 , 514 , 515
- K**
- Kanal 155 , 184 , 208
 - Kanäle scannen 165
 - Kanalplan 162 , 215
 - Keepalive-Periode 309
 - Kennwort für geschütztes Zertifikat 430
 - Key Hash Payloads senden 367
 - Klassen-ID 263 , 270
 - Klassenplan 263
 - Knotenname 451
 - Komprimierung 108 , 376
 - Konfiguration verschlüsseln 430
 - Konfiguration enthält Zertifikate/Schlüssel 430
 - Konfiguration von IPv4-Routen 232
 - Konfigurationsmodus 334
 - Konfigurationsschnittstelle 100
 - Konfigurierte Geschwindigkeit/konfigurierter Modus 136
 - Kontakt 87
 - Kontrollmodus 267 , 326
- L**
- L2TP 368
 - LAN 143
 - Land 128
 - Lastverteilung 226 , 250 , 505
 - Lastverteilungsgruppen 250

- Layer 4-Protokoll 236
 - LCP-Erreichbarkeitsprüfung 317 , 322 , 376
 - LDAP-URL-Pfad 134
 - Lease Time 419
 - Lebensdauer 347 , 356
 - LED-Modus 87
 - Letzte gespeicherte Konfiguration 84
 - Letztes Schreibergebnis 451
 - Level 470 , 485
 - Lizenzschlüssel 97
 - Lizenzseriennummer 97
 - Lokale GRE-IP-Adresse 380
 - Lokale IP-Adresse 235 , 284 , 316 , 321 , 334 , 371 , 374 , 380
 - Lokale PPTP-IP-Adresse 322
 - Lokale Zertifikatsbeschreibung 131 , 132 , 430
 - Lokale Adresse 491
 - Lokale IP-Adresse 487
 - Lokale Dienste 399
 - Lokale ID 331 , 487
 - Lokale IP-Adresse 140
 - Lokaler Dateiname 430
 - Lokaler Hostname 369
 - Lokaler ID-Typ 331 , 347
 - Lokaler ID-Wert 347
 - Lokaler Port 487 , 491
 - Lokaler Port 140
 - Lokales Zertifikat 347
 - Lokales Zertifikat 411
 - Long Retry Limit 162 , 165 , 215
 - Loopback aktiv 242
 - Löschen 228 , 239
- M**
- MAC-Adresse 144 , 422 , 451 , 491 , 495 , 505 , 506
 - MAC-Adresse des Rogue Clients 228
 - Mail-Exchanger (MX) 414
 - Manuelle IP-Adresse des WLAN-Controller 87
 - Max. Link-Entfernung 155
 - Max. Queue-Größe 273
 - Max. Scan-Dauer 193
 - Max. Übertragungsrate 160 , 213
 - Max. Anzahl Clients - Hard Limit 176 , 222
 - Max. Anzahl Clients - Soft Limit 176 , 222
 - Max. Zeitraum aktiver Scan 165
 - Max. Zeitraum passiver Scan 165
 - Maximale Antwortzeit 298
 - Maximale Anzahl der erneuten Einwählversuche 317 , 322
 - Maximale Upload-Geschwindigkeit 267 , 270 , 326
 - Maximale Anzahl der Accounting-Protokolleinträge 87
 - Maximale Anzahl der Syslog-Protokolleinträge 87
 - Maximale Gruppen 301
 - Maximale Quellen 301
 - Maximale Anzahl Wiederholungen 371
 - Maximale Anzahl gleichzeitiger Verbindungen 106
 - Maximale Anzahl der IGMP-Statusmeldungen 298
 - Maximale Anzahl der IGMP-Statusmeldungen 301
 - Maximale E-Mails pro Minute 477
 - Maximale TTL für negative Cacheeinträge 401
 - Maximale TTL für positive Cacheeinträge 401
 - Maximale Zeit zwischen Versuchen 371
 - Maximales Nachrichtenlevel von Systemprotokolleinträgen 87
 - Mbit/s 493
 - Metrik 235 , 239 , 334
 - Metrik-Offset für Inaktive Schnittstellen 290
 - Metrik-Offset für Aktive Schnittstellen 290
 - MIB-Variablen 430
 - Min. Queue-Größe 273

- Min. Zeitraum aktiver Scan 165
 - Min. Zeitraum passiver Scan 165
 - Minimale Zeit zwischen Versuchen 371
 - Mitglieder 392 , 398
 - MobiKE 340
 - Modus 126 , 140 , 184 , 236 , 241 , 284 , 298 , 301 , 344 , 347 , 361
 - Modus / Bridge-Gruppe 100
 - Modus des D-Kanals 344
 - Monitoring 224 , 484
 - MSDUs, die nicht übertragen werden konnten 494
 - MTU 380 , 487
 - Multicast 295
 - Multicast-Gruppen-Adresse 303 , 308 , 509 , 511 , 511 , 512 , 513 , 514 , 515
 - Multicast-Gruppenbereich 308
 - Multicast-Routing 297
- N**
- Nach Ausführung neu starten 430
 - Nachricht 485
 - Nachrichten 487
 - Nachrichtenkomprimierung 475
 - Nachrichtentyp 470
 - Name 207 , 361
 - Name der Quelldatei 464
 - Name der Zieldatei 464
 - Name Entferntes Gerät 193
 - NAT 242 , 491
 - NAT aktiv 242
 - NAT-Eintrag erstellen 316 , 321 , 374
 - NAT-Erkennung 487
 - NAT-Konfiguration 243
 - NAT-Methode 244
 - NAT-Schnittstellen 242
 - NAT-Traversal 352
 - Negativer Cache 401
 - Netzmaske 239 , 284 , 374 , 451
 - Netzwerk 232
 - Netzwerkadresse 284
 - Netzwerkkonfiguration 284
 - Netzwerkname (SSID) 172 , 182 , 184 , 218
 - Netzwerkname (SSID) 505
 - Neue Quell-IP-Adresse/Netzmaske 236 , 248
 - Neue Ziel-IP-Adresse/Netzmaske 248
 - Neuer Quell-Port 248
 - Neuer Ziel-Port 248
 - Neuer Dateiname 464
 - Neustart 467
 - Neustart des Geräts nach 430
 - Nicht entschlüsselbare MPDUs erhalten 494
 - Nicht geändert seit 490
 - Nicht-Mitglieder verwerfen 150
 - Nicht-schnittstellen-spezifischer Status 509
 - Nr. 241 , 485 , 490
 - Nutzungsbereich 155
- O**
- Öffentliche Quell-IP-Adresse 340
 - Optionen 121 , 240 , 301 , 364 , 379 , 390 , 441 , 452 , 459 , 462 , 473 , 482
 - Organisation 128
 - Organisationseinheit 128
 - Ort 128
 - OSPF-Modus 377
 - Override Interval 305
- P**
- Pakete 487
 - Parität 138
 - Passwort 126 , 131 , 132 , 314 , 320 , 361 , 369 , 373 , 413 , 430 , 464 , 477 , 482
 - Passwörter 89
 - Passwörter und Schlüssel als Klartext anzeigen 90
 - Peer-Adresse 331
 - Peer-ID 331
 - PFS-Gruppe verwenden 356

- Phase-1-Profil 338
 - Phase-1-Profile 346
 - Phase-2-Profil 338
 - Phase-2-Profile 355
 - Physikalische Schnittstellen 135
 - Physische Adresse 507
 - PIM 303 , 508
 - PIM-Modus 305
 - PIM-Optionen 309
 - PIM-Rendezvous-Punkte 307
 - PIM-Schnittstellen 304
 - PIM-Status 309
 - Ping 104
 - Ping-Generator 448
 - Ping-Test 460
 - PMTU propagieren 358
 - Poisoned Reverse 291
 - Pool-Verwendung 418
 - Pop-Up-Fenster für Statusanzeige 458
 - POP3-Server 477
 - POP3-Timeout 477
 - Port 415 , 506
 - Port-Modus 137 , 142
 - Portkonfiguration 135 , 150
 - Portnummer 140
 - Portweiterleitungen 242
 - Positiver Cache 401
 - PPPoE 313
 - PPPoE-Ethernet-Schnittstelle 314
 - PPPoE-Modus 314
 - PPPoE-Schnittstelle für Mehrfachlink 314
 - PPTP 319
 - PPTP-Adressmodus 322
 - PPTP-Ethernet-Schnittstelle 320
 - PPTP-Inaktivität 391
 - PPTP-Passthrough 242
 - Präfixlänge der Multicast-Gruppe 308
 - Präfixlänge der Multicast-Gruppe 509
 - Preshared Key 173 , 180 , 182 , 192 , 219 , 331
 - Primärer DNS-Server 404
 - Primärer DHCP-Server 423
 - Priorisierungsalgorithmus 267
 - Priorität 113 , 118 , 270 , 386 , 404
 - Priority Queueing 270
 - Privaten Schlüssel generieren 126
 - Propagation Delay 305
 - Proposals 347 , 356
 - Protokoll 245 , 256 , 260 , 276 , 337 , 395 , 415 , 430 , 470
 - Protokollformat 473
 - Protokollierte Aktionen 390
 - Protokollierungslevel 108
 - Provider 413
 - Providername 415
 - Provisioning-Server (code 3) 421
 - Proxy ARP 146 , 340
 - Proxy-ARP-Modus 377
 - Proxy-Schnittstelle 300
 - PVID 150
- Q**
- QoS 259 , 388 , 507
 - QoS anwenden 386
 - QoS-Filter 259
 - QoS-Klassifizierung 263
 - QoS-Queue 507
 - QoS-Schnittstellen/Richtlinien 266
 - Quell-IP-Adresse 425 , 430 , 443 , 448 , 511 , 512 , 514 , 515
 - Quell-IP-Adresse/Netzmaske 245 , 256 , 260 , 276 , 337
 - Quell-Port 236 , 245 , 337
 - Quell-Port/Bereich 245 , 256 , 260 , 276
 - Quelle 231 , 386 , 430 , 464
 - Quellportbereich 395
 - Quellschnittstelle 236 , 256 , 303
 - Queued 507
 - Queues/Richtlinien 267
- R**
- RA-Signierungszertifikat 126
 - RA-Verschlüsselungszertifikat 126
 - RADIUS 111

- RADIUS-Dialout 115
 - RADIUS-Passwort 113
 - RADIUS-Server 219
 - RADIUS-Server Gruppen-ID 361
 - Rate 500, 502, 504
 - Rauschen dBm 495, 497, 498, 500, 501, 502, 503, 504
 - Real Time Jitter Control 267
 - Real Time Jitter Control 326
 - Regelkette 280, 282
 - Regelketten 279
 - Region 194, 203
 - Register Suppression Timer 309
 - Regulierte Schnittstellen 326
 - Relais 141
 - Relaiskonfiguration 142
 - Remote Authentifizierung 111
 - Remote-Adresse 491
 - Rendezvous Point IP-Adresse 308
 - Retransmission Timer 293
 - Reverse-Path-Forwarding (RPF) 511, 512
 - RFC 2091-Variabler Timer 291
 - RFC 2453-Variabler Timer 291
 - Richtlinie 115, 119
 - Richtlinien 385
 - Richtung 263, 290
 - Richtung des Datenverkehrs 425
 - RIP 286
 - RIP-Filter 289
 - RIP-Optionen 291
 - RIP-Schnittstellen 286
 - RIP-UDP-Port 291
 - Roaming-Profil 165
 - Robustheit 298
 - Rogue Clients 228
 - Rogue APs 227
 - Rolle 361
 - Routen 232
 - Routenankündigung 287
 - Routeneinträge 316, 321, 334, 374, 380
 - Routenklasse 234
 - Routenselektor 254
 - Routentimeout 292
 - Routentyp 234, 239
 - Routing-Protokolle 286
 - RSA-Schlüsselstatus 107
 - RTS Threshold 162, 165, 215
 - RTS Frames ohne CTS 494
 - RTT-Modus (Realtime-Traffic-Modus) 270
 - ruhend 311
 - Rx-Bytes 490, 491
 - Rx-Fehler 490
 - Rx-Pakete 490, 491, 493, 495, 497, 498, 500, 501, 502, 503
- S**
- SAs mit dem Status der ISP-Schnittstelle synchronisieren 365
 - Scan-Intervall 165
 - Scan-Schwelle 165
 - SCEP-Server-URL 430
 - SCEP-URL 126
 - Schedule-Intervall 441
 - Scheduling 423
 - Schlüsselgröße 430
 - Schlüsselwert 380
 - Schnittstelle 101, 102, 105, 136, 150, 203, 234, 239, 241, 244, 253, 267, 282, 290, 298, 305, 326, 389, 404, 407, 413, 418, 430, 446, 447, 451, 456, 507, 507, 508, 509, 513, 514, 515
 - Schnittstelle - Verbindungsinformation - Link 85
 - Schnittstellen 100, 143, 263, 391, 445, 472, 489
 - Schnittstellenaktion 446
 - Schnittstellenauswahl 284
 - Schnittstellenbeschreibung 100
 - Schnittstellenmodus 144, 404
 - Schnittstellenmodus / Bridge-Gruppen 98
 - Schnittstellenspezifische Zustände 512
 - Schnittstellenstatus 425

- Schnittstellenstatus festlegen 430
- Schnittstellenzuweisung 281
- Schutz 180 , 192
- Schweregrad 475
- Sekundärer DNS-Server 404
- Sekundärer DHCP-Server 423
- Sendeleistung 155 , 208
- Senden 507
- Sequenznummern der Datenpakete 371
- Seriellen RX-Zwischenspeicher löschen 141
- Seriellen TX-Zwischenspeicher löschen 141
- Serieller Port 137 , 137
- Seriennummer 84
- Server 415
- Server Timeout 115
- Server-IP-Adresse 113 , 118
- Server-URL 430
- Serveradresse 430
- Serverfehler 410
- Setze COS Wert (802.1p/Layer 2) 263
- Setze DSCP/TOS Wert (Layer 3) 263
- Short Guard Interval 162 , 165 , 215
- Short Retry Limit 162 , 165 , 215
- Shortest Path Tree 511
- Sicherheitsalgorithmus 486
- Sicherheitsmodus 173 , 182 , 219
- Signal 184
- Signal dBm 193
- Signal dBm 228 , 495 , 497 , 498 , 500 , 501 , 502 , 503 , 504
- Slave Access Points 205
- Slave-AP-Konfiguration 205
- Slave-AP-Standort 203
- SMS-Gerät 478
- SMTP-Authentifizierung 477
- SMTP-Server 477
- SNMP 104 , 109 , 479
- SNMP Read Community 90
- SNMP Trap Broadcasting 480
- SNMP Write Community 90
- SNMP-Listen-UDP-Port 110
- SNMP-Trap-Community 480
- SNMP-Trap-Hosts 481
- SNMP-Trap-Optionen 479
- SNMP-Trap-UDP-Port 480
- SNMP-Version 110
- SNR dB 497 , 504
- Software & Konfiguration 462
- Special Handling Timer 256
- Special Session Handling 255
- Sperrzeit für Black List 223
- Sprache für Anmeldefenster 456
- SSH 104 , 105
- SSH-Dienst aktiv 106
- SSH-Port 106
- SSID 228
- Staat/Provinz 128
- Standard-Benutzerpasswort 113
- Standard-Timeout bei Inaktivität 458
- Standardeinstellungen wiederherstellen 104
- Standardmäßige Routenverteilung 291
- Standardroute 316 , 321 , 334 , 374 , 380
- Standort 87 , 207
- Startmodus 338
- Startzeit 428
- Statische Hosts 405
- Statische Black List 228
- Statistik 410 , 490
- Status 83 , 425 , 486 , 489 , 490 , 491
- Status festlegen 430
- Status des Auslösers 430
- Stoppbits 138
- Stoppzeit 428
- Stub Interface Mode 305
- Subjektnamen 430
- Subsystem 485
- Switch-Port 136
- Syslog-Server 470
- System 86
- System als Zeitserver 93
- Systemadministrator-Passwort bestäti-

- gen 90
- Systemdatum 84
- Systemlizenzen 95
- Systemlogik 464
- Systemmeldungen 484
- Systemname 87
- Systemneustart 467
- Systemprotokoll 469
- Systemverwaltung 83
- T**
- TACACS+ 117
- TACACS+-Passwort 118
- TCP-ACK-Pakete priorisieren 317 ,
322 , 376
- TCP-Inaktivität 391
- TCP-Keepalives 108
- TCP-MSS-Clamping 146
- TCP-Port 119
- Teldat Discovery 449
- Telnet 104
- Temperatur 84
- Tickettyp 458
- Timeout 119 , 140
- Timeout bei Inaktivität 314 , 320 , 373
- Timeout für Nachrichten 475
- Toleranzzeit beim Login 108
- Traceroute-Test 461
- Traffic Shaping 267 , 270 , 389
- Transparente MAC-Adresse 102
- Trigger 446 , 447
- Triggered-Hello-Intervall 305
- TTL 406
- Tunnelprofil 373
- Tunnelprofile 368
- Tx-Bytes 490 , 491
- Tx-Fehler 490
- Tx-Pakete 490 , 491 , 493 , 495 , 497
, 498 , 500 , 501 , 502 , 503
- Typ 260 , 276 , 395 , 490
- U**
- U-APSD 172
- Überbuchen zugelassen 270
- Überprüfung anhand einer Zertifika-
tatsperrliste (CRL) 123
- Überprüfung der Rückroute 340
- Überprüfung der Rückroute 241
- Übertragene MPDUs 494
- Übertragener Datenverkehr 425
- Übertragungsmodus 344
- Übertragungsschlüssel 173 , 180 ,
182 , 219
- Überwachte IP-Adresse 443
- Überwachte Schnittstelle 425 , 446
- Überwachte Subsysteme 475
- Überwachte Variable 425
- Überwachte Schnittstellen 482
- Überwachtes Zertifikat 425
- Überwachung 442
- UDP-Inaktivität 391
- UDP-Port 115
- UDP-Quellport 370
- UDP-Quellportauswahl 379
- UDP-Zielport 370 , 379 , 482
- Ungültige DNS-Pakete 410
- Unicast MPDUs erfolgreich erhalten
494
- Unicast MSDUs erfolgreich
übertragen 494
- Unveränderliche Parameter 258
- Upstream Nachbar-IP-Adresse 510 ,
511 , 511
- Upstream Join State 510 , 511 , 511
- Upstream Join Timer 510 , 511 , 511
- Upstream Override Timer 512
- Uptime 84 , 495 , 497 , 498 , 500 ,
501 , 502 , 503 , 504 , 509 , 510 ,
511 , 511 , 512 , 513 , 514 , 515
- URL 231 , 464
- V**
- Verbindungsstatus 260 , 276
- Verbindungstyp 373
- Verbleibende Gültigkeitsdauer 425
- Verbunden 184 , 193
- Vergleichsbedingung 425

- Vergleichswert 425
 - Vermeidung von Datenstau (RED) 273
 - Verschlüsselt 489
 - Verschlüsselung 119 , 376
 - Verschlüsselung der Konfiguration 464
 - Verschlüsselungsalgorithmen 107
 - Version in Empfangsrichtung 287
 - Version in Senderichtung 287
 - Versionsprüfung 430
 - Versuche 425 , 430 , 448
 - Verteilungsmodus 251
 - Verteilungsrichtlinie 251 , 253
 - Verteilungsverhältnis 253
 - Vertrauenswürdigkeit des Zertifikats erzwingen 123
 - Verwaltung 151 , 194
 - Verwaltungs-VID 151
 - Verwendeter Kanal 208
 - Verwerfen ohne Rückmeldung 282
 - Verwerfen ohne Rückmeldung 242
 - Verworfen 489 , 507
 - VLAN 147 , 224 , 314
 - VLAN Identifier 149
 - VLAN aktivieren 151
 - VLAN-ID 144 , 224 , 314
 - VLAN-Mitglieder 149
 - VLAN-Name 149
 - VLANs 149
 - Vollständige Filterung 390
 - Vollständige IPSec-Konfiguration löschen 364
 - Vom NAT ausnehmen (DMZ) 284
 - Vorrang 308
 - VPN 328
 - VSS 495
 - VSS-Beschreibung 505
- W**
- Walled Garden 456
 - Walled Garden URL 456
 - Walled Network / Netzmaske 456
 - WAN 311
- Wartung 230 , 460
 - WDS 498
 - WDS-Beschreibung 179 , 498 , 500
 - WDS-Links 178
 - Weitergeleitet 489
 - Weitergeleitete Anfragen 410
 - Weiterleiten 302 , 407
 - Weiterleiten an 407
 - WEP-Schlüssel 1 180
 - WEP-Schlüssel 2 180
 - WEP-Schlüssel 3 180
 - WEP-Schlüssel 4 180
 - WEP-Schlüssel 1-4 173 , 182 , 219
 - Wert 494
 - Wiederholungen 115
 - Wiederkehrender Hintergrund-Scan 215
 - Wildcard 414
 - Wildcard-MAC-Adresse 102
 - Wildcard-Modus 102
 - WINS-Server 401
 - Wird ausgeführt 230
 - Wireless LAN 152
 - Wireless LAN Controller 196
 - Wizard 196
 - WLAN 153 , 492
 - WLAN-Modul auswählen 430
 - WLANx 492
 - WLC-SSID 430
 - WMM 172 , 218
 - WPA Cipher 173 , 182 , 219
 - WPA-Modus 173 , 182 , 219
 - WPA2 Cipher 173 , 182 , 219
- X**
- XAUTH-Profil 338
 - XAUTH-Profile 360
- Z**
- Zeit 485
 - Zeit einstellen 92
 - Zeitaktualisierungsintervall 93
 - Zeitaktualisierungsrichtlinie 93

Zeitbedingung 428
Zeitstempel 470
Zeitzone 92
Zero Cookies verwenden 365
Zertifikat in Konfiguration schreiben
430
Zertifikat ist ein CA-Zertifikat 123
Zertifikate 122
Zertifikate und Schlüssel einschließen
464
Zertifikatsanforderung 125
Zertifikatsanforderungs-Payloads nicht
beachten 367
Zertifikatsanforderungs-Payloads sen-
den 367
Zertifikatsanforderungsbeschreibung
126 , 430
Zertifikatsketten senden 367
Zertifikatsliste 122
Zertifikatsserver 133
Ziel 386
Ziel-IP-Adresse 239 , 425 , 430 , 448
Ziel-IP-Adresse/Netzmaske 235 , 245
, 256 , 260 , 276 , 337
Ziel-Port/Bereich 245 , 256 , 260 ,
276
Zielport 236 , 337
Zielportbereich 395
Zielschnittstelle 303
Zuerst gesehen 228
Zugewiesene Drahtlosnetzwerke
(VSS) 208
Zugriffsfiler 275 , 280
Zugriffskontrolle 177 , 223
Zugriffsregeln 274
Zulässiger Hotspot-Client 458
Zuletzt gesehen 228
Zusammenfassend 128
Zusätzliche, frei zugängliche Domänen-
namen 456
Zusätzlicher Filter des Datenverkehrs
336 , 337
Zweiter Verwendeter Kanal 155
Zweiter Zeitserver 93