

Benutzerhandbuch bintec R1xxx/R3xxx/R4xxx

Referenz

Copyright© Version 5.0, 2009 Funkwerk Enterprise Communications GmbH

Rechtlicher Hinweis

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von funkwerk-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.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications 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 funkwerk-Gateways finden Sie unter www.funkwerk-ec.com.

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

Marken

funkwerk das funkwerk-Logo, bintec und das bintec-Logo, artem und das artem-Logo, elmeg und das elmeg-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications 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 Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH, Südwestpark 94, D-90449 Nürnberg, Deutschland, Telefon: +49 180 300 9191 0, Fax: +49 180 300 9193 0

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

Internet: www.funkwerk-ec.com

Inhaltsverzeichnis

Kapitel 1	Einleitung	1
1.1	Einsatzmöglichkeiten	2
1.2	Reinigen.	5
1.3	Zum Handbuch	5
Kapitel 2	Kurzanleitung	8
2.1	Einleitung	8
2.2	System-Voraussetzungen	8
2.3	Voreinstellungen	8
2.4	Inbetriebnahme.	10
2.4.1	Anschlüsse	11
2.4.2	Aufstellen und Anschließen	15
2.5	Konfiguration.	16
2.5.1	Vorbereitung	16
2.5.2	ADSL-Verbindung einrichten	22
2.5.3	Wireless LAN einrichten (nur bintec R1200w, R1200wu und R3000w)	23
2.6	Support Information	24
Kapitel 3	Technische Daten	25
3.1	bintec R1200	25
3.1.1	Lieferumfang.	25
3.1.2	Allgemeine Produktmerkmale	25
3.1.3	LEDs	27
3.1.4	Anschlüsse	29
3.1.5	Pin-Belegungen	30
3.2	bintec R1200w	32

3.2.1	Lieferumfang	32
3.2.2	Allgemeine Produktmerkmale	32
3.2.3	LEDs	35
3.2.4	Anschlüsse	36
3.2.5	Pin-Belegungen	37
3.3	bintec R1200wu	39
3.3.1	Lieferumfang	39
3.3.2	Allgemeine Produktmerkmale	40
3.3.3	LEDs	42
3.3.4	Anschlüsse	44
3.3.5	Pin-Belegungen	45
3.4	bintec R3000	49
3.4.1	Lieferumfang	49
3.4.2	Allgemeine Produktmerkmale	50
3.4.3	LEDs	52
3.4.4	Anschlüsse	54
3.4.5	Pin-Belegungen	54
3.5	bintec R3000w	57
3.5.1	Lieferumfang	57
3.5.2	Allgemeine Produktmerkmale	58
3.5.3	LEDs	60
3.5.4	Anschlüsse	62
3.5.5	Pin-Belegungen	63
3.6	bintec R3400	66
3.6.1	Lieferumfang	66
3.6.2	Allgemeine Produktmerkmale	67
3.6.3	LEDs	69
3.6.4	Anschlüsse	70
3.6.5	Pin-Belegungen	71
3.7	bintec R3800	74
3.7.1	Lieferumfang	74

3.7.2	Allgemeine Produktmerkmale	74
3.7.3	LEDs	77
3.7.4	Anschlüsse	79
3.7.5	Pin-Belegungen	79
3.8	bintec R4100	82
3.8.1	Lieferumfang	82
3.8.2	Allgemeine Produktmerkmale	83
3.8.3	LEDs	85
3.8.4	Anschlüsse	87
3.8.5	Pin-Belegungen	87
3.9	bintec R4300	90
3.9.1	Lieferumfang	91
3.9.2	Allgemeine Produktmerkmale	91
3.9.3	LEDs	93
3.9.4	Anschlüsse	95
3.9.5	Pin-Belegungen	96
Kapitel 4	Zugang und Konfiguration	100
4.1	Zugangsmöglichkeiten	100
4.1.1	Zugang über LAN.	100
4.1.2	Zugang über die serielle Schnittstelle	103
4.1.3	Zugang über ISDN	105
4.2	Anmelden	106
4.2.1	Benutzernamen und Passwörter im Auslieferungszustand	106
4.2.2	Anmelden zur Konfiguration	107
4.3	Konfigurationsmöglichkeiten	108
4.3.1	Funkwerk Configuration Interface	108
4.3.2	SNMP Shell	123
4.4	BOOTmonitor	124

Kapitel 5	Systemverwaltung	126
5.1	Status	126
5.2	Globale Einstellungen	129
5.2.1	System	129
5.2.2	Passwörter	132
5.2.3	Datum und Uhrzeit	133
5.2.4	Systemlizenzen	137
5.3	Schnittstellenmodus / Bridge-Gruppen	140
5.3.1	Schnittstellen.	142
5.4	Administrativer Zugriff	143
5.4.1	Zugriff	143
5.4.2	SSH	145
5.4.3	SNMP.	149
5.5	Remote-Authentifizierung	151
5.5.1	RADIUS	151
5.5.2	TACACS+	156
5.5.3	Optionen	160
Kapitel 6	Physikalische Schnittstellen	162
6.1	AUX	162
6.1.1	AUX	162
6.2	Ethernet-Ports	165
6.2.1	Portkonfiguration	165
6.3	ISDN-Ports	168
6.3.1	ISDN-Konfiguration	168
6.3.2	MSN-Konfiguration	176
6.4	ADSL-Modem	179
6.4.1	ADSL-Konfiguration.	179

6.5	SHDSL	182
6.5.1	SHDSL-Konfiguration	182
6.6	Serielle Ports	186
6.6.1	Optionen	186
6.7	UMTS / HSDPA	189
6.7.1	UMTS / HSDPA / HSUPA	189
Kapitel 7	LAN	192
7.1	IP-Konfiguration	192
7.1.1	Schnittstellen	192
7.2	VLAN	196
7.2.1	VLANs	197
7.2.2	Portkonfiguration	198
7.2.3	Verwaltung	199
Kapitel 8	Wireless LAN	201
8.1	WLAN1	202
8.1.1	Einstellungen Funkmodul	202
8.1.2	Drahtlosnetzwerke (VSS)	216
8.1.3	WDS Links.	222
8.1.4	Client Link	226
8.2	Verwaltung	230
8.2.1	Grundeinstellungen	230
Kapitel 9	Routing	232
9.1	Routen	232
9.1.1	IP-Routen	232
9.1.2	Optionen	237
9.2	NAT.	239

9.2.1	NAT-Schnittstellen	239
9.2.2	Portweiterleitung	241
9.3	RIP	245
9.3.1	RIP-Schnittstellen.	245
9.3.2	RIP-Filter	248
9.3.3	RIP-Optionen	251
9.4	Lastverteilung	254
9.4.1	Lastverteilungsgruppen	254
9.5	Multicast.	257
9.5.1	Weiterleiten	259
9.5.2	IGMP	260
9.5.3	Optionen	263
Kapitel 10	WAN.	266
10.1	Internet + Einwählen	266
10.1.1	PPPoE	268
10.1.2	PPTP	274
10.1.3	PPPoA	279
10.1.4	ISDN	284
10.1.5	GPRS/UMTS	293
10.1.6	AUX	298
10.1.7	IP Pools	305
10.2	ATM	306
10.2.1	Profile.	306
10.2.2	Dienstkategorien	311
10.2.3	OAM-Regelung.	314
10.3	Standleitung	318
10.3.1	Schnittstellen	319
10.4	Real Time Jitter Control	328
10.4.1	Regulierte Schnittstellen.	328

Kapitel 11	VPN	331
11.1	IPSec	331
11.1.1	IPSec-Peers	331
11.1.2	Phase-1-Profilе	341
11.1.3	Phase-2-Profilе	350
11.1.4	IP Pools	355
11.1.5	Optionen	356
11.2	L2TP	359
11.2.1	Tunnelprofile	360
11.2.2	Benutzer	364
11.2.3	Optionen	370
11.3	PPTP	371
11.3.1	PPTP Tunnel	371
11.3.2	Optionen	378
11.4	GRE	379
11.4.1	GRE-Tunnel	379
11.5	Zertifikate	381
11.5.1	Zertifikatsliste	382
11.5.2	CRLs	391
11.5.3	Zertifikatsserver	392
Kapitel 12	Firewall	394
12.1	Richtlinien	396
12.1.1	Filterregeln	396
12.1.2	QoS	399
12.1.3	Optionen	401
12.2	Schnittstellen.	403
12.2.1	Gruppen.	403

12.3	Adressen	404
12.3.1	Adressliste.	404
12.3.2	Gruppen.	406
12.4	Dienste	407
12.4.1	Diensteliste	407
12.4.2	Gruppen.	409
Kapitel 13	VoIP	411
13.1	Application Level Gateway	411
13.1.1	SIP-Proxys	411
13.1.2	SIP-Endpunkte	413
13.2	Media Gateway.	415
13.2.1	Teilnehmer	415
13.2.2	SIP-Konten	419
13.2.3	Anrufkontrolle	425
13.2.4	CLID-Umwandlung	429
13.2.5	Rufnummertransformation	431
13.2.6	Optionen	433
Kapitel 14	Lokale Dienste	437
14.1	DNS	437
14.1.1	Globale Einstellungen	439
14.1.2	Statische Hosts.	442
14.1.3	Domänenweiterleitung.	444
14.1.4	Cache.	446
14.1.5	Statistik	448
14.2	DynDNS-Client	449
14.2.1	DynDNS-Aktualisierung	449
14.2.2	DynDNS-Provider.	451
14.3	DHCP-Server	453

14.3.1	DHCP-Pool	454
14.3.2	IP/MAC-Bindung	456
14.3.3	DHCP-Relay-Einstellungen	458
14.4	Web-Filter	459
14.4.1	Globale Einstellungen	460
14.4.2	Filterliste	462
14.4.3	Black / White List	465
14.4.4	Verlauf	466
14.5	CAPI-Server	467
14.5.1	Benutzer	467
14.5.2	Optionen	469
14.6	Scheduling.	470
14.6.1	Zeitplan	470
14.6.2	Optionen	474
14.7	Überwachung	475
14.7.1	Hosts	476
14.7.2	Schnittstellen.	479
14.7.3	Ping-Generator	482
14.8	ISDN-Diebstahlsicherung	484
14.8.1	Optionen	484
14.9	Funkwerk Discovery	486
14.9.1	Gerätesuche	486
14.9.2	Optionen	491
14.10	UPnP	492
14.10.1	Schnittstellen.	492
14.10.2	Globale Einstellungen	494
Kapitel 15	Wartung	496
15.1	Diagnose	496
15.1.1	Ping-Test	496

15.1.2	DNS-Test	497
15.1.3	Traceroute-Test	498
15.2	Software & Konfiguration	498
15.2.1	Optionen	498
15.3	Neustart	503
15.3.1	Systemneustart.	503
Kapitel 16	Externe Berichterstellung.	505
16.1	Systemprotokoll	505
16.1.1	Syslog-Server	505
16.2	IP-Accounting	508
16.2.1	Schnittstellen.	508
16.2.2	Optionen	509
16.3	E-Mail-Benachrichtigung	510
16.3.1	E-Mail-Benachrichtigungs-Server	511
16.3.2	E-Mail-Benachrichtigungsempfänger	512
16.4	SNMP.	515
16.4.1	SNMP-Trap-Optionen	515
16.4.2	SNMP-Trap-Hosts	517
16.5	Activity Monitor	518
16.5.1	Optionen	519
Kapitel 17	Monitoring.	521
17.1	Internes Protokoll	521
17.1.1	Systemmeldungen	521
17.2	IPSec	522
17.2.1	IPSec-Tunnel	523
17.2.2	IPSec-Statistiken	525
17.3	ISDN/Modem	526

17.3.1	Aktuelle Anrufe	526
17.3.2	Anrufliste	528
17.4	Schnittstellen.	529
17.4.1	Statistik	529
17.5	WLAN.	530
17.5.1	WLAN1	530
17.5.2	VSS	532
17.5.3	WDS	535
17.5.4	Client Links	537
	Glossar	540
	Index	584

Kapitel 1 Einleitung

Die leistungsstarken Geräte **bintec R1xxx/R3xxx/R4xxx** wurden speziell für den High-speed Internet-Zugang und für die VPN-Anbindung in mittleren Unternehmen sowie Filialen entwickelt.

Über welche Fähigkeiten Ihr neues **bintec** Gateway verfügt, erfahren Sie in diesem Kapitel. Es gibt Ihnen einen Überblick über die Einsatzmöglichkeiten Ihres **bintec** Gateways. Ebenfalls in diesem Kapitel finden Sie Hinweise zu Struktur und Inhalt dieses Handbuchs.

Sicherheitshinweise

Was Sie im Umgang mit Ihrem **bintec** Gateway beachten müssen, erfahren Sie in den Sicherheitshinweisen, die im Lieferumfang Ihres Gerätes enthalten sind.

Installation

Wie Sie Ihr Gerät anschließen, erfahren Sie in [Inbetriebnahme](#) auf Seite 10. Dieses Kapitel sagt Ihnen auch, welche Vorbereitungen zur Konfiguration nötig sind.

Konfiguration

Wie Sie Ihr Gerät das Laufen lehren, erfahren Sie im Kapitel [Konfiguration](#) auf Seite 16. Dort zeigen wir Ihnen, wie Sie Ihr Gerät von einem Windows-PC aus in Betrieb nehmen und weitere nützliche Hilfsprogramme installieren. Am Ende dieses Kapitels sind Sie in der Lage, im Internet zu surfen, E-Mails zu verschicken und zu empfangen und eine Verbindung mit einem Partnernetz herzustellen, um beispielsweise auf Daten einer Firmenzentrale zuzugreifen.

Passwort

Wenn Sie bereits **bintec**-Geräte konfiguriert haben, Sie sich mit der Konfiguration gut auskennen und gleich beginnen möchten, fehlen Ihnen eigentlich nur noch der werkseitig eingestellte Benutzername und das Passwort.

Benutzername: *admin*

Passwort: *funkwerk*

**Achtung**

Denken Sie daran, das Passwort sofort zu ändern, wenn Sie sich das erste Mal auf Ihrem Gerät einloggen. Alle **bintec**-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 *Passwörter* auf Seite 132 beschrieben.

1.1 Einsatzmöglichkeiten

Netzwerke verbinden

Gateways werden verwendet, um Netzwerke miteinander zu verbinden und um Informationen zwischen den Netzwerken auszutauschen. So können Sie beispielsweise über Ihr Gerät eine Verbindung mit dem Netz Ihres Internet-Service-Providers herstellen und dadurch die gängigen Dienste des Internets nutzen, wie das World Wide Web (WWW) oder E-Mail.

Zugriff auf Zentrale

Über eine Verbindung zu einem anderen Partnernetz, z. B. Ihrer Firmenzentrale, können Sie bequem von Ihrem Heimarbeitsplatz oder von einer Filiale aus auf alle Informationen der Zentrale zugreifen, auch wenn diese geographisch weit entfernt liegt. Die Verbindung dieser lokalen Netze erfolgt über einen ISDN- oder über einen DSL-Anschluss. Wie groß dabei Ihr eigenes lokales Netzwerk ist - ob es aus mehreren Rechnern besteht oder ob es sich um einen Einzelarbeitsplatz handelt - spielt prinzipiell keine Rolle.

Ihr Gateway ist die Verbindung zur Außenwelt

Jedes Gerät dient als Bindeglied zwischen den einzelnen lokalen Netzwerken. Innerhalb jedes einzelnen Netzwerks (LAN) ist das Gerät wie ein normaler Rechner an das Netzwerk angeschlossen. Es hat die Aufgabe, gegebenenfalls Informationen aus dem eigenen Netz nach außen an ein anderes Netz (z. B. an das Netz Ihres Internet-Service-Providers oder das Netz einer Firmenzentrale) weiterzuleiten und dafür die geeigneten Wege (Routen) zu finden. Umgekehrt empfängt es Informationen und routet diese ins eigene Netz weiter.

Ein Gateway für alle

Wenn Sie ein lokales Netzwerk mit mehreren Rechnern haben, benötigen Sie nur ein einziges Gerät, um allen Rechnern im Netz den Zugriff auf das Internet oder die Firmenzentrale zu ermöglichen. Dies bedeutet bei mehreren Rechnern im Netz eine erhebliche Kostensparnis, da Sie sowohl weniger an Ausstattung als auch an Administration investieren. Beim Einsatz von ISDN-Karten oder Modems müssten Sie jeden Arbeitsplatz einzeln ausstatten.

High-Speed- Internetzugang

Wenn Sie mit den **bintec** Gateways einen High-Speed-Internetzugang realisieren, profitieren alle Teilnehmer im lokalen Netzwerk durch schnelleren Zugriff auf das Internet. Die verwendete Bandbreite ermöglicht wesentlich schnellere Internetanwendungen als herkömmliches ISDN oder Modems.

Automatisches Einwählen und Beenden

Ihr Gerät entscheidet - einmal konfiguriert - selbständig, ob und wie es eine Verbindung zum Internet-Service-Provider herstellen muss. Sie geben zum Beispiel in Ihren Browser eine externe WWW-Adresse ein, Ihr Gerät stellt fest, dass die angeforderte Adresse außerhalb Ihres eigenen LANs liegt und baut die Verbindung zu Ihrem Internet-Service-Provider und somit dem Internet automatisch auf. Und Ihr Gerät beendet die Verbindung wieder - damit Sie ggf. Kosten sparen - nach einer definierten Zeit (Shorthold), wenn keine Informationen mehr ausgetauscht werden.

Einfacher Datenzugriff

Entsprechend konfiguriert lässt Ihr Gerät Sie bequem auf Daten eines anderen Standortes, z. B. Ihrer Firmenzentrale, zugreifen. Sie können unter Windows ein Netzlaufwerk mit einem Rechner der Firmenzentrale verbinden. Im Windows Explorer klicken Sie dann einfach auf das Symbol dieser Verknüpfung und "surfen" in den Verzeichnissen und Daten des entfernten Rechners wie auf Ihrer eigenen Festplatte. Um den Auf- und Abbau der Verbindung kümmert sich Ihr Gateway.

Sicherheit/Firewall/DynDNS

Ihr Gerät verfügt über integrierte Firewall-Mechanismen. Es erfüllt damit alle Anforderungen an die Zugangssicherheit umfassend und kostengünstig. Es schirmt Ihr Netz gegen unbefugten Zugriff von außen ab. Dies wird möglich durch Funktionen wie NAT, Verschlüsselung, Filter, Monitoring sowie einer Stateful Inspection Firewall.

Die Stateful Inspection Firewall (SIF) bietet mittels dynamischer Paketfilterung einen wirkungsvollen Schutz vor Angriffen aus dem Internet. Die Handhabung der Firewall wird dabei durch zahlreiche vorkonfigurierte Dienste erleichtert. Um Partner trotz dynamischer IP Adressen ausfindig zu machen, unterstützen die Geräte die Funktion DynDNS. Die implementierte Funktion erlaubt die Verwendung des DynDNS-Dienstes führender DynDNS-Anbieter und es sind bereits einige Provider voreingestellt. Abgerundet werden die Sicherheitsfunktionen der Geräte durch eine optionale Content Filterung (kostenpflichtig, 30 Tage Testversion enthalten). Hierbei werden alle ausgehenden Internetanfragen klassifiziert, was das zuverlässige Ausfiltern nicht erwünschter Inhalte erlaubt.

Weitere Sicherheitsmerkmale

Mit der Scheduling-Funktion der Geräte lassen sich Zeiten definieren, in denen Benutzer

individuelle Rechte wie z. B. für den Internetzugang zugeteilt werden. Die VLAN Funktion der Geräte erlaubt die Zuteilung der Benutzer zu virtuellen Subnetzen und bietet ein zusätzliches Maximum an Sicherheit.

DMZ

Alle Geräte bieten die Möglichkeit, eine sogenannte "Demilitarisierte Zone" (DMZ) einzurichten. Dabei handelt es sich um ein separates Netzwerk, das sich zwischen dem internen LAN und dem Internet befindet. Die DMZ ist der Platz für alle Dienste, die direkt mit dem Internet Kontakt aufnehmen müssen. Wird ein Web- oder Mail-Server in der DMZ attackiert, so hat dies keinerlei Einfluss auf die Sicherheit Ihres internen Netzes.

IP Telefonie

Das Application Level Gateway erlaubt es, IP-Telefonen im LAN eine Verbindung zu SIP-Providern herzustellen, ohne dabei die Sicherheit der WAN-Anbindung zu vernachlässigen. Der SIP-Proxy überwacht hierzu den Signalisierungsprozess zwischen IP-Telefon und SIP-Provider und nimmt die notwendigen NAT- und Firewallfreigaben für die Dauer der Kommunikation dynamisch vor.

Wireless LAN

Die Wireless Schnittstelle überträgt die Daten mit max. 54 Mbit/s (802.11g) und ist kompatibel zur 11 Mbit/s Variante 802.11b im gleichen Frequenzbereich. Die Verschlüsselung über die WLAN-Schnittstelle kann über WPA und WPA2 erfolgen. Mittels Multi-SSID können virtuelle WLAN-Schnittstellen definiert werden. Hierdurch lassen sich unterschiedliche Zugangsregeln zum WLAN realisieren, z. B. zur Anmeldung von internen Mitarbeitern und externen Besuchern.

IPSec

Die Geräte verfügen über eine leistungsstarke IPSec Implementierung und besitzen zehn aktive VPN-Tunnel-Lizenzen ab Werk. Neben einer Verschlüsselung mittels AES oder 3DES bieten die Geräte eine Authentifizierung über Zertifikate oder Preshared Keys. Um den verschlüsselten Datenstrom zu optimieren, kann dieser mithilfe von IPComp komprimiert werden. Die Funktion Dead Peer Detection erlaubt die Überprüfung der Verfügbarkeit des Tunnelendpunktes und stellt diese bei Inaktivität wieder her. NAT-Traversal wird ebenso unterstützt wie die Einbindung von RADIUS oder TACACS+ zur Authentifizierung.

Konfiguration und Wartung

Für die Konfiguration Ihres Geräts bieten sich eine Reihe von Optionen. Die Konfiguration mit dem **Funkwerk Configuration Interface** erfolgt betriebssystemunabhängig.

Fernwartung

Die Geräte sind außerdem fernkonfigurier- und fernwartbar. Sobald Ihr Gerät - selbst im

Auslieferungszustand - an ISDN angeschlossen ist, können von einem anderen Standort aus (z. B. vom Administrator einer Firmenzentrale) Konfigurationseinstellungen vorgenommen werden. Die Einrichtung des Systems können Sie so einem Verantwortlichen in der Zentrale überlassen.

Modelle

Mit den Modellen **bintec R1xxx/R3xxx/R4xxx** stehen Ihnen flexible IP Access Router mit integriertem ADSL-Modem (**R3000** und **R3000w** mit Annex A und Annex B) und 4-Port-Switch zur Verfügung. Die Unterstützung von ADSL2+ erlaubt eine performante WAN-Anbindung und ermöglicht Download-Raten bis zu 24 Mbit/s. Ein SIP-Proxy regelt die transparente Kommunikation zu SIP-Providern und ermöglicht somit den Einsatz des Gerätes in VoIP-Szenarien, wie z. B. Internet-Telefonie.

Die Geräte **bintec R1200w**, **R1200wu** und **R3000w** bieten WLAN Funktionalität. Die WLAN-Funktion erlaubt die flexible Verwendung in kabellosen Umgebungen.

Neben einem 4-Port-Switch und einem weiteren Ethernet-Port für die LAN/WAN-Anbindung verfügen die Geräte über eine ISDN-Schnittstelle zum automatischen Backup oder zur Remote-Einwahl.

1.2 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 dadurch Ihr Gerät Schaden nimmt.

1.3 Zum Handbuch

Dieses Dokument ist gültig für **bintec**-Geräte mit einer System-Software ab Software-Version 7.8.1.

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


Benutzerhandbuch - Referenz

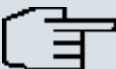


Kapitel	Beschreibung
Kurzanleitung	Diese enthält Anweisungen, wie Sie Ihr Gerät aufstellen, inbetriebnehmen und eine Basiskonfiguration erstellen.
Technische Daten	Dieser Abschnitt enthält eine Beschreibung aller technischen Eigenschaften der Geräte.

Kapitel	Beschreibung
Zugang und Konfiguration	Hier werden die verschiedenen Zugangs- und Konfigurationsmöglichkeiten erläutert.
Systemverwaltung	In diesen Kapiteln werden alle Konfigurationsoptionen des Funkwerk Configuration Interface beschrieben. Die einzelnen Menüs werden in der Reihenfolge in der Navigation beschrieben. In den einzelnen Kapiteln finden Sie auch weiterführende Erläuterungen zum jeweiligen Subsystem.
Physikalische Schnittstellen	
LAN	
Wireless LAN	
Routing	
WAN	
VPN	
Firewall	
VoIP	
Lokale Dienste	
Wartung	
Externe Berichterstattung	
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 sämtliche 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.

Symbol	Verwendung
	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 im Funkwerk Configuration Interface und in der Windows-Oberfläche.
nicht-proportional (Courier), z. B. <code>ping 192.168.1.254</code>	Kennzeichnet Kommandos, die Sie wie dargestellt eingeben müssen.
fett, z. B. Windows-Startmenü	Kennzeichnet Tasten, Tastenkombinationen und Windows-Begriffe.
fett, z. B. <i>biboAdmLoginTable</i>	Kennzeichnet Felder im Funkwerk Configuration Interface .
kursiv, z. B. <i>keiner</i>	Kennzeichnet Werte, die Sie eintragen bzw. die eingestellt werden können.
Online: blau und kursiv, z. B. www.funkwerk-ec.com	Kennzeichnet Hyperlinks.

Kapitel 2 Kurzanleitung

In diesem Kapitel erfahren Sie, wie Sie Ihr Gerät aufstellen, in Betrieb nehmen und eine Basiskonfiguration mit dem **Funkwerk Configuration Interface** erstellen.

2.1 Einleitung

Die Konfiguration Ihres Geräts wird mit dem **Funkwerk Configuration Interface** durchgeführt.

Der Weg zur Basiskonfiguration wird Ihnen im Folgenden Schritt für Schritt erläutert. Tiefergehende Netzwerkkenntnisse sind dabei nicht erforderlich. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

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

Die **BRICKware** enthält nützliche Applikationen zum Management Ihres Geräts.

2.2 System-Voraussetzungen

Ihr **bintec** Gateway bietet eine umfangreiche Ausstattung für den verschlüsselten Datentransfer und den Zugang zum Internet sowohl für Einzelarbeitsplätze als auch für Unternehmen.

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

- Betriebssystem Microsoft Windows ab Windows 2000
- Internet Explorer 6 oder 7, Mozilla Firefox ab Version 1.2
- Installierte Netzwerkkarte (Ethernet)
- CD-ROM-Laufwerk
- Installiertes TCP/IP-Protokoll
- Hohe Farb-Anzeige (mehr als 256 Farben) für die korrekte Darstellung der Grafiken

2.3 Voreinstellungen

Vorkonfigurierte Einstellungen

Ihr Gerät wird mit einer vordefinierten IP-Konfiguration ausgeliefert:

- **IP-Adresse:** *192.168.0.254*
- **Netzmaske:** *255.255.255.0*

Benutzen Sie im Auslieferungszustand folgende Zugangsdaten zur Konfiguration Ihres Geräts:

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



Hinweis

Alle **bintec**-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!

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 **Funkwerk Configuration Interface** im Menü **Wartung** -> **Software & Konfiguration** vornehmen.

2.4 Inbetriebnahme

Ihr Gateway ermöglicht Ihnen eine Vielzahl von Verbindungsvarianten:

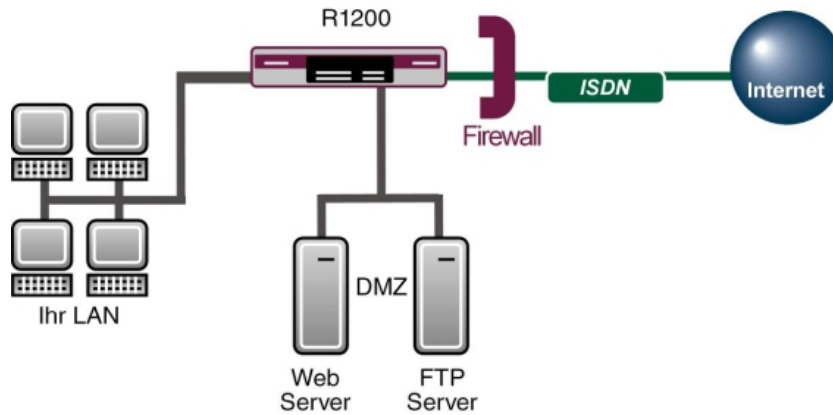


Abb. 2: Basisszenario **bintec R1200**

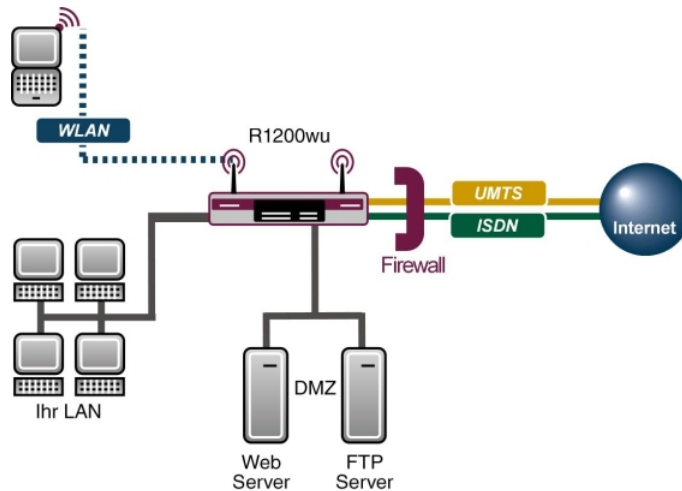


Abb. 3: Basisszenario **bintec R1200wu**



Achtung

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

2.4.1 Anschlüsse

Alle Anschlüsse befinden sich auf der Geräterückseite.

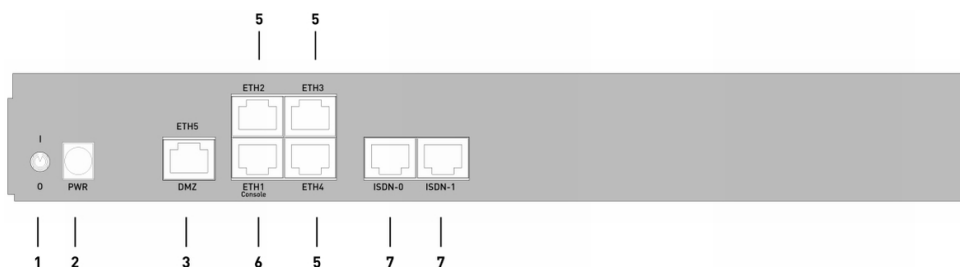


Abb. 4: Rückseite **bintec R1200**

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle

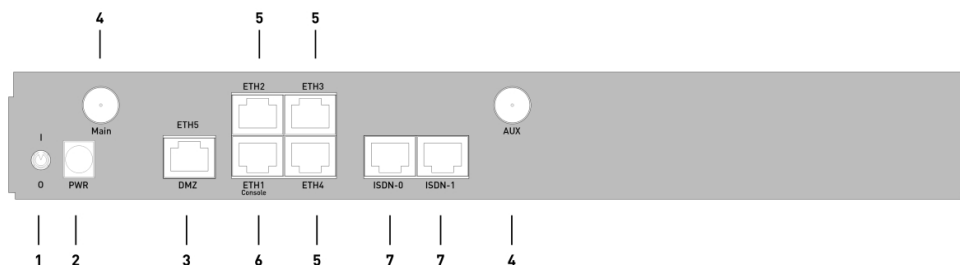


Abb. 5: Rückseite **bintec R1200w**

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
4	Main und AUX	RSMA-Anschluss
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle

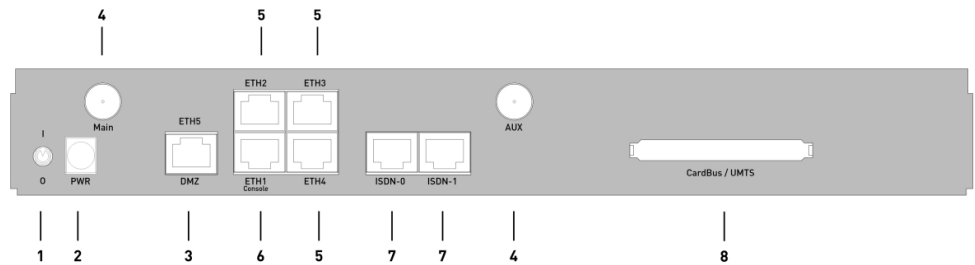


Abb. 6: Rückseite bintec R1200wu

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
4	Main und AUX	RSMA-Anschluss
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
8	CardBus / UMTS	CardBus Slot für UMTS-Modem

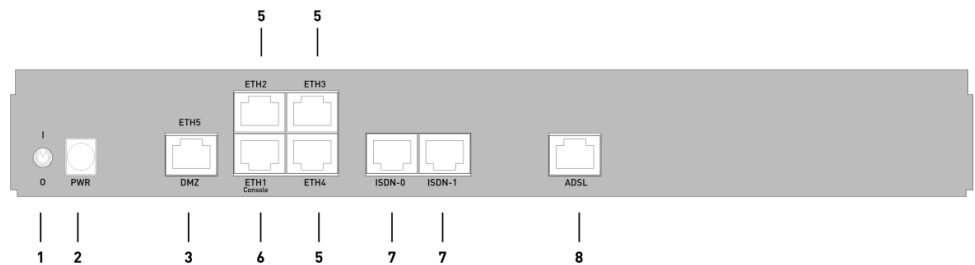


Abb. 7: Rückseite bintec R3000

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
8	ADSL	ADSL-Schnittstelle

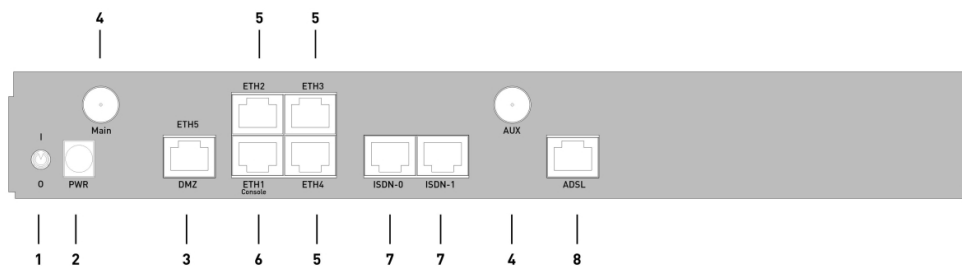


Abb. 8: Rückseite **bintec R3000w**

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
4	Main und AUX	RSMA-Anschluss
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
8	ADSL	ADSL-Schnittstelle

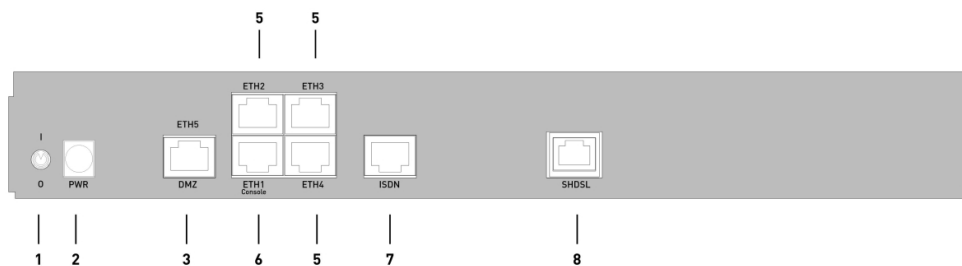
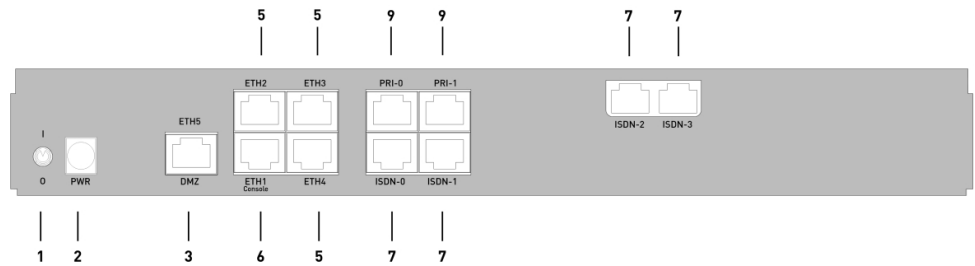
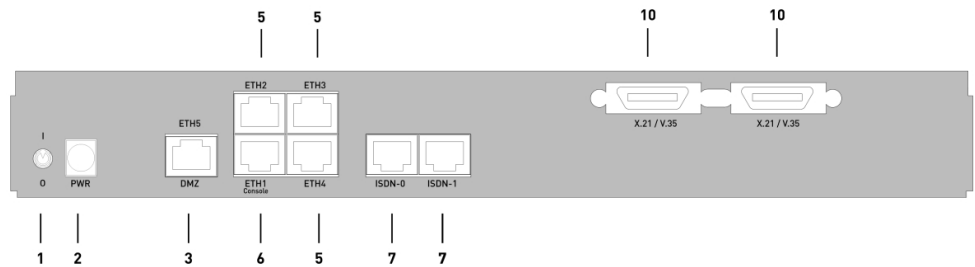


Abb. 9: Rückseite **bintec R3400 und R3800**

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN	ISDN-Schnittstelle
8	SHDSL	SHDSL-Schnittstelle

Abb. 10: Rückseite **bintec R4100**

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-3	ISDN-Schnittstelle
9	PRI-0 - PRI-1	ISDN-PRI-Schnittstelle

Abb. 11: Rückseite **bintec R4300**

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
10	X.21 / V.35	X.21-Schnittstelle

2.4.2 Aufstellen und Anschließen

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!

Bei falscher Verkabelung der ISDN- und ETH-Schnittstellen kann es zum Defekt Ihres Geräts kommen! Verbinden Sie immer nur die ETH-Schnittstelle des Geräts mit der LAN-Schnittstelle des Rechners/Hubs oder einer ggf. vorhandenen WAN-Schnittstelle und die ISDN-Schnittstelle des Geräts nur mit dem ISDN-Anschluss

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

- (1) Antennen (nur **R1200w**, **R1200wu** und **R3000w**): Schrauben Sie die mitgelieferte externe Standardantenne auf die dafür vorgesehenen RSMA-Anschlüsse **Main** und **AUX** und richten Sie die Antennen aus.
- (2) Stellen Sie Ihr Gerät auf eine feste, ebene Unterlage.
- (3) LAN: Zur Standardkonfiguration Ihres Geräts über Ethernet, verbinden Sie den ersten Switch-Port (**ETH1**) Ihres Geräts über das mitgelieferte Ethernet-Kabel mit Ihrem LAN. Das Gerät erkennt automatisch, ob es an einen Switch oder direkt an einen PC angeschlossen wird.
- (4) ADSL (nur **R3000** und **R3000w**): Verbinden Sie die ADSL-Schnittstelle (**ADSL**) Ihres Geräts über das mitgelieferte DSL-Kabel mit dem DSL-Ausgang des Splitters.
- (5) SHDSL (nur **R3400** und **R3800**): Verbinden Sie die SHDSL-Schnittstelle (**SHDSL**) Ihres Geräts über das mitgelieferte DSL-Kabel mit Ihrem SHDSL-Anschluss.
- (6) Netzanschluss: Schließen Sie das Gerät mit dem mitgelieferten Netzadapter an eine Steckdose an.

Optionale Anschlüsse

- ISDN: Schließen Sie die ISDN-Schnittstelle (**ISDN** oder **ISDN-x**) des Geräts mit dem mitgelieferten ISDN-Kabel an Ihre ISDN-Dose an.
- Weitere LANs/WANs: Schließen Sie beliebige weitere Endgeräte in Ihrem Netzwerk an den verbleibenden Switch-Ports (**ETH2**, **ETH3** oder **ETH4**) Ihres Geräts mittels weiterer Ethernet-Kabel an.
- Serielle Verbindung: Für alternative Konfigurationsmöglichkeiten verbinden Sie die serielle Schnittstelle Ihres PCs mit der seriellen Schnittstelle des Geräts. Die serielle Schnittstelle ist als zusätzliche Belegung der Ethernetbuchse 1 (**ETH1**) realisiert. Verwenden

Sie dazu das mitgelieferte serielle Kabel, und schließen Sie Ihr Netzwerk ggf. an einer anderen Ethernetbuchse an. Standardmäßig ist die Konfiguration über die serielle Schnittstelle jedoch nicht vorgesehen.

- xDSL-Modem oder DMZ: Verbinden Sie die WAN-Schnittstelle (**ETH5/DMZ**) Ihres Geräts über ein weiteres Ethernet-Kabel mit einem xDSL-Modem (nicht im Lieferumfang enthalten) oder mit dem Ethernet-Anschluss Ihrer DMZ.
- PRI (nur **R4100**): Schließen Sie die ISDN-PRI-Schnittstelle (**PRI-0** oder **PRI-1**) des Geräts an Ihrem PRI-Anschluss an.
- X.21 (nur **R4300**): Verbinden Sie eine X.21-Schnittstelle Ihres Geräts über ein geeignetes Kabel (welches Sie als Zubehör zu Ihrem Router bestellen können) mit Ihrem **X.21/V.35**- oder **X.21/V.36**-Anschluss. Achten Sie darauf, dass Sie eine freigeschaltete X.21-Schnittstelle benutzen. Ab Werk ist die linke X.21-Schnittstelle auf die Rückseite des Geräts freigeschaltet. Die rechte X.21-Schnittstelle kann zusätzlich per Lizenz freigeschaltet werden.
- UMTS (nur **R1200wu**): Schieben Sie die UMTS-Karte in den **CardBus / UMTS** Slot.

Das Gerät ist nun für die Konfiguration mit dem **Funkwerk Configuration Interface** vorbereitet.

2.5 Konfiguration

In diesem Kapitel erfahren Sie, wie Sie die Konfiguration vorbereiten, welche Daten Sie vorher sammeln müssen, wie Sie die Konfiguration eines üblichen ADSL-Anschlusses durchführen, ggf. Anpassungen der PC-Konfigurationen im Netzwerk machen und nach Abschluss der Konfiguration die Verbindung testen.

2.5.1 Vorbereitung

Zur Vorbereitung der Konfiguration sollten Sie...

- die benötigten Daten für die Grundkonfiguration und den Internet-Anschluss bereitlegen sowie ggf. die nötigen Daten für die Anbindung der gewünschten WLAN-Clients sammeln
- überprüfen, ob der PC, von dem aus Sie die Konfiguration vornehmen wollen, die notwendigen Voraussetzungen erfüllt.

Darüber hinaus können Sie ...

- die **BRICKware**-Software installieren, die Ihnen weitere Werkzeuge zur Arbeit mit Ihrem Gerät zur Verfügung stellt. Die Installation ist optional und für die Konfiguration oder den Betrieb des Geräts nicht zwingend erforderlich.

2.5.1.1 Daten sammeln

Die wesentlichen Daten für die Konfiguration mit dem **Funkwerk Configuration Interface** haben Sie schnell gesammelt, denn es sind keine Informationen erforderlich, die vertiefte Netzwerkkenntnisse voraussetzen.

Gegebenenfalls können Sie die Beispielwerte übernehmen.

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

- Grundkonfiguration (sofern sich Ihr Gerät im Auslieferungszustand befindet)
- Internetzugang (optional)
- Wireless LAN (optional, nur für **R1200w**, **R1200wu** und **R300w**)
- Firmennetzanbindung (optional)

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

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:

Basisinformationen

Zugangsdaten	Beispielwert	Ihre Werte
IP-Adresse Ihres Gateways	192 . 168 . 0 . 254	
Netzmaske Ihres Gateways	255 . 255 . 255 . 0	

Internetzugang

Wenn Sie einen Internetzugang einrichten wollen, brauchen Sie einen Internet-Service-Provider (kurz ISP). Von Ihrem ISP bekommen Sie Ihre persönlichen Zugangsdaten mitgeteilt. Die Bezeichnungen der benötigten Zugangsdaten können unter Umständen von ISP zu ISP variieren. Grundsätzlich jedoch handelt es sich um die gleiche Art von Information, die Sie zur Einwahl benötigen.

In der nachfolgenden Tabelle sind die Zugangsdaten zusammengestellt, die Ihr Gerät für eine DSL-Internet-Verbindung benötigt:

Daten für den Internetzugang

Zugangsdaten	Beispielwert	Ihre Werte
Provider-Name	<i>GoInternet</i>	
Protokoll	<i>PPP over Ethernet (PPPoE)</i>	
Enkapsulierung	<i>bridged-no-fcs</i>	
VPI (Virtual Path Identifier)	<i>1</i>	
VCI (Virtual Circuit Identifier)	<i>32</i>	
Ihr Benutzername	<i>MyName</i>	
Passwort	<i>TopSecret</i>	

Einige ISPs, wie z. B. T-Online, benötigen zusätzlich Informationen:

Zusätzliche Informationen für T-Online

Zugangsdaten	Beispielwert	Ihre Werte
T-Online-Nummer	<i>081512345678</i>	
Mitbenutzerkennung	<i>0001</i>	

**Hinweis**

Geben Sie bei der Konfiguration eines T-Online-Internetzugangs in das Feld **Benutzername** nacheinander und ohne Leerzeichen folgende Nummern ein:

Anschlusskennung (12-stellig) + T-Online Nummer (meist 12-stellig) + Mitbenutzer-
nummer (für den Hauptnutzer immer 0001)

Sollte Ihre T-Online Nummer weniger als 12 Stellen enthalten, muss zwischen der T-
Online Nummer und der Mitbenutzernummer das Zeichen "#" stehen.

Wenn Sie T-DSL nutzen, müssen Sie dieser Zahlenfolge noch die Endung
"@t-online.de" hinzufügen.

Ihr Benutzername könnte dann so aussehen:

00012345678906112345678#0001 @t-online.de

Wireless LAN (nur bei bintec R1200w, bintec R1200wu und bintec R3000w)

Sie können Ihr Gerät als Access-Point betreiben und somit mittels WLAN (Wireless LAN) einzelne Arbeitsstationen (z. B. Laptops, PCs mit Wireless-Karte oder Wireless-Adapter) per Funk in Ihr lokales Netzwerk einbinden und miteinander kommunizieren lassen. Die Ta-

belle “Daten für die Wireless LAN Konfiguration” zeigt die Angaben, die dazu benötigt werden.

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.

Beachten Sie dazu Folgendes:

- Folgen Sie den Sicherheitshinweisen bei der Konfiguration Ihres WLANs.
- Bitte lesen Sie auch die Informationen zum WLAN-Betrieb, die vom Bundesministerium für Sicherheit in der Informationstechnik herausgegeben werden (<http://www.bsi.bund.de>).

Daten für die Wireless LAN Konfiguration

Zugangsdaten	Beispielwert	Ihre Werte
Preshared Key für WPA-PSK	ohne Vorgabe	
Aufstellungsort Ihres Geräts	<i>Germany</i>	
Kanal, der für WLAN verwendet werden soll	3	
Netzwerkname (SSID) für Ihr WLAN	ohne Vorgabe	
Sichtbarkeit des Netzwerknamens	<i>nicht sichtbar</i>	
Sicherheitseinstellung	<i>WPA-PSK</i>	

Firmennetzanbindung

Für die Anbindung eines entfernten Netzwerkes (z. B. Firmenzentrale) müssen Sie einige Daten der Gegenstelle kennen, die Ihren Ruf annehmen soll. Genauso muss die Gegenstelle Ihre Daten kennen. Diese Daten müssen Sie gemeinsam absprechen.

Vor jeder Verbindung prüfen Ihr Gerät und das Gerät Ihrer Firmenzentrale, ob sie den Ruf des Partners entgegennehmen. Die Rufannahme geschieht nur bei korrekter Authentifizierung, um das Netz vor unbefugtem Zugriff zu schützen. Die Authentifizierung erfolgt anhand des gemeinsamen Passwortes und anhand von zwei Kennungen, die Sie und Ihr Partner für die Verbindung verwenden.

Daten für die Anbindung an ein Firmennetz

Zugangsdaten	Beispielwert	Ihre Werte
Partnername (Kennung der Firmenzentrale)	<i>BigBoss</i>	
Einwahlnummer: (Rufnummer des Geräts der Firmenzentrale)	<i>0911987654321</i>	
Lokaler Name (Ihre eigene Kennung. Diesen Namen muss der Partner (Ihre Firmenzentrale) bei seinem Gerät als Partnernamen eintragen.)	<i>LittleIndian</i>	
Passwort (Gemeinsames Passwort für diese Verbindung, das auf beiden Geräten eingetragen wird.)	<i>Secret</i>	
Netzadresse(n) der Firmenzentrale	<i>10.1.1.0</i>	
Netzmaske(n) der Firmenzentrale	<i>255.255.255.0</i>	

2.5.1.2 PC einrichten

Um Ihr Gerät über das Netzwerk erreichen und eine Konfiguration mittels **Schnellinstallations-Assistent** 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.
- Weisen Sie Ihrem PC eine feste IP-Adresse zu.

TCP/IP-Protokoll prüfen

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

- (1) Klicken Sie im Startmenü auf **Einstellungen -> Netzwerk- und DFÜ-Verbindungen** (Windows 2000) bzw. **Systemsteuerung -> Netzwerkverbindungen** (Windows XP).
- (2) Klicken Sie auf **LAN-Verbindung**.
- (3) Klicken Sie im Statusfenster auf **Eigenschaften**.

- (4) Suchen Sie in der Liste der Netzwerkkomponenten den Eintrag **Internetprotokoll (TCP/IP)**.

TCP/IP-Protokoll installieren

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

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

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 ein.

Gateway IP-Adresse im PC eintragen

Fahren Sie dann fort, indem Sie wie folgt die IP-Adresse des Gateways in die Konfiguration Ihres PCs eintragen:

- (1) Geben Sie in **Internetprotokoll (TCP/IP)** -> **Eigenschaften** unter **Standardgateway** die IP-Adresse Ihres Gateways ein.
- (2) Tragen Sie unter **Folgende DNS-Serveradressen verwenden** die IP-Adresse Ihres Geräts ein.
- (3) Klicken Sie auf **OK**.
- (4) Schließen Sie das Statusfenster mit **OK**.



Der Rechner verfügt nun über eine IP-Konfiguration und kann über das Gateway auf das Internet zugreifen.



Hinweis

Das **Funkwerk Configuration Interface** erreichen Sie, indem Sie in einem unterstützten Browser (Internet Explorer 6 oder 7, Mozilla Firefox ab Version 1.2) die IP-Adresse Ihres Gerätes eingeben (192.168.0.254) und sich mit den voreingestellten Anmeldedaten (**User:** *admin*, **Password:** *funkwerk*) anmelden.

2.5.2 ADSL-Verbindung einrichten

- (1) Gehen Sie in das Menü **WAN** -> **ATM** -> **Profile**. Es existiert bereits ein vorkonfiguriertes Profil, das Sie Ihren Bedürfnisse anpassen können.
- (2) Wählen Sie , um die Einstellungen des vorhandenen Profils überprüfen zu können.
- (3) Überprüfen Sie lediglich, ob die Werte für **Virtueller Pfad-Identifizier (VPI)** und **Virtueller Kanal-Identifizier (VCI)** sowie die **Enkapsulierung** mit den Daten übereinstimmen, die Sie von Ihrem ISP bekommen haben. Wenn Sie keine entsprechenden Daten bekommen haben, belassen Sie es bei den Standardwerten. Der Wert *Ethernet über ATM* für **Typ** entspricht einer PPPoE-Verbindung.
- (4) Ändern Sie die Beschreibung des Profils nach Belieben, z. B. *GoInternet*.
- (5) Wenn Sie Änderungen vorgenommen haben, bestätigen Sie mit **OK**.
- (6) Gehen Sie nun ins das Menü **Internet+Einwählen** -> **PPPoE** und klicken Sie auf **Neu**.
- (7) Geben Sie eine **Beschreibung** für die Verbindung ein, z. B. *GoInternet*
- (8) Wählen Sie für **PPPoE-Ethernet-Schnittstelle** *ethoa50-0* aus.
- (9) Geben Sie bei **Benutzername** und **Passwort** die Daten ein, die Sie als Zugangsdaten von Ihrem ISP bekommen haben.
- (10) Wenn Sie einen Anschluss mit einer Flatrate haben, aktivieren Sie die Checkbox bei **Immer aktiv**. Die ADSL-Verbindung wird dadurch konstant aufrecht erhalten und bei einem Verbindungsabbruch sofort wieder hergestellt.
- (11) Aktivieren Sie die Checkboxen bei **Standardroute** und **NAT-Eintrag erstellen**.
- (12) Lassen Sie alle anderen Werte auf den Standardeinstellungen.
- (13) Bestätigen Sie mit **OK**. Sie gelangen zurück in die Übersicht der PPPoE-Verbindungen.
- (14) Wenn die Verbindung aktiv ist, sehen Sie in der Spalte **Status** folgendes Symbol: . Dies muss jedoch nicht automatisch der Fall sein, daher sollten Sie die Verbindung wie in *Konfiguration prüfen* auf Seite 23 beschrieben überprüfen.
- (15) Speichern Sie die Konfiguration mit dem Button **Konfiguration speichern** oberhalb der Menünavigation.

2.5.2.1 Konfiguration prüfen

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

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

- (1) Testen Sie die Verbindung zum Gerät. Klicken Sie im Startmenü auf **Ausführen** und geben Sie `ping` gefolgt von einem Leerzeichen und der IP-Adresse Ihrer Anlage ein (z. B. `192.168.0.254`). Es erscheint ein Fenster mit dem Hinweis "Antwort von...".
- (2) Testen Sie den Internetzugang, indem Sie im Internet Browser www.funkwerk-ec.com eingeben. Auf den Internet-Seiten der Funkwerk Enterprise Communications GmbH finden Sie Neuigkeiten, Updates und weiterführende Dokumentation.



Hinweis


Durch eine Fehlkonfiguration der Geräte im LAN kann es zu ungewollten Verbindungen und erhöhten Gebühren kommen! Kontrollieren Sie, ob das Gerät Verbindungen nur zu gewollten Zeiten aufbaut! Beobachten Sie die Leuchtanzeigen Ihres Geräts (Leuchtanzeige ISDN, ADSL und die Ethernet-Schnittstellen, an denen Sie ein oder mehrere WANs angeschlossen haben).

2.5.3 Wireless LAN einrichten (nur bintec R1200w, R1200wu und R3000w)

Gehen Sie folgendermaßen vor, um ihr Gerät als Access Point im WPA-PSK-Modus zu nutzen:

- (1) Gehen Sie in das Menü **Wireless LAN** -> **WLAN1**. Es existiert bereits ein vorkonfiguriertes VSS: **Funkwerk-ec**.
- (2) Wählen Sie , um die Einstellungen des vorhandenen VSS anpassen zu können.
- (3) Stellen Sie den Betriebsmodus auf *Access-Point* und bestätigen Sie Ihre Angabe mit **OK**.
- (4) Jetzt können Sie im Menü **Wireless LAN** -> **WLAN1** -> **Drahtlosnetzwerke (VSS)** -> **Neue VSS** neue Drahtlosnetzwerke einrichten.
- (5) Ändern Sie den **Netzwerkname (SSID)** nach Belieben, z. B. *Client-1*.
- (6) Wählen Sie unter **Sicherheitsmodus** *WPA-PSK*.
- (7) Geben Sie unter **Preshared Key** ein beliebiges Passwort ein. Es muss mindestens acht Zeichen lang sein und sollte zur Sicherheit Sonderzeichen, Zahlen sowie

Groß- und Kleinbuchstaben enthalten.

- (8) Behalten Sie für alle anderen Felder die voreingestellten Werte bei und bestätigen Sie mit **OK**. Sie gelangen zurück zur VSS-Übersicht.
- (9) Klicken Sie in der Zeile des gerade angepassten VSS unter **Aktion** auf , um das VSS und das Funkmodul zu aktivieren.
- (10) Speichern Sie die Konfiguration mit dem Button **Konfiguration speichern** oberhalb der Menünavigation.

2.5.3.1 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 die Wireless-LAN-Verbindung zu konfigurieren, gehen Sie bitte folgendermaßen vor:

- (1) Klicken Sie mit der rechten Maustaste auf **Start -> Einstellungen -> Netzwerkverbindungen -> Drahtlose Netzwerkverbindung**.
- (2) Wählen Sie anschließend **Eigenschaften** 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 *WPA-PSK*.
- (3) Bei **Datenverschlüsselung** konfigurieren Sie *TKIP*.
- (4) Unter **Netzwerkschlüssel** und **Netzwerkschlüssel bestätigen** geben Sie den zuvor konfigurierten Preshared Key an.
- (5) Verlassen Sie die Menüs jeweils mit **OK**.

2.6 Support Information

Wenn Sie zu Ihrem neuen Produkt Fragen haben oder zusätzliche Informationen wünschen, erreichen Sie das Support Center von Funkwerk Enterprise Communications GmbH unter folgender Telefonnummer oder E-Mail Hotline:

+49 911 9673 1550

hotline@funkwerk-ec.com

Ausführliche Informationen zu unseren Support Leistungen erhalten Sie unter www.funkwerk-ec.com.

Kapitel 3 Technische Daten

In diesem Kapitel sind alle Hardware-Eigenschaften der Geräte **R1200**, **R1200w**, **R1200wu**, **R3000**, **R3000w**, **R3400**, **R3800**, **R4100** und **R4300** zusammengefasst.

3.1 bintec R1200

3.1.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - Steckernetzteil
- **bintec Companion CD**
- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.1.2 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
Produktname	bintec R1200

Eigenschaft	Wert
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	18 (1x Power, 1x Status, 5x2 Ethernet, 3x2 Funktion)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 13 Watt
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud

Eigenschaft	Wert
ISDN-WAN S0 (2)	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)

3.1.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

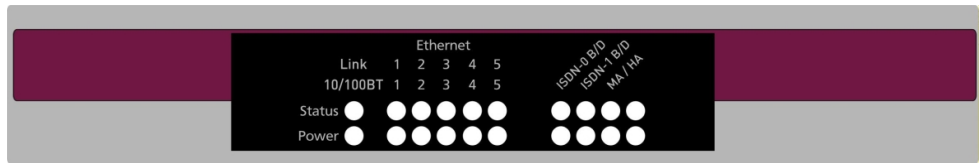


Abb. 12: LEDs von **bintec R1200**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ISDN-1 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.

LED	Status	Information
ISDN-1 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
MA / HA obere Reihe	blinkend	BRRP-Pakete werden empfangen.
MA / HA untere Reihe	an	Ein Benutzer ist auf dem System eingeloggt (z. B. über Telnet).

3.1.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R1200** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle und zwei ISDN-Schnittstellen.

Die Anschlüsse sind folgendermaßen angeordnet:

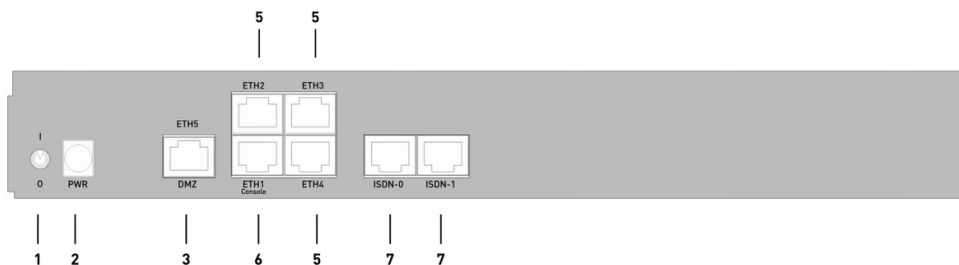


Abb. 13: **bintec R1200** Rückseite

bintec R1200 Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle

3.1.5 Pin-Belegungen

3.1.5.1 Ethernet-Schnittstelle

bintec R1200 verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

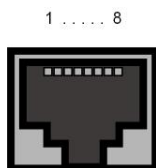


Abb. 14: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.1.5.2 ISDN-So-Schnittstelle

bintec R1200 verfügt über zwei zusätzliche ISDN-So-Schnittstellen, die z. B. für Backup-Funktionen genutzt werden können.

Der Anschluss erfolgt über eine RJ45-Buchse:

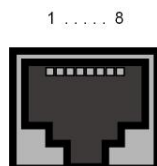


Abb. 15: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.2 bintec R1200w

3.2.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - Steckernetzteil
- Antennen:
 - zwei Standardantennen
- **bintec Companion CD**
- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.2.2 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
Produktname	bintec R1200w
Maße und Gewicht:	

Eigenschaft	Wert
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm + 8 mm (Antennenbuchse)
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 4x2 Function)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 13 Watt
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0 (2)	Fest eingebaut.
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port

Eigenschaft	Wert
Vorhandene Buchsen:	802.11b, 802.11g und 802.11a mit Antenna Diversity
Serielle Schnittstelle V.24	
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	RJ45-Buchse
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)



Hinweis

Antenna Diversity

Die beiden Antennen sind nicht gleichberechtigt. Eine wird sowohl zum Senden und Empfangen verwendet (als "Main", "Primary" oder "1" gekennzeichnet; die Antenne neben dem Power-Schalter), die zweite nur zum Empfangen. Während des Empfangs prüft der AP (Access Point), auf welcher Antenne ein besseres Signal ankommt, dieses wird dann zur Dekodierung verwendet.

3.2.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

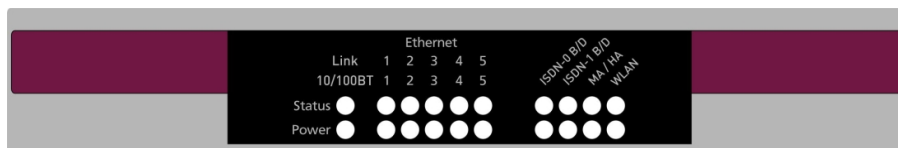


Abb. 16: LEDs von **bintec R1200w**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D	an	Ein ISDN B-Kanal ist aktiv.

LED	Status	Information
untere Reihe		
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ISDN-1 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-1 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
MA / HA obere Reihe	blinkend	BRRP-Pakete werden empfangen.
MA / HA untere Reihe	an	Ein Benutzer ist auf dem System eingeloggt (z. B. über Telnet).
WLAN obere Reihe	an	Das WLAN-Modul ist aktiv.
WLAN untere Reihe	blinkend	Datenverkehr über die WLAN-Schnittstelle.

3.2.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R1200w** verfügt über einen 4-Port-Ethernet-Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle und zwei ISDN-Schnittstellen.

Die Anschlüsse sind folgendermaßen angeordnet:

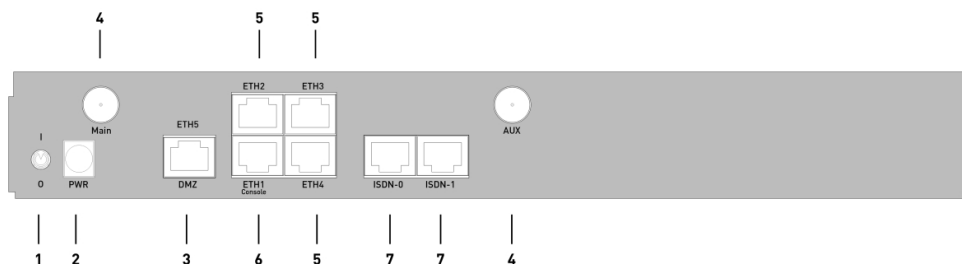


Abb. 17: bintec R1200w Rückseite

bintec R1200w Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
4	Main und AUX	RSMA-Anschluss
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle

3.2.5 Pin-Belegungen

3.2.5.1 Ethernet-Schnittstelle

bintec R1200w verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port-Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

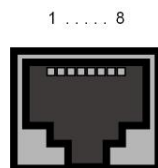


Abb. 18: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.2.5.2 ISDN-So-Schnittstelle

bintec R1200w verfügt über zwei zusätzliche ISDN-So-Schnittstellen, die z. B. für Backup-Funktionen genutzt werden können.

Der Anschluss erfolgt über eine RJ45-Buchse:

1 8

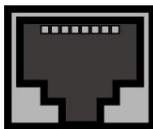


Abb. 19: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.3 bintec R1200wu

3.3.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - Steckernetzteil
- Antennen:
 - zwei Standardantennen
- **bintec Companion CD**

- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.3.2 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
Produktname	bintec R1200wu
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm + 8 mm (Antennenbuchse)
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 4x2 Function)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 13 Watt
Spannungsversorgung	24 V AC 1 A EU PSU
Umweltanforderungen:	

Eigenschaft	Wert
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
Ethernet IEEE 802.3 LAN (4 Port Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0 (2)	Fest eingebaut.
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
WLAN-Schnittstelle (Antennen)	802.11b, 802.11g und 802.11a mit Antenna Diversity
CardBus Schnittstelle (PCMCIA)	Schnittstelle zur Integration einer UMTS-Modemkarte
Vorhandene Buchsen:	
Serielle Schnittstelle	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
CardBus Schnittstelle	68-polige PCMCIA-Buchse
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPsec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix

Eigenschaft	Wert
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)



Hinweis

Antenna Diversity

Die beiden Antennen sind nicht gleichberechtigt. Eine wird sowohl zum Senden und Empfangen verwendet (als "Main", "Primary" oder "1" gekennzeichnet; die Antenne neben dem Power-Schalter), die zweite nur zum Empfangen. Während des Empfangs prüft der AP (Access Point), auf welcher Antenne ein besseres Signal ankommt, dieses wird dann zur Dekodierung verwendet.

3.3.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

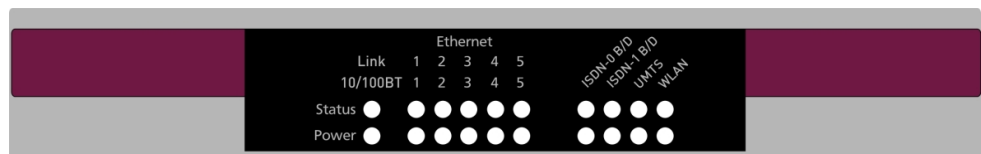


Abb. 20: LEDs von **bintec R1200wu**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.

LED	Status	Information
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ISDN-1 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-1 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
UMTS obere Reihe	an	UMTS-Verbindung hergestellt.
UMTS untere Reihe	blinkend	Datenverkehr über UMTS.

LED	Status	Information
WLAN obere Reihe	blinkend	Datenverkehr über die WLAN-Schnittstelle.
WLAN untere Reihe	langsam blinkend	Das WLAN-Modul ist aktiv.
	an	Mindestens ein WLAN-Client ist verbunden.

3.3.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R1200wu** verfügt über einen 4-Port-Ethernet-Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle und zwei ISDN-Schnittstellen sowie über einen CardBus Slot zur Integration eines UMTS-Modems.

Die Anschlüsse sind folgendermaßen angeordnet:

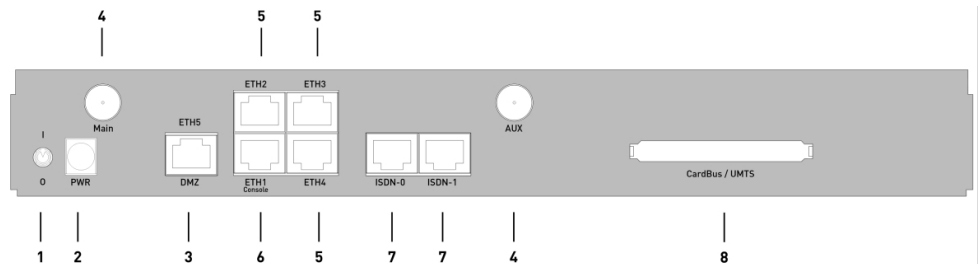


Abb. 21: **bintec R1200wu** Rückseite

bintec R1200wu Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
4	Main und AUX	RSMA-Anschluss
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
8	CardBus	CardBus Slot für UMTS-Modem

3.3.5 Pin-Belegungen

3.3.5.1 Ethernet-Schnittstelle

bintec R1200wu verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port-Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

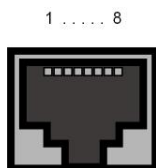


Abb. 22: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.3.5.2 ISDN-So-Schnittstelle

bintec R1200wu verfügt über zwei zusätzliche ISDN-So-Schnittstellen, die z. B. für Backup-Funktionen genutzt werden können.

Der Anschluss erfolgt über eine RJ45-Buchse:

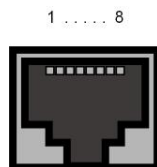


Abb. 23: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.3.5.3 CardBus-Schnittstelle (PCMCIA)

Die CardBus-Schnittstelle erlaubt die Integration eines UMTS-CardBus- Modems in das System.

Die Modemkarte wird in den vorhandenen CardBus Slot eingeführt und vom System automatisch integriert. Sie können die Karte in das laufende Gerät einführen (hot-pluggable).

Falls die Karte nicht automatisch integriert wird, unterstützt das System diese spezielle Karte nicht. Bei Fragen steht Ihnen unser Support zur Verfügung.

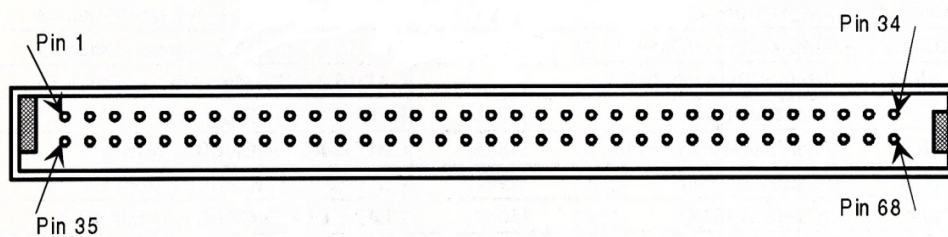


Abb. 24: 68-Pin-CardBus-Steckplatz für UMTS-Modemkarte

Die Pin-Zuordnung ist wie folgt:

Pin-Zuordnung des CardBus-Steckplatzes

Pin	Funktion	Beschreibung
1	GND	Masse
2	CAD0	Mpx-Adresse/Daten 0
3	CAD1	Mpx-Adresse/Daten 1
4	CAD3	Mpx-Adresse/Daten 3
5	CAD5	Mpx-Adresse/Daten 5
6	CAD7	Mpx-Adresse/Daten 7
7	CCBE0#	Befehl/Byte möglich 0
8	CAD9	Mpx-Adresse/Daten 9
9	CAD11	Mpx-Adresse/Daten 11
10	CAD12	Mpx-Adresse/Daten 12
11	CAD14	Mpx-Adresse/Daten 14
12	CCBE1#	Befehl/Byte möglich 1
13	CPAR	CardBus Parity
14	CPERR#	CardBus-Parity-Fehler

Pin	Funktion	Beschreibung
15	CGNT#	CardBus Grant
16	CINT#	CardBus IREQ
17	VCC	Kartenstromversorgung
18	VPP1	Programmierspannung 1
19	CCLK	CardBus-Takt
20	CIRDY#	CardBus-Initiator bereit
21	CCBE2#	Befehl/Byte möglich 2
22	CAD18	Mpx-Adresse/Daten 18
23	CAD20	Mpx-Adresse/Daten 20
24	CAD21	Mpx-Adresse/Daten 21
25	CAD22	Mpx-Adresse/Daten 22
26	CAD23	Mpx-Adresse/Daten 23
27	CAD24	Mpx-Adresse/Daten 24
28	CAD25	Mpx-Adresse/Daten 25
29	CAD26	Mpx-Adresse/Daten 26
30	CAD27	Mpx-Adresse/Daten 27
31	CAD29	Mpx-Adresse/Daten 29
32	RFU	Reserviert
33	CCLKRUN#	CardBus Takt starten
34	GND	Masse
35	GND	Masse
36	CCD1#	Kartenerkennung 1
37	CAD2	Mpx-Adresse/Daten 2
38	CAD4	Mpx-Adresse/Daten 4
39	CAD6	Mpx-Adresse/Daten 6
40	RFU	Reserviert
41	CAD8	Mpx-Adresse/Daten 8
42	CAD10	Mpx-Adresse/Daten 10
43	CVS1	Spannungserkennung 1
44	CAD13	Mpx-Adresse/Daten 13
45	CAD15	Mpx-Adresse/Daten 15
46	CAD16	Mpx-Adresse/Daten 16

Pin	Funktion	Beschreibung
47	RFU	Reserviert
48	CBLOCK#	CardBus gesperrt
49	CSTOP#	CardBus-Stop
50	CDEVSEL#	CardBus-Gerätewahl
51	VCC	Kartenstromversorgung
52	VPP2	Programmierspannung 2
53	CTRDY#	CardBus-Ziel bereit
54	CFRAME#	CardBus Cycle Frame
55	CAD17	Mpx-Adresse/Daten 17
56	CAD19	Mpx-Adresse/Daten 19
57	CVS2	Spannungserkennung 2
58	CRST#	CardBus zurücksetzen
59	CSERR#	CardBus-Systemfehler
60	CREQ#	CardBus-Anfrage
61	CCBE3#	Befehl/Byte möglich 3
62	CAUDIO	CardBus-Audio
63	CSTSCHG	CardBus-Statusänderung
64	CAD28	Mpx-Adresse/Daten 28
65	CAD30	Mpx-Adresse/Daten 30
66	CAD31	Mpx-Adresse/Daten 31
67	CCD2#	Kartenerkennung 2
68	GND	Masse

3.4 bintec R3000

3.4.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel

- Serielles Anschlusskabel
- 2 DSL-Kabel (für Annex A und für Annex B)
- Steckernetzteil
- **bintec Companion CD**
- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.4.2 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
Produktname	bintec R3000
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	18 (1x Power, 1x Status, 5x2 Ethernet, 3x2 Funktion)

Eigenschaft	Wert
Leistungsaufnahme Gerät	max. 15 Watt, typ. 13 Watt
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
ADSL-Schnittstelle	Internes ADSL-Modem für Annex A und Annex B.
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0 (2)	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
ADSL-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG

Eigenschaft	Wert
	CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)

3.4.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

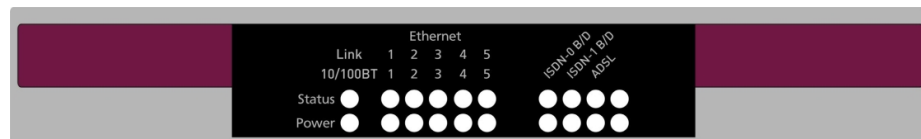


Abb. 25: LEDs von **bintec R3000**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.

LED	Status	Information
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ISDN-1 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-1 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ADSL obere Reihe	blinkend	Das Gerät synchronisiert sich mit dem DSLAM des ADSL-Providers.
	an	Das Gerät hat sich erfolgreich mit dem DSLAM des ADSL-Providers synchronisiert.
ADSL untere Reihe	blinkend	Datenverkehr über die ADSL-Schnittstelle.

LED	Status	Information
	synchron blinkend	ADSL Handshake.
	asynchron blinkend	ADSL Systemfehler.

3.4.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R3000** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle, zwei ISDN-Schnittstellen sowie über eine ADSL-Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

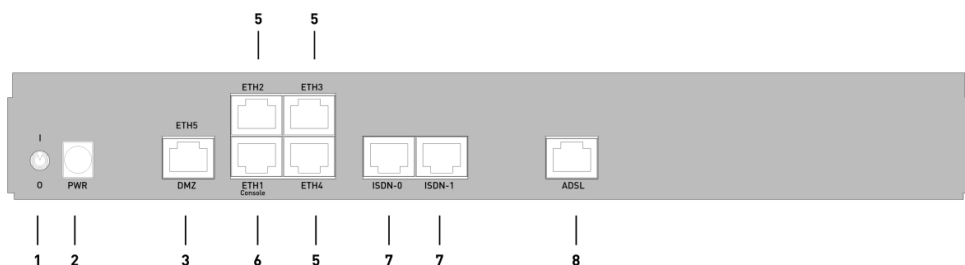


Abb. 26: **bintec R3000** Rückseite

bintec R3000 Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
8	ADSL	ADSL-Schnittstelle

3.4.5 Pin-Belegungen

3.4.5.1 Ethernet-Schnittstelle

bintec R3000 verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

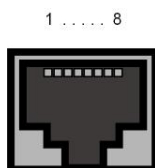


Abb. 27: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)

Pin	Funktion
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.4.5.2 ADSL-Schnittstelle

Die ADSL-Schnittstelle wird mittels eines RJ45-Steckers angebunden. Das eine mitgelieferte Kabel verbindet den RJ45-Stecker, der für das Gerät benötigt wird, mit einem RJ45-Stecker, der für Annex A vorgesehen ist. Das zweite mitgelieferte Kabel verbindet den RJ45-Stecker mit einem RJ45-Stecker für Annex B.

Folgende Pins werden für die ADSL-Verbindung verwendet:

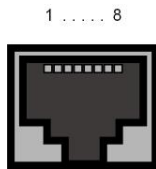


Abb. 28: ADSLSchnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ADSL-Anschluss

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

3.4.5.3 ISDN-So-Schnittstelle

bintec R3000 verfügt über zwei zusätzliche ISDN-So-Schnittstellen, die z. B. für Backup-Funktionen genutzt werden können.

Der Anschluss erfolgt über eine RJ45-Buchse:

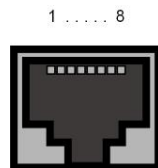


Abb. 29: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.5 bintec R3000w

3.5.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - 2 DSL-Kabel (für Annex A und für Annex B)
 - Steckernetzteil
- Antennen:

- zwei Standardantennen
- **bintec Companion CD**
- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.5.2 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
Produktname	bintec R3000w
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm + 8 mm (Antennenbuchse)
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 4x2 Funktion)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 13 Watt

Eigenschaft	Wert
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
ADSL-Schnittstelle	Internes ADSL-Modem für Annex A und Annex B.
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0 (2)	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
WLAN-Schnittstelle (Antennen)	802.11b, 802.11g und 802.11a mit Antenna Diversity. Datenraten von 1-, 2-, 5.5-, 6-, 9-, 11-, 12-, 18-, 24-, 36-, 48-, 54 MBit/s
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
ADSL-Schnittstelle	RJ45-Buchse

Eigenschaft	Wert
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)



Hinweis

Antenna Diversity

Die beiden Antennen sind nicht gleichberechtigt. Eine wird sowohl zum Senden und Empfangen verwendet (als "Main", "Primary" oder "1" gekennzeichnet; die Antenne neben dem Power-Schalter), die zweite nur zum Empfangen. Während des Empfangs prüft der AP (Access Point), auf welcher Antenne ein besseres Signal ankommt, dieses wird dann zur Dekodierung verwendet.

3.5.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

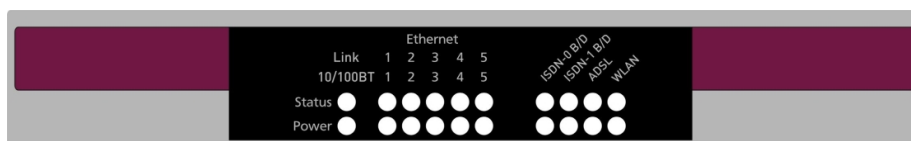


Abb. 30: LEDs von **bintec R3000w**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ISDN-1 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.

LED	Status	Information
ISDN-1 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ADSL obere Reihe	blinkend	Das Gerät synchronisiert sich mit dem DSLAM des ADSL-Providers.
	an	Das Gerät hat sich erfolgreich mit dem DSLAM des ADSL-Providers synchronisiert.
ADSL untere Reihe	blinkend	Datenverkehr über die ADSL-Schnittstelle.
	synchron blinkend	ADSL Handshake.
	asynchron blinkend	ADSL Systemfehler.
WLAN obere Reihe	blinkend	Datenverkehr über die WLAN-Schnittstelle.
WLAN untere Reihe	langsam blinkend	Das WLAN-Modul ist aktiv.
	an	Mindestens ein WLAN-Client ist verbunden.

3.5.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R3000w** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle, zwei ISDN-Schnittstellen sowie über eine ADSL-Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

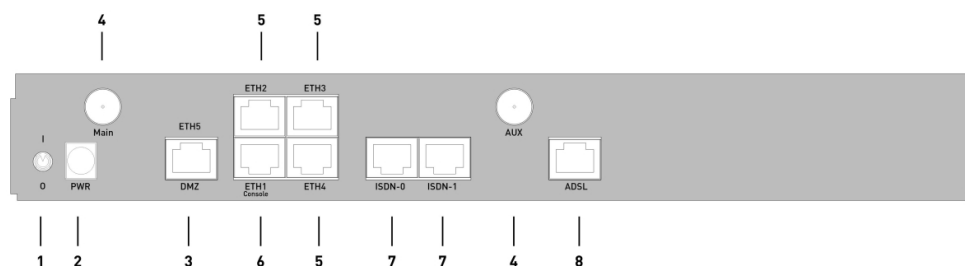


Abb. 31: bintec R3000w Rückseite

bintec R3000w Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
4	Main und AUX	RSMA-Anschluss
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
8	ADSL	ADSL-Schnittstelle

3.5.5 Pin-Belegungen

3.5.5.1 Ethernet-Schnittstelle

bintec R3000w verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

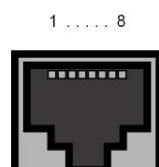


Abb. 32: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.5.5.2 ADSL-Schnittstelle

Die ADSL-Schnittstelle wird mittels eines RJ45-Steckers angebunden. Das eine mitgelieferte Kabel verbindet den RJ45-Stecker, der für das Gerät benötigt wird, mit einem RJ45-Stecker, der für Annex A vorgesehen ist. Das zweite mitgelieferte Kabel verbindet den RJ45-Stecker mit einem RJ45-Stecker für Annex B.

Folgende Pins werden für die ADSL-Verbindung verwendet:

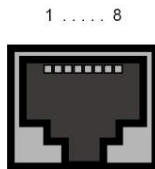


Abb. 33: ADSLSchnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ADSL-Anschluss

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

3.5.5.3 ISDN-So-Schnittstelle

bintec R3000w verfügt über zwei zusätzliche ISDN-So-Schnittstellen, die z. B. für Backup-Funktionen genutzt werden können.

Der Anschluss erfolgt über eine RJ45-Buchse:

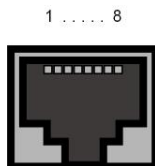


Abb. 34: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.6 bintec R3400

3.6.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - DSL-Kabel
 - Steckernetzteil
- **bintec Companion CD**
- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.6.2 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
Produktname	bintec R3400
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	18 (1x Power, 1x Status, 5x2 Ethernet, 3x2 Funktion)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 10 Watt
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung

Eigenschaft	Wert
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
SHDSL-Schnittstelle	Internes SHDSL-4-Draht-Modem für Annex A und Annex B. Bonding-Technologie mit 2-/4-Draht auch als inverser Multiplexer - realisiert über IMA gemäß ATM-Forum.
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
SHDSL-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte	Kurzanleitung

Eigenschaft	Wert
Dokumentation	
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)

3.6.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

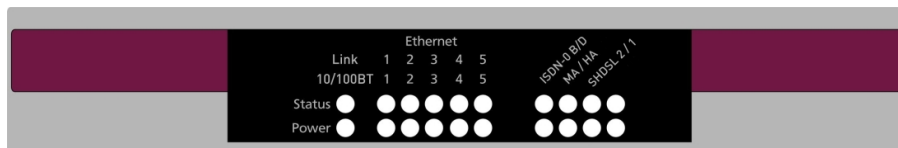


Abb. 35: LEDs von **bintec R3400**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.

LED	Status	Information
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
MA / HA obere Reihe	blinkend	BRRP-Pakete werden empfangen.
MA / HA untere Reihe	an	Ein Benutzer ist auf dem System eingeloggt (z. B. über Telnet).
SHDSL-2/1 obere Reihe	an	Das Draht-Paar 4-5 der SHDSL-Leitung hat sich erfolgreich mit dem DSLAM des SHDSL-Providers synchronisiert.
	blinkend	Datenverkehr über das SHDSL-Draht-Paar 4-5.
SHDSL-2/1 obere Reihe	an	Das Draht-Paar 7-8 der SHDSL-Leitung hat sich erfolgreich mit dem DSLAM des SHDSL-Providers synchronisiert.
	blinkend	Datenverkehr über das SHDSL-Draht-Paar 7-8.

3.6.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R3400** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle, eine ISDN-Schnittstelle sowie über eine SHDSL-Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

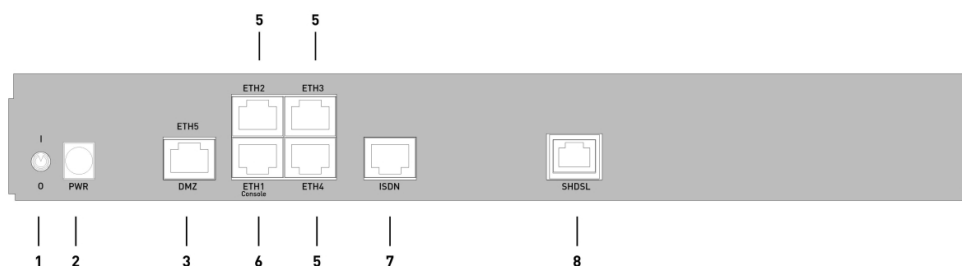


Abb. 36: **bintec R3400 Rückseite**

bintec R3400 Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN	ISDN-Schnittstelle
8	SHDSL	SHDSL-Schnittstelle

3.6.5 Pin-Belegungen

3.6.5.1 Ethernet-Schnittstelle

bintec R3400 verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

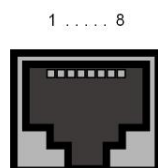


Abb. 37: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.6.5.2 SHDSL-Schnittstelle

Die SHDSL-Schnittstelle wird mittels eines RJ45-Steckers angebunden. Das mitgelieferte Kabel verbindet den RJ45-Stecker, der für das Gerät benötigt wird, mit einem RJ45-Stecker, der für den SHDSL-Anschluss benötigt wird.

Folgende Pins werden für die SHDSL-Verbindung verwendet:

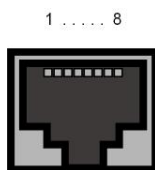


Abb. 38: SHDSL-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für SHDSL-Anschluss

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt
3	Nicht genutzt
4	Leitung a1
5	Leitung b1
6	Nicht genutzt
7	Leitung a2
8	Leitung b2

3.6.5.3 ISDN-So-Schnittstelle

bintec R3400 verfügt über eine zusätzliche ISDN-So-Schnittstelle, die z. B. für Backup-Funktionen genutzt werden kann.

Der Anschluss erfolgt über eine RJ45-Buchse:

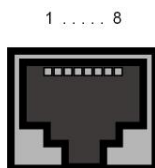


Abb. 39: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

Pin	Funktion
1	Nicht genutzt
2	Nicht genutzt

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

3.7 bintec R3800

3.7.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- **Kabelsätze/Netzteil:**
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - DSL-Kabel
 - Splitter (Y-Adapter)
 - Steckernetzteil
- **bintec Companion CD**
- **Dokumentation:**
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.7.2 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
Produktname	bintec R3800
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 4x2 Funktion)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 12 Watt
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	

Eigenschaft	Wert
SHDSL-Schnittstelle	Internes SHDSL-8-Draht-Modem für Annex A und Annex B. Bonding-Technologie mit 2-/4-/6-/8-Draht auch als inverser Multiplexer - realisiert über IMA gemäß ATM-Forum.
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
Vorhandene Buchsen :	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
SHDSL-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.)

Eigenschaft	Wert
	Software Reference (engl.)

3.7.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

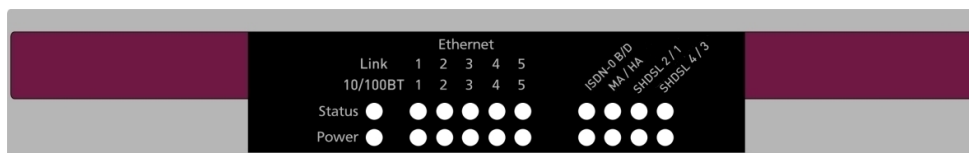


Abb. 40: LEDs von **bintec R3800**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.

LED	Status	Information
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
MA / HA obere Reihe	blinkend	BRRP-Pakete werden empfangen.
MA / HA untere Reihe	an	Ein Benutzer ist auf dem System eingeloggt (z. B. über Telnet).
SHDSL-2/1 obere Reihe	an	Das Draht-Paar 4-5 der SHDSL-Leitung hat sich erfolgreich mit dem DSLAM des SHDSL-Providers synchronisiert.
	blinkend	Datenverkehr über das SHDSL-Draht-Paar 4-5.
SHDSL-2/1 obere Reihe	an	Das Draht-Paar 7-8 der SHDSL-Leitung hat sich erfolgreich mit dem DSLAM des SHDSL-Providers synchronisiert.
	blinkend	Datenverkehr über das SHDSL-Draht-Paar 7-8.
SHDSL-4/3 obere Reihe	an	Das Draht-Paar 3-6 der SHDSL-Leitung hat sich erfolgreich mit dem DSLAM des SHDSL-Providers synchronisiert.
	blinkend	Datenverkehr über das SHDSL-Draht-Paar 3-6.
SHDSL-4/3 obere Reihe	an	Das Draht-Paar 1-2 der SHDSL-Leitung hat sich erfolgreich mit dem DSLAM des SHDSL-Providers synchronisiert.
	blinkend	Datenverkehr über das SHDSL-Draht-Paar 1-2.

3.7.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R3800** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle, eine ISDN-Schnittstellen sowie über eine SHDSL-Schnittstelle.

Die Anschlüsse sind folgendermaßen angeordnet:

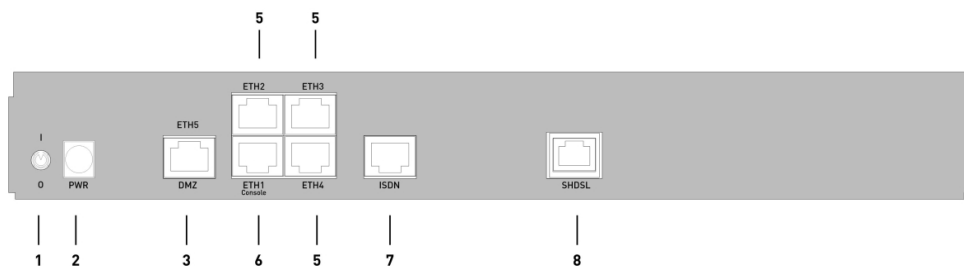


Abb. 41: **bintec R3800** Rückseite

bintec R3800 Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN	ISDN-Schnittstelle
8	SHDSL	SHDSL-Schnittstelle

3.7.5 Pin-Belegungen

3.7.5.1 Ethernet-Schnittstelle

bintec R3800 verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

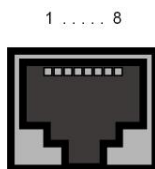


Abb. 42: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.7.5.2 SHDSL-Schnittstelle

Die SHDSL-Schnittstelle wird mittels eines RJ45-Steckers angebunden. Das mitgelieferte Kabel verbindet den RJ45-Stecker, der für das Gerät benötigt wird, mit einem RJ45-Stecker, der für den SHDSL-Anschluss benötigt wird.

Folgende Pins werden für die SHDSL-Verbindung verwendet:

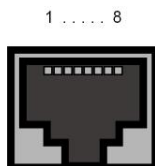


Abb. 43: SHDSL-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für SHDSL-Anschluss

Pin	Funktion
1	Leitung a4
2	Leitung b4
3	Leitung a3
4	Leitung a1
5	Leitung b1
6	Leitung b3
7	Leitung a2
8	Leitung b2

3.7.5.3 ISDN-So-Schnittstelle

bintec R3800 verfügt über eine zusätzliche ISDN-So-Schnittstelle, die z. B. für Backup-Funktionen genutzt werden kann.

Der Anschluss erfolgt über eine RJ45-Buchse:

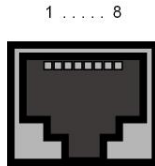


Abb. 44: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.8 bintec R4100

3.8.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - Splitter (Y-Adapter) seriell/Ethernet
 - Steckernetzteil
- **bintec Companion CD**
- Dokumentation:

- **Kurzanleitung** (gedruckt)
- **Benutzerhandbuch** (auf CD)
- **Release Notes**, falls erforderlich
- **Sicherheitshinweise**

3.8.2 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
Produktname	bintec R4100
Maße und Gewicht:	
Gerätemaße ohne Kabel (B x H x T)	295 mm x 45 mm x 160 mm
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 4x2 Funktion)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 10 Watt
Spannungsversorgung	24 V DC 1 A EU PSU
Umweltanforderungen:	

Eigenschaft	Wert
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0 (2)	Fest eingebaut
ISDN-PRI (2)	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
ISDN-PRI-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec

Eigenschaft	Wert
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)

3.8.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

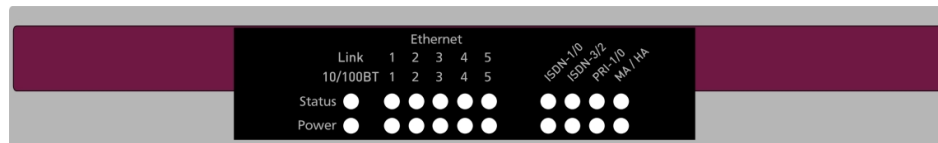


Abb. 45: LEDs von **bintec R4100**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.

LED	Status	Information
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-1/0 obere Reihe	an	ISDN-0: ISDN D-Kanal ist aktiv.
	blinkend	ISDN-0: Mindestens ein ISDN B-Kanal ist aktiv.
ISDN-1/0 untere Reihe	an	ISDN-1: ISDN D-Kanal ist aktiv.
	blinkend	ISDN-1: Mindestens ein ISDN B-Kanal ist aktiv.
ISDN-3/2 obere Reihe	an	ISDN-2: ISDN D-Kanal ist aktiv.
	blinkend	ISDN-2: Mindestens ein ISDN B-Kanal ist aktiv.
ISDN-3/2 untere Reihe	an	ISDN-3: ISDN D-Kanal ist aktiv.
	blinkend	ISDN-3: Mindestens ein ISDN B-Kanal ist aktiv.
PRI 1/0 obere Reihe	an	PRI-0: ISDN D-Kanal ist aktiv.
	blinkend	PRI-0: Mindestens ein ISDN B-Kanal ist aktiv.
PRI 1/0 untere Reihe	an	PRI-1: ISDN D-Kanal ist aktiv.
	blinkend	PRI-1: Mindestens ein ISDN B-Kanal ist aktiv.

LED	Status	Information
MA / HA obere Reihe	blinkend	BRRP-Pakete werden empfangen.
MA / HA untere Reihe	an	Ein Benutzer ist auf dem System eingeloggt (z. B. über Telnet).

3.8.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R4100** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle, vier ISDN-Schnittstellen sowie über zwei ISDN-PRI-Schnittstellen.

Die Anschlüsse sind folgendermaßen angeordnet:

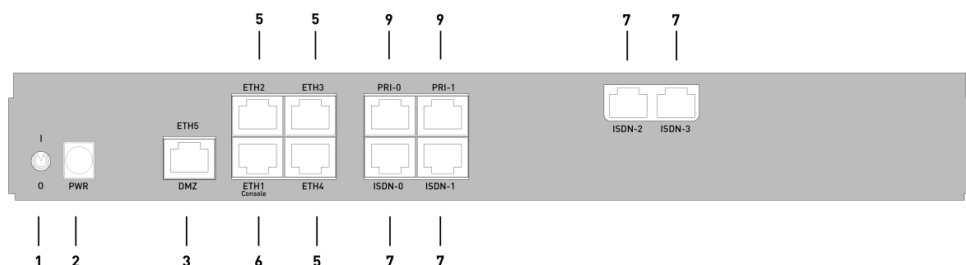


Abb. 46: **bintec R4100** Rückseite

bintec R4100 Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-3	ISDN-Schnittstelle
9	PRI-0 - PRI-1	ISDN-PRI-Schnittstelle

3.8.5 Pin-Belegungen

3.8.5.1 Ethernet-Schnittstelle

bintec R4100 verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

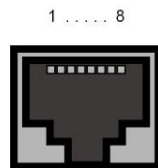


Abb. 47: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)

Pin	Funktion
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.8.5.2 ISDN-So-Schnittstelle

bintec R4100 verfügt über eine zusätzliche ISDN-So-Schnittstelle, die z. B. für Backup-Funktionen genutzt werden kann.

Der Anschluss erfolgt über eine RJ45-Buchse:

1 8

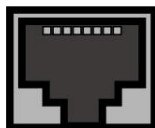


Abb. 48: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.8.5.3 ISDN-PRI-Schnittstelle

Die beiden ISDN-PRI-Schnittstellen werden mittels RJ45-Steckers angebunden. Das mitgelieferte Kabel verbindet den RJ45-Stecker, der für das Gerät benötigt wird, mit einem RJ45-Stecker, der für den PRI-Anschluss benötigt wird.

Folgende Pins werden für die Verbindung verwendet:

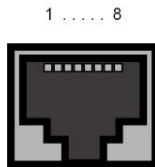


Abb. 49: ISDN-PRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-PRI-Anschluss

Pin	Funktion
1	T +
2	T -
3	Nicht genutzt
4	R +
5	R -
6	Nicht genutzt
7	Nicht genutzt
8	Nicht genutzt

Hinweis für NTs in Deutschland



Hinweis

In Deutschland wird "Senden" (NT-->TE) oft mit "S2Mab" (a und b) auf dem Anschlussstecker benannt, "Empfangen (TE-->NT) mit "S2Man" (a und b).

3.9 bintec R4300

3.9.1 Lieferumfang

Ihr Gerät wird zusammen mit folgenden Teilen ausgeliefert:

- Kabelsätze/Netzteil:
 - Ethernet-Kabel
 - ISDN-Kabel
 - Serielles Anschlusskabel
 - Steckernetzteil
 - X.21 DTE (optional erhältlich)
 - X.21 DCE (optional erhältlich)
 - V.35 DTE (optional erhältlich)
- **bintec Companion CD**
- Dokumentation:
 - **Kurzanleitung** (gedruckt)
 - **Benutzerhandbuch** (auf CD)
 - **Release Notes**, falls erforderlich
 - **Sicherheitshinweise**

3.9.2 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
Produktname	bintec R4300
Maße und Gewicht:	
Gerätemaße ohne Kabel	295 mm x 45 mm x 160 mm

Eigenschaft	Wert
(B x H x T)	
Gewicht	ca. 1260 g
Transportgewicht (inkl. Dokumentation, Kabel, Verpackung)	ca. 2,6 kg
Speicher	32 MB SDRAM, 8 MB Flash-ROM
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 4x2 Funktion)
Leistungsaufnahme Gerät	max. 15 Watt, typ. 13 Watt
Spannungsversorgung	15 V AC 1.3 A EU PSU
Umweltanforderungen:	
Lagertemperatur	-20° bis +70 °C
Betriebstemperatur	0° bis 40 °C
Relative Luftfeuchtigkeit	10 % bis 90 % nichtkondensierend im Betrieb, 5 % bis 95 % nichtkondensierend bei Lagerung
Raumklassifizierung	Nur in trockenen Räumen betreiben.
Verfügbare Schnittstellen:	
Ethernet IEEE 802.3 LAN (4-Port-Switch), ein Port mit serieller Schnittstellenfunktion	Fest eingebaut (nur twisted-pair), 10/100 MBit/s, autosensing, MDIX; unterstützt die Baudraten: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 Baud
ISDN-WAN S0 (2)	Fest eingebaut
DMZ/ETH5	Zusätzlicher Ethernet Switch-Port

Eigenschaft	Wert
X.21-Schnittstelle (2)	Fest eingebaut
Vorhandene Buchsen:	
Serielle Schnittstelle V.24	RJ45-Buchse
Ethernet-Schnittstelle	RJ45-Buchse
ISDN-Schnittstelle	RJ45-Buchse
X.21-Schnittstelle	RJ45-Buchse
Richtlinien & Normen	R&TTE-Richtlinie 1999/5/EG CE-Zeichen für alle EU-Länder
SAFERNET™ Security Technology	Community Passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN mit PPTP oder IPSec
Mitgelieferte Software	BRICKware for Windows BRICKtools for Unix
Mitgelieferte gedruckte Dokumentation	Kurzanleitung
Online-Dokumentation	Benutzerhandbuch BRICKware for Windows (engl.) Software Reference (engl.)

3.9.3 LEDs

Die LEDs Ihres Geräts geben Aufschluss über bestimmte Aktivitäten und Zustände des Geräts.

Die sind folgendermaßen angeordnet:

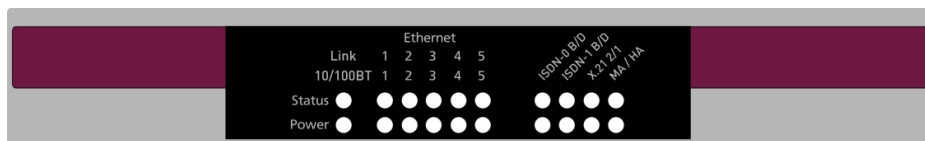


Abb. 50: LEDs von **bintec R4300**

Im Betriebsmodus zeigen die LEDs folgende Statusinformationen Ihres Geräts an:

LED Statusanzeige

LED	Status	Information
Power	an	Stromversorgung ist angeschlossen.
Status	permanent an oder aus	Fehler.
	blinkend	Das Gerät ist aktiv.
ETH 1 bis 5 obere Reihe	an	Das Gerät ist an das Ethernet angeschlossen.
	blinkend	Datenverkehr über die Ethernet-Schnittstelle.
ETH 1 bis 5 untere Reihe	an	Datenverkehr mit 100Mbit/s.
	aus	Datenverkehr mit 10Mbit/s.
ISDN-0 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.
ISDN-0 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
ISDN-1 B/D obere Reihe	an	ISDN D-Kanal ist aktiv.

LED	Status	Information
ISDN-1 B/D untere Reihe	an	Ein ISDN B-Kanal ist aktiv.
	blinkend	Beide ISDN B-Kanäle sind aktiv.
X.21 2/1 obere Reihe	an	X.21 1: Verbindung ist aufgebaut.
	blinkend	X.21 1: Datenverkehr.
X.21 2/1 untere Reihe	an	X.21 2: Verbindung ist aufgebaut.
	blinkend	X.21 2: Datenverkehr.
MA / HA obere Reihe	blinkend	BRRP-Pakete werden empfangen.
MA / HA untere Reihe	an	Ein Benutzer ist auf dem System eingeloggt (z. B. über Telnet).

3.9.4 Anschlüsse

Alle Anschlüsse befinden sich auf der Rückseite des Geräts. **bintec R4300** verfügt über einen 4-Port Ethernet Switch inklusive eines Ports mit serieller Schnittstellenfunktion, einer DMZ/ETH5-Schnittstelle, zwei ISDN-Schnittstellen sowie über zwei X.21-Schnittstellen.

Die Anschlüsse sind folgendermaßen angeordnet:

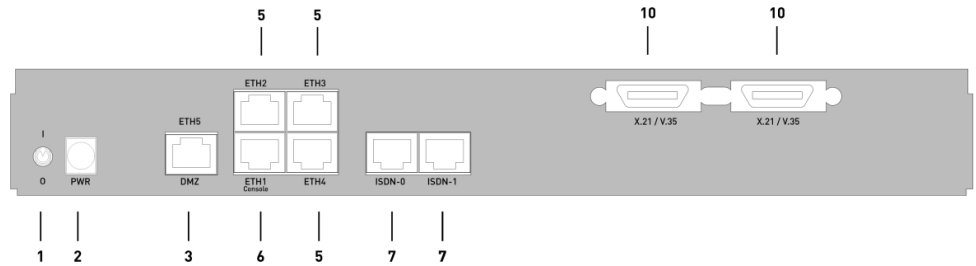


Abb. 51: **bintec R4300 Rückseite**

bintec R4300 Rückseite

1	I/O	Netzschalter
2	PWR	Buchse für Steckernetzteil
3	DMZ/ETH5	Ethernet-Schnittstelle
5	ETH2 - ETH4	Ethernet-Schnittstelle
6	ETH1 / Console	Ethernet-Schnittstelle mit serieller Schnittstellenfunktion
7	ISDN-0 - ISDN-1	ISDN-Schnittstelle
10	X.21/V.35	X.21-Schnittstelle

3.9.5 Pin-Belegungen

3.9.5.1 Ethernet-Schnittstelle

bintec R4300 verfügt über eine Ethernet-Schnittstelle mit integriertem 4-Port Switch (ETH1 - ETH4) und eine separate Ethernet-Schnittstelle (DMZ/ETH5).

Der 4-Port Switch dient zur Anbindung einzelner PCs oder weiterer Switches. Die Schnittstelle *ETH1/Console* kann auch als serielle Schnittstelle genutzt werden. Die DMZ/ETH5-Schnittstelle dient zur Anbindung eines optionalen DSL-Modems oder einer DMZ.

Der Anschluss erfolgt über eine RJ45-Buchse.

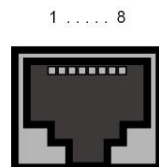


Abb. 52: Ethernet-10/100Base-T-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für Ethernet-Anschluss

Pin	Funktion
1	TD +
2	TD -
3	RD +
4	Nicht genutzt
5	Nicht genutzt
6	RD -
7	Nicht genutzt
8	Nicht genutzt

Die Ethernet 10/100 BASE-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

Die Pin-Zuordnung für die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle (RJ45-Buchse) ist wie folgt:

RJ45-Buchse für Ethernet-Anschluss bzw. serielle Schnittstelle (Console)

Pin	Funktion
1	TD + (Ethernet)
2	TD - (Ethernet)
3	RD + (Ethernet)
4	RX (Console)
5	GND (Console)
6	RD - (Ethernet)
7	GND (Console)
8	TX (Console)

Die kombinierte Serielle-Ethernet10/100Base-T-Schnittstelle besitzt keine Auto-MDI-X Funktion.

3.9.5.2 ISDN-So-Schnittstelle

bintec R4300 verfügt über zwei zusätzliche ISDN-So-Schnittstellen, die z. B. für Backup-Funktionen genutzt werden können.

Der Anschluss erfolgt über eine RJ45-Buchse:

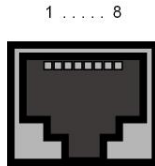


Abb. 53: ISDN-So-BRI-Schnittstelle (RJ45-Buchse)

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

RJ45-Buchse für ISDN-Anschluss

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

3.9.5.3 X.21-Schnittstelle

bintec R4300 verfügt über zwei X.21-Schnittstellen

Der Anschluss erfolgt über eine 26-polige Mini-Delta-Ribbon-Buchse:

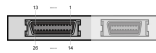


Abb. 54: X.21-Schnittstelle (26-polige Mini-Delta-Ribbon-Buchse)

Die Pins der 26-poligen Mini-Delta-Ribbon-Buchse sind folgendermaßen belegt:

Pinbelegung der 26-poligen Mini-Delta-Ribbon-Buchse

Signal	Pin-Nr.	X.21	X.21	V.35	V.35	V.36	V.36
		(DB-15)	(DB-15)	(M34)	(M34)	(DB-37)	(DB-37)
		DTE	DCE	DTE	DCE	DTE	DCE
Schirm	A1 (1)	1	1	A	A	1	1
GND	A2 (2)	8	8	B	B	19	19
TxD (B)	A3 (3)	9	11	S	T	22	24

Signal	Pin-Nr.	X.21 (DB-15)	X.21 (DB-15)	V.35 (M34)	V.35 (M34)	V.36 (DB-37)	V.36 (DB-37)
		DTE	DCE	DTE	DCE	DTE	DCE
TxD (A)	A4 (4)	2	4	P	R	4	6
RxD (B)	A5 (5)	11	9	T	S	24	22
RxD (A)	A6 (6)	4	2	R	P	6	4
RTS (B)	A7 (7)	10	12			25	27
RTS (A)	A(8)	3	5	C	D	7	9
CBS (B)	A9 (9)	12	10			27	25
CBS (A)	A10 (10)	5	3	D	C	9	7
RxC (B)	A11 (11)	13	14	X	W	26	35
RxC (A)	A12 (12)	6	7	V	U	8	17
Mode DCE	A13 (13)		8		B		19
Mode 0	B1 (14)					19	19
DTR (B)	B2 (15)					30	29
DTR (A)	B3 (16)			H	E	12	11
DCD (B)	B4 (17)					31	31
DCD (A)	B5 (18)			F	F	13	13
DSR (B)	B6 (19)					29	30
DSR (A)	B7 (20)			E	H	11	12
TxC (B)	B8 (21)			AA	AA	23	23
TxC (A)	B9 (22)			Y	Y	5	5
Mode 1	B10 (23)						
Mode 2	B11 (24)	8	8				
TxCE (B)	B12 (25)		13	W	X	35	26
TxCE (A)	B13 (26)		6	U	V	36	8

Kapitel 4 Zugang und Konfiguration

Im diesem Kapitel werden alle Zugangs- und Konfigurationsmöglichkeiten beschrieben.

4.1 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
- Über eine ISDN-Verbindung

4.1.1 Zugang über LAN

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

4.1.1.1 HTTP/HTTPS

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

- `http://192.168.0.254`

oder

`https://192.168.0.254`

4.1.1.2 Telnet

Abgesehen von der Konfiguration über einen Web-Browser können Sie mit einer Telnet-Verbindung auf die SNMP-Shell zugreifen und weitere Konfigurationsmöglichkeiten nutzen. Diese sind in *Konfigurationsmöglichkeiten* auf Seite 108 beschrieben.

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 107.

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 107.

4.1.1.3 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 106).
- (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 **Funkwerk Configuration Interface** auf und melden Sie sich an Ihrem Gerät an (siehe [Das Funkwerk Configuration Interface aufrufen](#) auf Seite 110).
- (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 106 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 106 fort.



Hinweis

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

4.1.2 Zugang über die serielle Schnittstelle

Jedes **bintec** Gateway 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 (192.168.0.254/255.255.255.0) nicht möglich ist.

Windows

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 Win-

dows-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.

Wenn Sie die **BRICKware** unter www.funkwerk-ec.com abgerufen und installiert haben, stehen Ihnen im Windows-Startmenü zwei Verknüpfungen zur Verfügung. Wenn Sie diese verwenden, müssen Sie für die serielle Verbindung zu Ihrem Gerät keine weiteren Einstellungen vornehmen.

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

- (1) Klicken Sie im Windows-Startmenü auf **Programme -> BRICKware -> Gerät an COM1** (bzw. **Gerät an COM2**, wenn Sie die COM2-Schnittstelle des Rechners benutzen), um HyperTerminal zu starten.
- (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*
 - Flusssteuerung: *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`

4.1.3 Zugang über ISDN

Alle Geräte, die über eine ISDN-Schnittstelle verfügen, können von einem anderen Gerät aus mittels eines ISDN-Rufs erreicht und konfiguriert werden.

Der Zugang über ISDN mit ISDN-Login empfiehlt sich vor allem dann, wenn Ihr Gerät aus der Ferne konfiguriert oder gewartet werden soll. Dies ist auch dann möglich, wenn Ihr Gerät sich noch im Auslieferungszustand befindet. Der Zugang erfolgt dann mit Hilfe eines bereits konfigurierten Geräts oder eines Rechners mit ISDN-Karte im Remote-LAN. Das zu konfigurierende Gerät im eigenen LAN wird über eine Rufnummer des ISDN-Anschlusses (z. B. 1234) erreicht. So kann z. B. der Administrator im Remote-LAN Ihr Gerät konfigurieren, ohne vor Ort zu sein.



Hinweis

Wenn Sie ein unkonfiguriertes Gerät parallel zu einer Telefonanlage an einen ISDN-Anschluss anschließen, kann die Telefonanlage solange keine Rufe annehmen, bis auf dem Gerät eine ISDN-Nummer konfiguriert ist.

Der Zugang über ISDN verursacht Kosten. Wenn Ihr Gerät und Ihr Rechner im gleichen LAN sind, ist es günstiger, auf Ihr Gerät über das LAN oder über die serielle Schnittstelle zuzugreifen.

Ihr Gerät in Ihrem LAN muss lediglich mit dem ISDN-Anschluss verbunden und eingeschaltet sein.

Gehen Sie folgendermaßen vor, um Ihr Gerät über ISDN-Login zu erreichen:

- (1) Schließen Sie Ihr Gerät an das ISDN an.
- (2) Loggen Sie sich wie gewohnt als Administrator auf dem Gerät im Remote-LAN ein.

- (3) Geben Sie in der SNMP-Shell `isdnlogin <Rufnummer des ISDN-Anschlusses Ihres Geräts>` ein, z. B. `isdnlogin 1234`.
- (4) Es erscheint der Login-Prompt. Sie befinden sich auf der SNMP-Shell Ihres Geräts.

Fahren Sie fort mit [Anmelden zur Konfiguration](#) auf Seite 107.

4.2 Anmelden

Mittels 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.

4.2.1 Benutzernamen und Passwörter im Auslieferungszustand

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

Benutzernamen und Passwörter im Auslieferungszustand

Benutzername	Passwort	Befugnisse
<code>admin</code>	<code>funkwerk</code>	Systemvariablen lesen und ändern, Konfigurationen speichern; Funkwerk Configuration Interface benutzen.
<code>write</code>	<code>public</code>	Systemvariablen (außer Passwörter) lesen und schreiben (Änderungen gehen bei Ausschalten Ihres Geräts verloren).
<code>read</code>	<code>public</code>	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 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 **bintec**-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 *Passwörter* auf Seite 132 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!

4.2.2 Anmelden zur Konfiguration

Stellen Sie eine Verbindung mit dem Gerät her. Die Zugangsmöglichkeiten sind in *Zugangsmöglichkeiten* auf Seite 100 beschrieben.

Funkwerk Configuration 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 **Funkwerk Configuration Interface**.

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. `funkwerk`, und bestätigen Sie mit der **Eingabetaste**.

Ihr Gerät meldet sich mit dem Eingabeprompt, z. B. `TR200bw:>`. 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**.

4.3 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:

- **Funkwerk Configuration Interface**
- Setup Tool für Experten
- 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	Funkwerk Configuration Interface , 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.

4.3.1 Funkwerk Configuration Interface

Das **Funkwerk Configuration Interface** 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 **Funkwerk Configuration Interface** 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 [Software & Konfiguration](#) auf Seite 498 auf www.funkwerk-ec.com heruntergeladen und auf dem Gerät installiert werden. Gehen Sie hierzu vor wie in beschrieben.

Die Einstellungsänderungen, die Sie mit dem **Funkwerk Configuration Interface** vorneh-

men, 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 **Funkwerk Configuration Interface** können Sie ebenfalls die wichtigsten Funktionsparameter Ihres Geräts überwachen.

The screenshot displays the Funkwerk Configuration Interface for a bintec R1200 device. The interface is in German and includes a navigation menu on the left and a main content area on the right.

Navigation Menu (Left):

- Konfiguration speichern
- Systemverwaltung
 - Status
 - Globale Einstellungen
 - Schnittstellenmodus /
 - Bridge-Gruppen
 - Administrativer Zugriff
 - Remote Authentifizierung
- Physikalische Schnittstellen
 - LAN
 - Wireless LAN
 - Routing
 - WAN
 - VPN
 - Firewall
 - VoIP
 - Lokale Dienste
 - Wartung
 - Externe Berichterstellung
 - Monitoring

Main Content Area (Right):

Automatisches Aktualisierungsintervall: 60 Sekunden **Übernehmen**

Warnung: Systempasswort nicht geändert!

Systeminformationen

Uptime	1 Tag(e) 3 Stunde(n) 42 Minute(n)
Systemdatum	Fr 21 Januar 2005 03:58:00
Seriennummer	R1E180006500018
BOSS-Version	V.7.8 Rev. 2 IPSec from 2008/11/27 00:00:00

Ressourceninformationen

CPU-Nutzung	0%
Arbeitsspeichernutzung	20.3/31.9 MB (64%)
ISDN Verwendung Extern	0 / 4B-Kanäle
Aktive Sitzungen (SIF, RTP, etc...)	0
Aktive IPSec-Tunnel	0 / 0

Physikalische Schnittstelle

Physikalische Schnittstelle	Schnittstellendetails	Link
en1-0	192.168.0.254 / 255.255.255.0	+
en1-4	Nicht konfiguriert / Nicht konfiguriert	+
WLAN1	Aus	+
com0-8	Nicht konfiguriert	+
bri2-0	Nicht konfiguriert	+
com6-0	Konfiguriert	+

Aktuelle Systemprotokolle

Zeit	Level	Subsystem	Nachricht
00:16:03	Informationen	USB	usb6-0-2: Sierra Wireless, Incorporated AirCard, rev 1.10/0.02
00:16:03	Informationen	INET	sshd: pid 56 - listening on 0.0.0.0 port 22.
00:16:03	Fehler	TTY	UMTS Ctl umtsctl_open(): can't open umts device!
00:16:03	Fehler	TTY	Modem answer to <AT+CPIN?> is 'SIM busy'
00:16:02	Informationen	IPSec	init: starting...
00:16:02	Informationen	IPSec	BinTec ipsecd version 3.0 Copyright (c) 1996-2008 by Funkwerk Enterprise Communications GmbH
00:16:02	Informationen	IPSec	init: running
00:16:01	Informationen	Konfiguration	system r1200 started at Thu Jan 20 0:16:01 2005
00:15:59	Fehler	INET	PIM: no valid license found, disabling it.
00:15:58	Informationen	USB	usb6-1-1: HUB with 1 port (1 removable), self-powered

Abb. 55: Funkwerk Configuration Interface Startseite

4.3.1.1 Das Funkwerk Configuration Interface aufrufen

- (1) Überprüfen Sie, ob das Gerät angeschlossen und eingeschaltet ist und alle nötigen Kabel richtig verbunden sind (siehe [Anschlüsse](#) auf Seite 11).
- (2) Überprüfen Sie die Einstellungen des PCs, von dem aus Sie die Konfiguration Ihres Geräts durchführen möchten (siehe [PC einrichten](#) auf Seite 20).
- (3) Öffnen Sie einen Webbrowser.
- (4) Geben Sie `http://192.168.0.254` in das Adressfeld des Webbrowsers ein.
- (5) Geben Sie in das Feld **User** `admin` und in das Feld **Password** `funkwerk` ein und klicken Sie auf **LOGIN**.

Sie befinden sich nun im Statusmenü des **Funkwerk Configuration Interface** Ihres Geräts (siehe [Status](#) auf Seite 126).

4.3.1.2 Bedienelemente

Funkwerk Configuration Interface Fenster

Das **Funkwerk Configuration Interface** Fenster ist in drei Bereiche geteilt:

- Die Kopfleiste
- Die Navigationsleiste
- Das Hauptkonfigurationsfenster

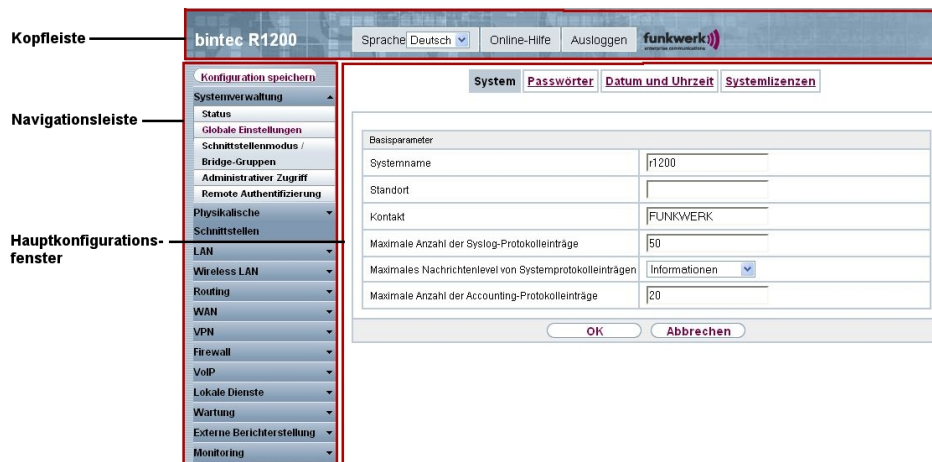




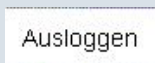
Abb. 56: Bereiche des **Funkwerk Configuration Interface**

Kopfleiste



Abb. 57: Funkwerk Configuration Interface *Kopfleiste*

Funkwerk Configuration Interface Kopfleiste

Menü	Funktion
	<p>Sprachauswahl: Wählen Sie in dem Dropdown-Menü die gewünschte Sprache aus, in der das Funkwerk Configuration Interface angezeigt werden soll. Hier können Sie die Sprache auswählen, in der Sie die Konfiguration durchführen möchten. Zur Auswahl stehen Deutsch und Englisch.</p>
	<p>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.</p>
	<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"> • mit der Konfiguration fortfahren, • die Konfiguration speichern und das Fenster schließen, • die Konfiguration ohne Speichern verlassen.

Navigationsleiste



Abb. 58: Konfiguration speichern Schaltfläche



Abb. 59: Menüs

Über der Navigationsleiste ist die Schaltfläche **Konfiguration speichern** zu finden. Klicken Sie auf die Schaltfläche **Konfiguration speichern**, um alle Konfigurationsänderungen zu speichern, so dass sie beim nächsten Neustart des Geräts als Boot-Konfiguration geladen werden.

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 **Funkwerk Configuration Interface** 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 **Funkwerk Configuration Interface** ausführen können, werden mit Hilfe folgender Schaltflächen ausgelöst:

Funkwerk Configuration Interface Schaltflächen

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

Funkwerk Configuration Interface Schaltflächen für spezielle Funktionen

Schaltfläche	Funktion
Finden	Im Menü Access-Point-Suche starten Sie mit dieser Schaltfläche die automatische Erkennung aller im Netzwerk vorhandener und per Ethernet verbundener Access-Points.
Importieren	Im Menü VPN -> Zertifikate -> Zertifikate und im Menü VPN -> Zertifikate -> CRLs werden mit dieser Schaltfläche die Untermenüs für die Konfiguration des Zertifikate- bzw. CRL-Imports aufgerufen.
Anforderung	Im Menü VPN -> Zertifikate -> Zertifikate wird mit dieser Schaltfläche das Untermenü für die Konfiguration der Zertifikatsanforderung aufgerufen.
Verb. beenden	Im Menü Überwachung -> ISDN/Modem -> Aktuelle Anrufe

Schaltfläche	Funktion
	werden durch Drücken dieser Schaltfläche die in der Spalte  ausgewählten aktiven Rufe beendet.

Verschiedene Symbole weisen auf folgende mögliche Aktionen oder Zustände hin:

Funkwerk Configuration Interface Symbole

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

In der Listenansicht haben Sie folgende Bedienfunktionen zur Auswahl:

Funkwerk Configuration Interface 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 Filter in x <Option> 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>

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

Abb. 60: Konfiguration des Aktualisierungsintervalls



Ansicht pro Seite **<<** **>>** Filter in **Los**

Abb. 61: Liste filtern

Struktur der Funkwerk Configuration Interface Konfigurationsmenüs





Die Menüs des **Funkwerk Configuration Interface** enthalten folgende Grundstrukturen:

Funkwerk Configuration Interface 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 Erweiterte Einstellungen	Klicken Sie auf diesen Reiter, um erweiterte Konfigurationsoptionen anzuzeigen.

Für die Konfiguration stehen folgende Optionen zur Verfügung:

Funkwerk Configuration Interface Konfigurationselemente

Menü	Funktion				
Eingabefelder	z. B. leeres Textfeld  Textfeld mit verdeckter Eingabe  Geben Sie entsprechende Daten ein.				
Radiobuttons	z. B.  Wählen Sie die entsprechende Option aus.				
Checkboxen	z. B. Aktivieren durch Auswahl der Checkbox  Auswahl verschiedener möglicher Optionen <table border="1" data-bbox="644 1487 1315 1567"> <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	z. B.				

Menü	Funktion									
	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; flex-direction: column; gap: 2px;"> <div style="border: 1px solid #ccc; padding: 2px;">Vollständige automatische Aushandlung ▾</div> <div style="border: 1px solid #ccc; padding: 2px;">Vollständige automatische Aushandlung ▾</div> <div style="border: 1px solid #ccc; padding: 2px;">Vollständige automatische Aushandlung ▾</div> <div style="border: 1px solid #ccc; padding: 2px;">Vollständige automatische Aushandlung ▾</div> </div> <p>Klicken Sie auf den Pfeil, um die Liste zu öffnen. Wählen Sie die gewünschte Option mit der Maus.</p> </div>									
Interne Listen	<p>z. B.</p> <div style="border: 1px solid #ccc; padding: 5px; width: fit-content;"> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 2px;">IP-Adresse</td> <td style="width: 50%; padding: 2px;">Netzmaske</td> <td style="width: 20px;"></td> </tr> <tr> <td style="padding: 2px;"><input type="text"/></td> <td style="padding: 2px;">255.255.255.0</td> <td style="text-align: center; padding: 2px;"></td> </tr> <tr> <td colspan="3" style="text-align: center; padding: 5px;">Hinzufügen</td> </tr> </table> </div> <p>Klicken Sie auf die Schaltfläche Hinzufügen. Ein neuer Listeneintrag wird angelegt. Geben Sie die entsprechenden Daten ein. Bleiben die Felder des Listeneintrags leer, wird dieser bei Bestätigen mit OK nicht gespeichert. Löschen Sie Einträge, indem Sie auf das -Symbol klicken.</p>	IP-Adresse	Netzmaske		<input type="text"/>	255.255.255.0		Hinzufügen		
IP-Adresse	Netzmaske									
<input type="text"/>	255.255.255.0									
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 **Funkwerk Configuration Interface** verändern, kann dies Inkonsistenzen oder Fehlfunktionen verursachen. Daher wird empfohlen, die Konfiguration mit dem Setup

Tool fortzuführen.

4.3.1.3 Funkwerk Configuration Interface 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.funkwerk-ec.com.

Das **Funkwerk Configuration Interface** enthält folgende Menüs:

Systemverwaltung

Menü	Funktion
Status	In diesem Menü werden allgemeine Informationen über Ihr Gerät auf einen Blick angezeigt. Hierzu gehören u. a. Seriennummer, Softwareversion, aktuelle Speicher- und Prozessornutzung, Status der physikalischen Schnittstellen und die letzten zehn Systemmeldungen.
Globale Einstellungen	In diesem Menü tragen Sie die grundlegenden Systemeinstellungen Ihres Geräts ein, wie z. B. Systemname, -datum, -uhrzeit und Passwörter. Sie können weiterhin Lizenzen verwalten, die für die Verwendung bestimmter Funktionen notwendig sind.
Schnittstellenmodus / Bridge-Gruppen	In diesem Menü definieren Sie, in welchem Modus die Schnittstellen Ihres Geräts betrieben werden sollen (Routing oder Bridging) und können ggf. Bridge-Gruppen definieren.
Administrativer Zugriff	In diesem Menü konfigurieren Sie die Zugangsmöglichkeiten zu den einzelnen Schnittstellen.
Remote Authentifizierung	In diesem Menü konfigurieren Sie die Authentifizierung über einen RADIUS-Server oder einen TACAS+-Server.

Physikalische Schnittstellen

Menü	Funktion
AUX	In diesem Menü können Sie unterschiedliche Vorgaben für die Kommunikation zwischen Gateway und Modem definieren.
Ethernet-Ports	In diesem Menü konfigurieren Sie die Ethernet-Schnittstellen Ihres Geräts. Hier wählen Sie z. B. die Geschwindigkeit und die Art der Schnittstelle aus.
ISDN-Ports	In diesem Menü konfigurieren Sie die ISDN-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, an welcher Art von ISDN-Anschluss Ihr Gerät angeschlossen ist.
ADSL-Modem	Nur für R3000 und R3000w . In diesem Menü konfigurieren Sie die ADSL-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, ob für den Breitbandanschluss Annex A oder Annex B als ADSL Modus benutzt wird.
SHDSL	Nur für R3400 und R3800w . In diesem Menü konfigurieren Sie die SHDSL-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, wieviele Andernpaare für die SHDSL-Verbindung genutzt werden.
Serielle Ports	Nur für R4300 . In diesem Menü konfigurieren Sie die serielle(n) WAN Schnittstelle(n) Ihres Geräts, d.h. je nach Lizenz eine oder zwei integrierte X.21/V.35-Schnittstellen. Hier tragen Sie z. B. ein, welche Übertragungsrate für die Verbindung genutzt wird.
UMTS	Nur für R1200wu . In diesem Menü konfigurieren Sie die CardBus-Schnittstelle Ihres Geräts. Hier tragen Sie z. B. ein, dass UMTS aktiviert wird.

LAN

Menü	Funktion
IP-Konfiguration	In diesem Menü nehmen Sie die IP-Konfiguration der LAN-Schnittstellen Ihres Geräts vor.
VLAN	In diesem Menü konfigurieren Sie die VLANs.

Wireless LAN (nur bintec R1200w, R1200wu und R3000w)

Menü	Funktion
WLAN1	In diesem Menü konfigurieren Sie Ihr Funkmodul als Access Point oder als Access Client.
Verwaltung	In diesem Menü nehmen Sie grundlegende WLAN-Einstellungen vor.

Routing

Menü	Funktion
Routen	In diesem Menü tragen Sie weitere Routen ein.
NAT	In diesem Menü konfigurieren Sie die NAT-Firewall (NAT, Network Address Translation).
RIP	In diesem Menü konfigurieren Sie die dynamische Aktualisierung der Routing-Tabelle mittels RIP.
Lastverteilung	In diesem Menü konfigurieren Sie applikationsgesteuertes Bandbreitenmanagement.
Multicast	In diesem Menü konfigurieren sie die Verwendung von Multimedia-Streaming-Protokollen für z. B. Voice-over-IP oder Video- und Audio-Streaming (z. B. IPTV oder Webradio) oder das sog. TriplePlay (Voice, Video, Daten).

WAN

Menü	Funktion
Internet + Einwählen	In diesem Menü definieren Sie Internetverbindungen für die verschiedenen Verbindungsprotokolle oder Einwahlverbindungen ein.
ATM	In diesem Menü nehmen Sie die Konfiguration der ATM-Profile vor, die für alle ADSL-Verbindungen benötigt werden, sowie das Verbindungsmonitoring (OAM) und ATM QoS.
Standleitung	In diesem Menü werden die permanenten Verbindungen zweier Kommunikationspartner angezeigt.
Real Time Jitter Control	In diesem Menü können Sie die Upload Geschwindigkeit festlegen.

VPN

Menü	Funktion
IPSec	In diesem Menü konfigurieren Sie VPN-Verbindungen über IP-Sec.
L2TP	In diesem Menü konfigurieren Sie die Verwendung von L2TP (Layer 2 Tunneling Protocol).
PPTP	In diesem Menü konfigurieren Sie einen verschlüsselten PPTP-Tunnel.
GRE	In diesem Menü wird eine Liste aller konfigurierten GRE-Tunnel angezeigt.
Zertifikate	In diesem Menü können Sie Schlüssel generieren, importieren und zertifizieren lassen.

Firewall

Menü	Funktion
Richtlinien	In diesem Menü konfigurieren Sie die Filterregeln der Firewall.
Schnittstellen	In diesem Menü können Sie die zu filternden Schnittstellen in Gruppen zusammenfassen.
Adressen	In diesem Menü können Sie zu filternde Adress-Aliase anlegen.
Dienste	In diesem Menü können Sie zu filternde Service-Aliase anlegen.

VoIP

Menü	Funktion
Application Level Gateway	In diesem Menü konfigurieren Sie einen Proxy für IP-Telefonie, der für die Verbindung zum VoIP-Provider die notwendigen NAT- und Firewall-Freigaben vornimmt.
Media Gateway	In diesem Menü konfigurieren Sie einen Netzübergang zwischen unterschiedlichen Telekommunikationsnetzen.

Lokale Dienste

Menü	Funktion
DNS	In diesem Menü konfigurieren Sie die Namensauflösung.

Menü	Funktion
DynDNS-Client	In diesem Menü konfigurieren Sie die dynamische Namensauflösung.
DHCP-Server	In diesem Menü konfigurieren Sie Ihr Gerät als DHCP-Server.
Web-Filter	In diesem Menü konfigurieren Sie die Verwendung des URL-basierten Proventia Web Filters der Fa. ISS (www.iss.net).
CAPI-Server	In diesem Menü konfigurieren Sie Ihr Gerät als CAPI-Server.
Scheduling	In diesem Menü konfigurieren Sie zeitabhängige Standardaktionen Ihres Geräts.
Überwachung	In diesem Menü konfigurieren Sie die Überwachung von Schnittstellen oder von Hosts im Netzwerk.
ISDN-Diebstahlsicherung	In diesem Menü können Sie die Funktion ISDN-Diebstahlsicherung schnittstellenabhängig konfigurieren.
Funkwerk Discovery	In diesem Menü können Sie Management-Funktionen für bin-tec Access Points konfigurieren.
UPnP	In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Wartung

Menü	Funktion
Diagnose	In diesem Menü können Sie die Erreichbarkeit von Hosts, DNS Servern oder Routen testen.
Software & Konfiguration	In diesem Menü verwalten Sie die Konfigurationsdateien Ihres Geräts. Sie speichern sie z. B. lokal auf Ihrem Gerät oder aber auf Ihrem Rechner ab. Sie können außerdem eine Aktualisierung der Systemsoftware initiieren.
Neustart	In diesem Menü können Sie den Neustart des Geräts initiieren.

Externe Berichterstellung

Menü	Funktion
Systemprotokoll	In diesem Menü konfigurieren Sie den Host, zu dem die intern auf dem Gerät protokollierten Daten zur Speicherung und Weiterverarbeitung weitergeleitet werden sollen.
IP-Accounting	In diesem Menü legen Sie fest, für welche Schnittstellen Accounting-Meldungen generiert werden sollen.
E-Mail-Benachrichtigung	In diesem Menü werden dem Administrator je nach Konfiguration Emails gesendet, sobald relevante Syslog Meldungen auftreten.
SNMP	In diesem Menü konfigurieren Sie, ob das Gerät auf externe SNMP-Zugriffe lauschen und SNMP Traps senden soll.
Activity Monitor	In diesem Menü konfigurieren Sie die Überwachung Ihres Geräts mit dem Windows-Tool Activity Monitor (Bestandteil von BRICKware for Windows).

Monitoring Menüs

Menü	Funktion
Internes Protokoll	In diesem Menü werden die Systemmeldungen angezeigt.
IPSec	In diesem Menü werden die aktuell aktiven IPSec-Verbindungen und Verbindungsstatistiken angezeigt.
ISDN/Modem	In diesem Menü werden die ISDN-Verbindungen angezeigt.
Schnittstellen	In diesem Menü werden Verbindungsstatistiken und der Status aller Schnittstellen angezeigt.
WLAN	In diesem Menü können Sie die WLAN-Verbindungsstatistiken einsehen.

4.3.2 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.

4.4 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. Seriennummer, MAC-Adresse und Software-Versionen.

Der BOOTmonitor wird wie folgt gestartet.

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

R232aw Bootmonitor V.7.2 Rev. 4 from 2005/09/06 00:00:00
Copyright (c) 1996-2005 by Funkwerk Enterprise Communications 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> _

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 5 Systemverwaltung

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

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

5.1 Status

Wenn Sie sich in das **Funkwerk Configuration Interface** 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-, ISDN- WLAN- und ADSL-Schnittstellen
- Informationen über gegebenenfalls gesteckte Zusatzmodule
- die letzten zehn Systemmeldungen

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



Achtung

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

bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen 

Konfiguration speichern

Systemverwaltung

- Status
- Globale Einstellungen
- Schnittstellenmodus / Bridge-Gruppen
- Administrativer Zugriff
- Remote Authentifizierung
- Physikalische Schnittstellen
- LAN
- Wireless LAN
- Routing
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

Automatisches Aktualisierungsintervall: Sekunden **Übernehmen**

Warnung: Systempasswort nicht geändert!

Systeminformationen

Uptime	1 Tag(e) 3 Stunde(n) 42 Minute(n)
Systemdatum	Fr 21 Januar 2005 03:58:00
Seriennummer	R1E180006500018
BOSS-Version	V.7.8 Rev. 2 IPSec from 2008/11/27 00:00:00

Ressourceninformationen

CPU-Nutzung	0%
Arbeitsspeichernutzung	20.3/31.9 MB (64%)
ISDN Verwendung Extern	0 / 4B-Kanäle
Aktive Sitzungen (SIF, RTP, etc...)	0
Aktive IPSec-Tunnel	0 / 0

Physikalische Schnittstelle Schnittstellendetails Link

en1-0	192.168.0.254 / 255.255.255.0	
en1-4	Nicht konfiguriert / Nicht konfiguriert	
WLAN1	Aus	
com0-8	Nicht konfiguriert	
bri2-0	Nicht konfiguriert	
com6-0	Konfiguriert	

Aktuelle Systemprotokolle

Zeit	Level	Subsystem	Nachricht
00:16:03	Informationen	USB	usb6-0-2: Sierra Wireless, Incorporated AirCard, rev 1.10/0.02
00:16:03	Informationen	INET	sshd: pid 56 - listening on 0.0.0.0 port 22.
00:16:03	Fehler	TTY	UMTS Ctl umtsctl_open(): can't open umts device!
00:16:03	Fehler	TTY	Modem answer to <AT+CPIN?> is 'SIM busy'
00:16:02	Informationen	IPSec	init: starting...
00:16:02	Informationen	IPSec	BinTec ipsecd version 3.0 Copyright (c) 1996-2008 by Funkwerk Enterprise Communications GmbH
00:16:02	Informationen	IPSec	init: running
00:16:01	Informationen	Konfiguration	system r1200 started at Thu Jan 20 0:16:01 2005
00:15:59	Fehler	INET	PIM: no valid license found, disabling it.
00:15:58	Informationen	USB	usb6-1-1: HUB with 1 port (1 removable), self-powered

Abb. 63: Systemverwaltung -> Status

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

Felder im Menü Status 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.

Felder im Menü Status Ressourceninformationen

Feld	Wert
CPU-Nutzung	Zeigt die CPU-Auslastung in Prozent an.
Arbeitsspeichernutzung	Zeigt die Auslastung des Arbeitsspeichers in MByte relativ zum verfügbaren Gesamtarbeitsspeicher in MByte an. Die Auslastung wird außerdem in Klammern in Prozent angezeigt.
ISDN Verwendung Intern	Zeigt die Anzahl der aktiven B-Kanäle und die maximale Anzahl an zur Verfügung stehenden B-Kanäle für interne Verbindungen.
ISDN Verwendung Extern	Zeigt die Anzahl der aktiven B-Kanäle und die maximale Anzahl an zur Verfügung stehenden B-Kanäle für ausgehende Verbindungen.
Aktive Sitzungen (SIF, RTP, etc...)	Zeigt die Summe aller SIF, TDRS und IP-Lastenausgleich Sessions an.
Aktive IPSec-Tunnel	Zeigt die Anzahl der aktuell aktiven IPSec-Verbindungen relativ zur Anzahl an konfigurierten IPSec-Verbindungen an.

Felder im Menü Status Module

Feld	Wert
DSP-Modul	Zeigt den Typ eines gegebenenfalls gesteckten DSP-Moduls an.

Weitere Felder im Menü Status

Feld	Wert
Physikalische Schnittstelle - Schnittstellendetails - 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

Feld	Wert
	<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 • Softwareversion der Funkkarte <p>Access Client-Modus:</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> <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
Aktuelle Systemprotokolle	Zeigt die letzten zehn Systemmeldungen an.

5.2 Globale Einstellungen

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

5.2.1 System

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

The screenshot shows the web interface for a bintec R1200 device. At the top, there's a header with 'bintec R1200', a language dropdown set to 'Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. Below the header is a navigation menu with 'Konfiguration speichern' and a sub-menu for 'Systemverwaltung'. The 'Systemverwaltung' menu is expanded to show 'Status', 'Globale Einstellungen', 'Schnittstellenmodus / Bridge-Gruppen', 'Administrativer Zugriff', and 'Remote Authentifizierung'. The 'Globale Einstellungen' menu is further expanded to show 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'System' tab is selected, showing a form for 'Basisparameter' with the following fields:

Basisparameter	
Systemname	r1200
Standort	
Kontakt	FUNKWERK
Maximale Anzahl der Syslog-Protokolleinträge	50
Maximales Nachrichtenlevel von Systemprotokolleinträgen	Informationen
Maximale Anzahl der Accounting-Protokolleinträge	20

At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 64: Systemverwaltung -> Globale Einstellungen -> System

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

Felder im Menü System Basisparameter

Feld	Wert
Systemname	Geben Sie den Systemnamen Ihres Geräts ein. Dieser wird auch als PPP-Host-Name benutzt. Möglich ist eine Zeichenkette mit bis zu 255 Zeichen. Als Standardwert ist der Gerätetyp voreingestellt.
Standort	Geben Sie an, wo sich Ihr Gerät befindet.
Kontakt	Geben Sie die zuständige Kontaktperson an. Hier kann z. B. die E-Mail-Adresse des Systemadministrators eingetragen werden. Möglich ist eine Zeichenkette mit bis zu 255 Zeichen. Standardwert ist <i>funkwerk</i> .
Maximale Anzahl der Syslog-Protokolleinträge	Geben Sie die maximale Anzahl an Systemprotokoll-Nachrichten an, die auf dem Gerät intern gespeichert werden sollen.

Feld	Wert
	<p>Mögliche Werte sind 0 bis 1000 .</p> <p>Standardwert ist 50 . Sie können die gespeicherten Meldungen in Monitoring -> Internes Protokoll anzeigen lassen.</p>
<p>Maximales Nachrichten-level 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 zur Gebührenerfassung auf dem Gerät intern gespeichert werden sollen.</p> <p>Mögliche Werte sind 0 bis 1000 .</p> <p>Standardwert ist 20 .</p>

5.2.2 Passwörter

Auch das Einstellen der Passwörter gehört zu den grundlegenden Systemeinstellungen.

Abb. 65: Systemverwaltung -> Globale Einstellungen -> Passwörter



Hinweis

Alle **bintec**-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 Passwörter Systempasswort

Feld	Wert
Systemadministrator-Pass	Geben Sie das Passwort für den Benutzernamen admin an.

Feld	Wert
wort	Dieses Passwort wird bei SNMPv3 auch für Authentication (MD5) und Encryption (DES) verwendet.
Systemadministrator-Passwort bestätigen	Bestätigen Sie das Passwort, indem Sie es erneut eingeben.

Felder im Menü **Passwörter 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.

Felder im Menü **Passwörter Globale Passwörteroptionen**

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

5.2.3 Datum und Uhrzeit

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

Abb. 66: Systemverwaltung -> Globale Einstellungen -> Datum und Uhrzeit

Für die Ermittlung der Systemzeit haben Sie folgende Möglichkeiten:

- Sie können die Systemzeit automatisch beziehen, z. B. über ISDN oder/und verschiedene Zeit-Server. Um sicherzustellen, dass das Gerät die gewünschte aktuelle Zeit verwendet, sollten Sie einen oder mehrere Zeit-Server konfigurieren.
- Sie können die Systemzeit manuell auf dem Gerät einstellen.



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 Datum und Uhrzeit Systemzeit

Feld	Beschreibung
Aktuelle Systemzeit	Hier werden das aktuelle Datum und die aktuelle Systemzeit angezeigt. Der Eintrag kann nicht verändert werden.

Felder im Menü Datum und Uhrzeit Manuelle Zeiteinstellungen

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

Felder im Menü Datum und Uhrzeit Automatische Zeiteinstellung (Zeitprotokoll)

Feld	Beschreibung
Systemzeit über ISDN aktualisieren	<p>Hier können Sie die ISDN-Funktion aktivieren oder deaktivieren.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Primärer Zeitserver	<p>Geben Sie den ersten Zeit-Server an, entweder mittels Domainnamen oder mittels IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeit-Servers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol mit UDP-Port 123. • <i>Time Service / UDP</i>: Dieser Server nutzt den Zeit-Dienst mit UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst mit TCP-Port 37. • <i>Keiner</i>: Dieser Zeit-Server wird momentan nicht für die Zeitabfrage benutzt.

Feld	Beschreibung
Sekundärer Zeitserver	<p>Geben Sie den zweiten Zeit-Server an, entweder mit Domainnamen oder mit IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeit-Servers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol mit UDP-Port 123. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst mit UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst mit TCP-Port 37. • <i>Keiner</i>: Dieser Zeit-Server wird momentan nicht für die Zeitabfrage benutzt.
Dritter Zeitserver	<p>Geben Sie den dritten Zeit-Server an, entweder mit Domainnamen oder mit IP-Adresse.</p> <p>Wählen Sie außerdem das Protokoll für die Abfrage des Zeit-Servers aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (Standardwert): Dieser Server nutzt das Simple Network Time Protocol mit UDP-Port 123. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst mit UDP-Port 37. • <i>Time Service / TCP</i>: Dieser Server nutzt den Zeit-Dienst mit TCP-Port 37. • <i>Keiner</i>: Dieser Zeit-Server wird momentan nicht für die Zeitabfrage benutzt.
Zeitverschiebung von GMT	<p>Wählen Sie die Abweichung in Stunden zwischen der Systemzeit und der vom Zeit-Server erhaltenen Zeit (meist GMT) aus.</p> <p>Mögliche Werte von <i>-12</i> bis <i>13</i>.</p> <p>Standardwert ist <i>0</i>.</p>
Zeitaktualisierungsintervall	<p>Geben Sie das Zeitintervall in Minuten ein, in dem die automatische Zeitaktualisierung durchgeführt wird.</p>

Feld	Beschreibung
Zeitaktualisierungsrichtlinie	<p>Der Standardwert ist <i>1440</i>.</p> <p>Geben Sie an, in welchen Abständen nach einer gescheiterten Zeitaktualisierung versucht wird, den Zeit-Server erneut zu erreichen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Normal</i> (Standardwert): Es wird nach 1, 2, 4, 8 und 16 Minuten versucht, den Zeit-Server zu erreichen. • <i>Aggressiv</i>: Zehn Minuten lang wird versucht, den Zeit-Server nach 1, 2, 4, 8 Sekunden und danach in 10-Sekunden-Abständen zu erreichen. • <i>Endlos</i>: Es wird ohne zeitliche Begrenzung versucht, den Zeit-Server 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>
Interner 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>

5.2.4 Systemlizenzen

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

Es sind generell folgende Lizenztypen zu unterscheiden:

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

- kostenpflichtige Zusatzlizenzen

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

Lizenzdaten eintragen

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

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

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


Im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **Systemlizenzen** 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.

5.2.4.1 Bearbeiten/Neu

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

The screenshot shows the bintec R1200 web interface. At the top, there is a header with the title 'bintec R1200', a language dropdown set to 'Deutsch', and links for 'Online-Hilfe' and 'Ausloggen'. The 'funkwerk' logo is also present. On the left, a navigation menu is visible with categories like 'Systemverwaltung', 'Status', 'Globale Einstellungen', and various network settings. The main content area shows a breadcrumb trail: 'System' > 'Passwörter' > 'Datum und Uhrzeit' > 'Systemlizenzen'. Below this, there is a form titled 'Basisparameter' with two input fields: 'Lizenzseriennummer' and 'Lizenzschlüssel'. At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 67: 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 Systemlizenzen Basisparameter

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 Funktionalität dieser Lizenz nicht nutzen können.

Lizenz ausschalten

Gehen Sie folgendermaßen vor, um eine Lizenz auszuschalten:

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

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

5.3 Schnittstellenmodus / Bridge-Gruppen

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

Routing versus Bridging

Mit Bridging werden gleichartiger Netze verbunden. Im Gegensatz zum Routing 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 der Schicht 3 (Netzwerkschicht) des OSI-Modells verbunden und Informationen von einem Netz in das andere weitergeleitet (routen).

Konventionen für die Port-/Schnittstellennamen

Die Namen der Funk-Ports in der Benutzeroberfläche Ihres Geräts setzen sich 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, dabei steht en für Ethernet
- (b) Nummer des Ports

Beispiel: *ETH1*

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

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

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

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

- (a) Abkürzung für den Schnittstellentyp
- (b) Nummer der Bridge-Gruppe

Beispiel: *br0* (erste Bridge-Gruppe)

Der Name der Drahtlosnetzwerke setzt sich aus den folgenden Bestandteilen zusammen:

- (a) Abkürzung für den Schnittstellentyp
- (b) Nummer des Funkmoduls
- (c) Nummer der Schnittstelle

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

Der Name der 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-Links konfiguriert ist
- (c) Nummer des WDS-Links bzw. Bridge-Links

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

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

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

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

5.3.1 Schnittstellen

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

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

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

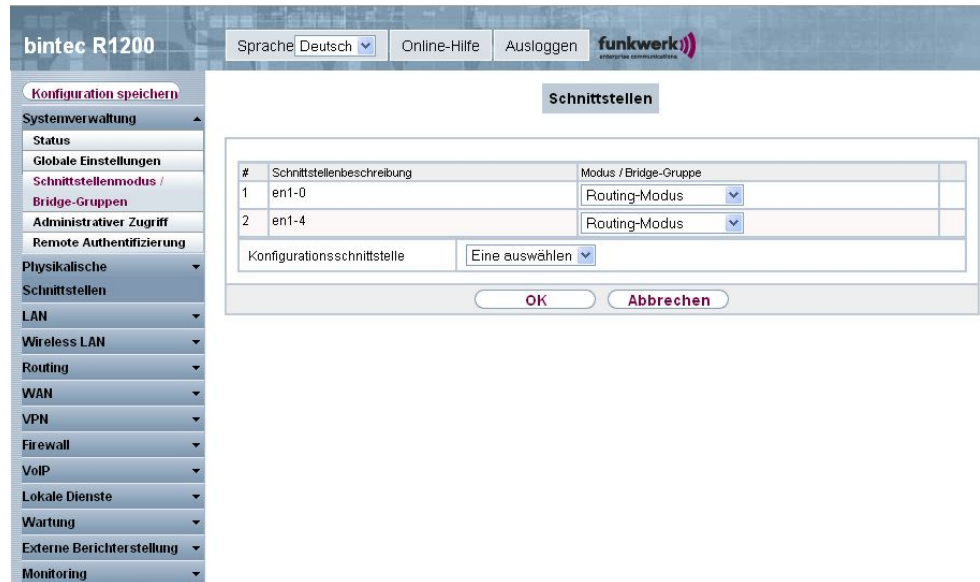


Abb. 68: Systemverwaltung -> Schnittstellenmodus / Bridge-Gruppen -> Schnittstellen

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

Felder im Menü Schnittstellen

Feld	Beschreibung
#	Hier wird die laufende Nummer der Schnittstelle angezeigt.
Schnittstellenbeschreibung	Hier wird der Name der Schnittstelle angezeigt.

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


5.4 Administrativer Zugriff

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

5.4.1 Zugriff

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

bintec R1200

Sprache Deutsch ▼ Online-Hilfe Ausloggen 

Konfiguration speichern

Zugriff **SSH** **SNMP**

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"/>		
bri2-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
com6-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

Hinzufügen **OK** **Abbrechen**

Systemverwaltung

- Status
- Globale Einstellungen
- Schnittstellenmodus /
- Bridge-Gruppen
- Administrativer Zugriff**
- Remote Authentifizierung
- Physikalische Schnittstellen
- LAN
- Wireless LAN
- Routing
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

Abb. 69: Systemverwaltung -> Administrativer Zugriff -> Zugriff

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

5.4.1 Hinzufügen

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

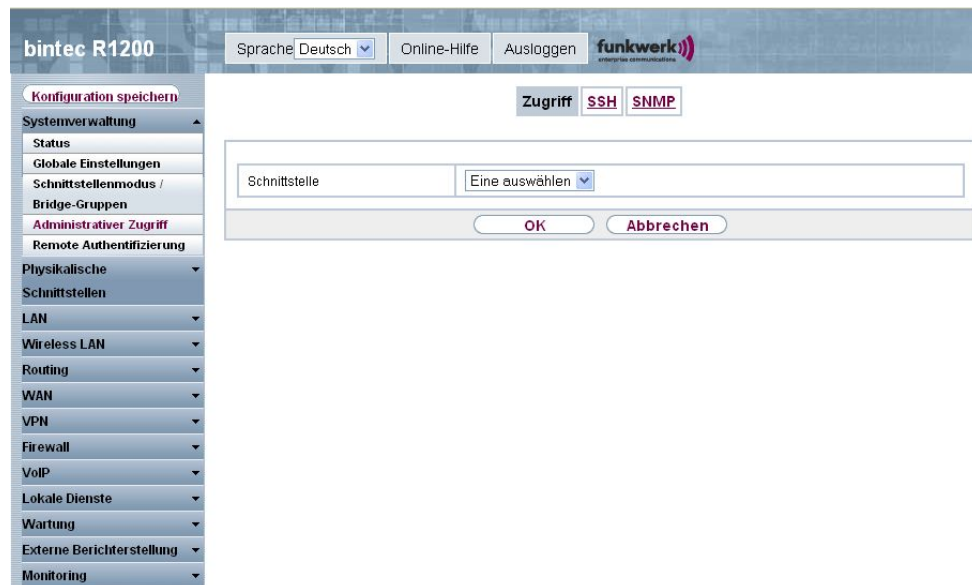


Abb. 70: **Systemverwaltung -> Administrativer Zugriff -> Zugriff -> Hinzufügen**

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.

5.4.2 SSH

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

The screenshot shows the configuration page for SSH on a bintec R1200 device. The interface includes a top navigation bar with 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. Below this is a 'Konfiguration speichern' button and three tabs: 'Zugriff', 'SSH', and 'SNMP'. The main configuration area is titled 'SSH-Parameter (Secure Shell)' and contains the following settings:

SSH-Parameter (Secure Shell)	
SSH-Dienst aktiv	<input checked="" type="checkbox"/> Aktiviert
Komprimierung	<input type="checkbox"/> Aktiviert
TCP-Keepalives	<input checked="" type="checkbox"/> Aktiviert
Protokollierungslevel	Informationen <input type="button" value="v"/>
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	Generiert

At the bottom of the configuration area are 'OK' and 'Abbrechen' buttons.

Abb. 71: 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.funkwerk-ec.com.

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



Hinweis

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

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

Felder im Menü SSH SSH-Parameter (Secure Shell)

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

Feld	Wert
	Standardmäßig ist die Funktion aktiv.
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.

Felder im Menü SSH Authentifizierungs- und Verschlüsselungsparameter

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

Feld	Wert
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>RipeMD160</i> <p>Standardmäßig sind <i>MD5</i>, <i>SHA-1</i> und <i>RipeMD160</i> aktiv.</p>

Felder im Menü SSH Schlüsselstatus

Feld	Wert
RSA-Schlüsselstatus	<p>Hier wird der Status des RSA-Schlüssels angezeigt.</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>Hier wird der Status des DSA-Schlüssels angezeigt.</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>

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

5.4.3 SNMP

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

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

Mit SNMP können folgende Aufgaben des Netzwerkmanagements erfüllt werden:

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

In diesem Menü konfigurieren Sie die Verwendung von SNMP.

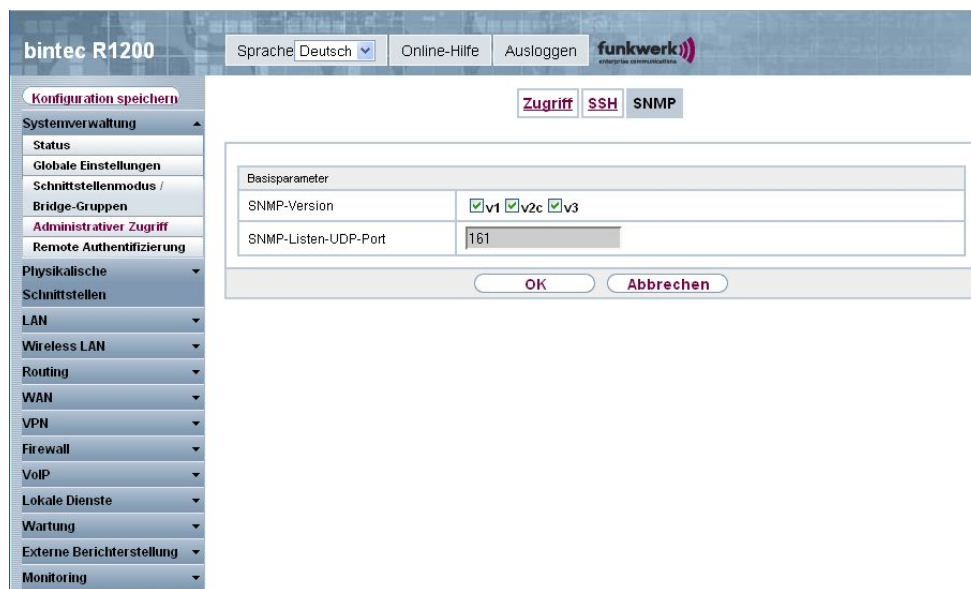


Abb. 72: Systemverwaltung -> Administrativer Zugriff -> SNMP

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

Felder im Menü SNMP Basisparameter

Feld	Wert
SNMP-Version	<p>Wählen Sie aus, mit welcher SNMP-Version Ihr Gerät auf externe SNMP-Zugriffe lauschen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <code>v1</code>: SNMP-Version 1 • <code>v2c</code>: Community-Based SNMP-Version 2 • <code>v3</code>: SNMP-Version 3 <p>Standardmäßig sind <code>v1</code>, <code>v2c</code> und <code>v3</code> aktiv.</p> <p>Ist keine Option ausgewählt, ist die Funktion nicht aktiv.</p>
SNMP-Listen-UDP-Port	<p>Hier wird der UDP-Port (<code>161</code>) angezeigt, 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.

5.5 Remote-Authentifizierung

In diesem Menü finden Sie die Einstellungen für die Benutzerauthentifizierung.

5.5.1 RADIUS

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

RADIUS kann angewendet werden für:

- Authentifizierung
- Gebührenerfassung
- Austausch von Konfigurationsdaten

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

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

RADIUS Pakete


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

Pakettypen

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

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

5.5.1.1 Bearbeiten/Neu

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

bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk**
enterprise communications

Konfiguration speichern

Systemverwaltung

- Status
- Globale Einstellungen
- Schnittstellenmodus /
- Bridge-Gruppen
- Administrativer Zugriff
- Remote Authentifizierung
- Physikalische Schnittstellen
- LAN
- Wireless LAN
- Routing
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

RADIUS TACACS+ Optionen

Basisparameter

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

Erweiterte Einstellungen

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

OK Abbrechen

Abb. 73: Systemverwaltung -> Remote-Authentifizierung -> RADIUS -> Neu

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

Felder im Menü RADIUS Basisparameter

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

Feld	Wert
	wendet, um Konfigurationsdaten für IPSec-Peers an Ihr Gerät zu übermitteln. <ul style="list-style-type: none"> • <i>WLAN (802.1X)</i>: Der RADIUS-Server wird verwendet, um den Zugang zu einem Drahtlosnetzwerk zu regeln.
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.
Priorität	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 nächst niedrigeren Priorität verwendet usw. Mögliche Werte von 0 (höchste Priorität) bis 7 (niedrigste Priorität). Standardwert ist 0 . Siehe auch Richtlinie in den Erweiterten Einstellungen .
Eintrag aktiv	Wählen Sie aus, ob der in diesem Eintrag konfigurierte RADIUS-Server 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	Wert
Richtlinie	Wählen Sie aus, wie Ihr Gerät reagieren soll, wenn eine negative Antwort auf eine Anfrage eingeht. Mögliche Werte: <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

Feld	Wert
	konfigurierten Server erhält.
UDP-Port	<p>Geben Sie den zu verwendenden UDP-Port für RADIUS-Daten ein.</p> <p>Gemäß RFC 2138 sind die Standard-Ports 1812 für die Authentifizierung (1645 in älteren RFCs) und 1813 für Gebührenerfassung (1646 in älteren RFCs) vorgesehen. Der Dokumentation Ihres RADIUS-Servers können Sie entnehmen, welcher Port zu verwenden ist.</p> <p>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 Erreichbarkeit wird 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 Aktiv-Überprüfung = <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>

Feld	Wert
	<p>Mögliche Werte sind ganze Zahlen zwischen 0 und 10 .</p> <p>Standardwert ist 1 . Um zu verhindern, dass Status auf <i>inaktiv</i> gesetzt wird, setzen Sie diesen Wert auf 0.</p>
RADIUS-Dialout	<p>Nur für Authentifizierungstyp = <i>Authentifizierung</i> und <i>IPSec-Authentifizierung</i>.</p> <p>Wählen Sie aus, ob Ihr Gerät vom RADIUS-Server Dialout-Routen abfragt. Auf diesem Weg können automatisch temporäre Schnittstellen angelegt werden und Ihr Gerät kann ausgehende Verbindungen initiieren, die nicht fest konfiguriert sind.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiv ist, können Sie folgende Optionen eingeben:</p> <ul style="list-style-type: none"> • <i>Neulade-Intervall</i>: Geben Sie den Zeitabstand zwischen den Aktualisierungsintervallen in Sekunden ein. <p>Standardmäßig ist hier 0 eingetragen, d. h. ein automatischer Reload wird nicht durchgeführt.</p> <ul style="list-style-type: none"> • <i>Standard-Benutzerpasswort</i>: Dies ist das für die Kommunikation zwischen RADIUS-Server und Ihrem Gerät gemeinsam genutzte Passwort.

5.5.2 TACACS+

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

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

Folgende TACACS+-Funktionen sind auf Ihrem Gerät verfügbar:


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

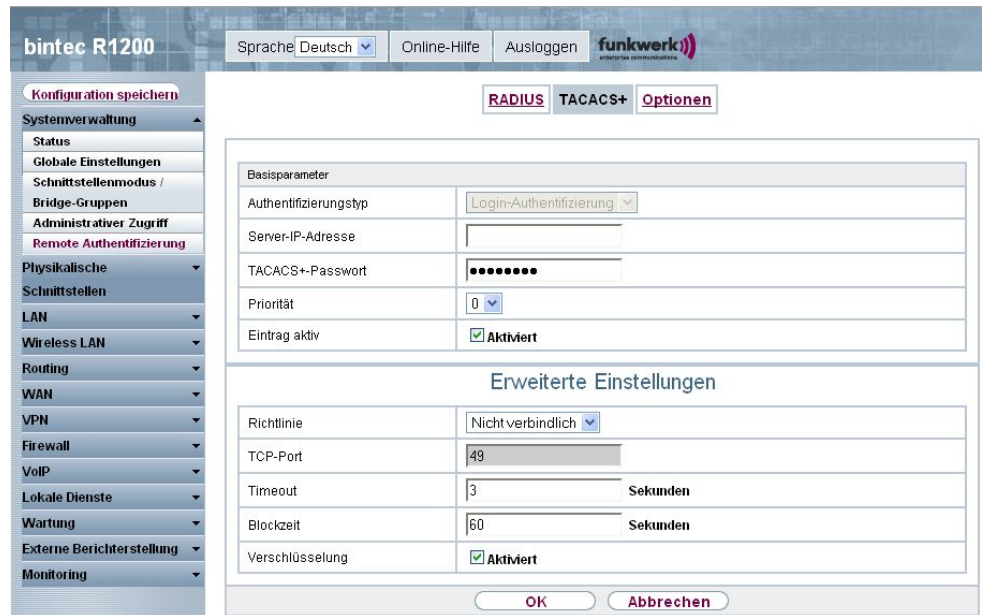
TACACS+ verwendet TCP Port 49 und stellt eine gesicherte und verschlüsselte Verbin-

dung her.

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

5.5.2.1 Bearbeiten/Neu

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



bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Systemverwaltung

- Status
- Globale Einstellungen
- Schnittstellenmodus / Bridge-Gruppen
- Administrativer Zugriff
- Remote Authentifizierung

Physikalische Schnittstellen

- LAN
- Wireless LAN
- Routing
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

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. 74: Systemverwaltung -> Remote-Authentifizierung -> TACACS+ -> Neu

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

Felder im Menü TACACS+ Basisparameter

Feld	Beschreibung
Authentifizierungstyp	<p>Hier wird angezeigt, 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.

Feld	Beschreibung
Server-IP-Adresse	Geben Sie die IP-Adresse des TACACS+-Servers ein, der für eine Login-Authentifizierung abgefragt werden soll.
TACACS+-Passwort	Geben Sie das Passwort ein, welches benutzt werden soll, um den Datenaustausch zwischen dem TACACS+-Server und dem 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 gibt oder der Zugriff verweigert wurde (nur für Richtlinie = Nicht verbindlich), 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 kommt. • <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.

Feld	Beschreibung
TCP-Port	<p>Hier wird der für das TACACS+-Protokoll benutzte Standard-TCP-Port (49) angezeigt. Der Wert kann nicht verändert werden.</p>
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 = Nicht verbindlich) 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 bleiben soll.</p> <p>Nach Ende der Blockierungsdauer wird der Server in den Status versetzt, der im Feld Administrativer Status angegeben ist.</p> <p>Mögliche Werte sind 0 bis 3600 , der Standardwert ist 60 . Der Wert 0 bedeutet, dass der Server nie in einen <i>blockiert</i> - Status versetzt wird und somit keine weiteren Server angefragt werden.</p>
Verschlüsselung	<p>Wählen Sie aus, ob der Datenaustausch zwischen dem TACACS+-Server und dem NAS mit MD5 verschlüsselt werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Ist die Funktion nicht aktiv, werden die Pakete und damit alle dazugehörigen Informationen unverschlüsselt übertragen. Eine unverschlüsselte Übertragung wird nicht als Standardeinstellung sondern nur für Debug-Zwecke empfohlen.</p>

5.5.3 Optionen

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

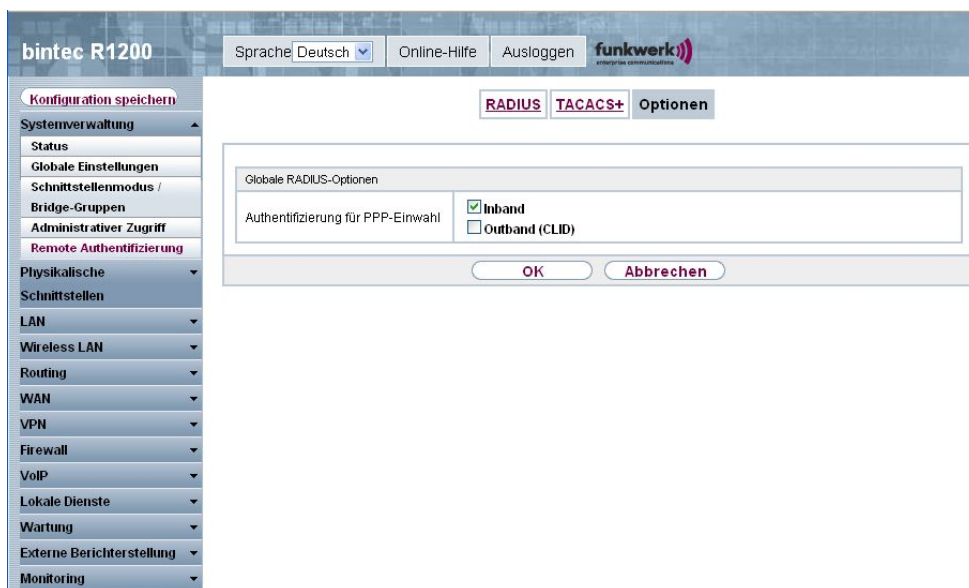


Abb. 75: Systemverwaltung -> Remote-Authentifizierung -> Optionen

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

Felder im Menü Optionen 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 Rufnummerniden-

Feld	Beschreibung
	<p>tifizierung) werden zum in Server-IP-Adresse definierten RADIUS-Server geschickt.</p> <ul style="list-style-type: none">• <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>

Kapitel 6 Physikalische Schnittstellen

6.1 AUX

Für den Anschluss eines externen Analogmodems an den AUX Port eines **bintec**-Gateways, benötigen Sie ein spezielles Kabel für den Konsolen-Port (z. B. AUX-Backup Cable) Ihres Gateways.

6.1.1 AUX

Mit seinem Analog-/GSM-Interface (auxiliary) unterstützt das Gateway auch den Anschluß analoger und GSM-Modems (z. B. als Backup). Dazu können Sie im Prinzip jedes Hayes- bzw. GSM07.07-kompatible Modem mit serieller Schnittstelle verwenden. Folgende Modems sind für **bintec** erfolgreich getestet worden:

- US Robotics Sportster Flash (Analogmodem)
- US Robotics 56K Faxmodem (Analogmodem)
- Siemens TC35i (GSM-Modem)



Abb. 76: PIN-Belegung Modemkabel

Konfiguration speichern

Sprache: Deutsch | Online-Hilfe | Ausloggen | **funkwerk** enterprise communications

AUX

Grundeinstellungen	
AUX-Portstatus	<input checked="" type="checkbox"/> Aktiviert
Leitungsgeschwindigkeit	9600 Bit/s
Eingehender Dienstyp	<input type="radio"/> Deaktiviert <input type="radio"/> ISDN-Login <input checked="" type="radio"/> PPP-Einwahl
SIM-Karte verwendet PIN	<input type="text"/>
Escape-Zeichen des Modems	+ <input type="text"/>
Initialisierungssequenz des Modems	<input type="text"/>
APN (Name des Access-Points)	<input type="text"/>

OK Abbrechen

Abb. 77: Physikalische Schnittstellen -> AUX -> AUX

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

Felder im Menü AUX Basisparameter

Feld	Beschreibung
AUX-Portstatus	<p>Wählen Sie aus, ob der AUX Port aktiv sein soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> ist der Port aktiv. Standardmäßig ist der Port nicht aktiv.</p>
Leitungsgeschwindigkeit	<p>Wählen Sie die Geschwindigkeit, mit der das Modem vom Gateway angesprochen wird (in Bit/s).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i>: Die Baud-Rate der seriellen Terminal-Verbindung wird beibehalten. (9600 im Auslieferungszustand) <p>Alle anderen Werte bedeuten, dass das Modem mit der entsprechenden Geschwindigkeit in Bit/s angesprochen wird.</p> <ul style="list-style-type: none"> • 9600 Bit/s • 19200 Bit/s • 38400 Bit/s • 57600 Bit/s (Standardwert): für die Kommunikation mit einem GSM-Modem empfohlen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>115200 Bit/s</i>: Für die Kommunikation mit einem analogen Modem empfohlen.
Eingehender Diensttyp	<p>Wählen Sie aus, welchem Subsystem des Gateways ein über das Modem eingehender Ruf zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i>: Es erfolgt keine Rufannahme. • <i>ISDN-Login</i> (Standardwert): Der Ruf wird dem ISDN-Login-Subsystem zugewiesen. • <i>PPP-Einwahl</i>: Der Ruf wird dem PPP-Subsystem zugewiesen.
SIM-Karte verwendet PIN	<p>Geben Sie die PIN Ihres GSM-Modems ein, sofern Ihr Modem dies erfordert.</p> <p>Die Eingabe einer falschen PIN unterbindet die Kommunikation mit dem Modem, bis der Eintrag im Profil korrigiert wird.</p>
Escape-Zeichen des Modems	<p>Der Wert für dieses Feld ist per Default auf <i>+</i> gesetzt. Er sollte nur dann verändert werden, wenn der Escape Character des Modems ein anderer ist.</p>
Initialisierungssequenz des Modems	<p>Sie können einen Initialisierungsstring für Ihr Modem eingeben. Standardmäßig ist der Befehl <i>ATX3&K3\V1</i> (das Modem wartet vor dem Wählen nicht auf ein Freizeichen) eingestellt.</p> <p>Sie können weitere AT-Befehle durch Semikola getrennt anhängen. Die Eingabe ist auf 50 Zeichen begrenzt. Stellen Sie sicher, dass Sie den Befehl zur Aktivierung der XON/XOFF Software Flow Control eingeben. Dieser ist herstellerabhängig und kann nicht automatisch eingestellt werden. Die Befehlssequenz erfahren Sie ggf. im Handbuch Ihres Modems oder beim Hersteller.</p>
APN (Name des Access-Points)	<p>Wenn GPRS benutzt werden soll, ist hier der sogenannte Access Point Name des Providers einzutragen, z. B. <i>internet.eplus.de</i> bei <i>eplus</i> usw.</p> <p>Maximal können 40 Zeichen eingegeben werden. Wird hier nichts oder ein falscher APN angegeben, so funktioniert eine konfigurierte GPRS Verbindung nicht.</p>

6.2 Ethernet-Ports

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

ETH1 - ETH4, ETH5

Bei der Trennung der Switch Ports (ETH1 - ETH4) voneinander wird jedem separierten Port im Menü **Portkonfiguration** im Feld **Ethernet-Schnittstellenauswahl** die gewünschte Ethernet-Schnittstelle zugewiesen. Für jede zugewiesene Ethernet-Schnittstelle wird im Menü **Portkonfiguration** eine weitere Schnittstelle in der Liste angezeigt und eine jeweils vollständig eigenständige Konfiguration der Schnittstelle ermöglicht.



Hinweis

Die Ethernet-Ports des Vier-Port-Switches sind im Auslieferungszustand einer einzigen Ethernet-Schnittstelle zugeordnet. Die Ethernet-Schnittstelle en1-0 ist zugewiesen und vorkonfiguriert mit **IP-Adresse** `192.168.0.254` und **Netzmaske** `255.255.255.0`.

Zusätzlich verfügt Ihr Gateway über einen separaten Ethernet-Port (ETH5), der z. B. für die Einrichtung einer DMZ genutzt werden kann. Diesem ist standardmäßig die Ethernet-Schnittstelle en1-4 zugewiesen.

Um die Erreichbarkeit Ihres Geräts zu gewährleisten, achten Sie beim Aufteilen der Ports darauf, dass die Ethernet-Schnittstelle `en1-0` mit der vorkonfigurierten IP-Adresse und Netzmaske einem Port zugewiesen wird, der per Ethernet erreichbar ist. Führen Sie im Zweifelsfall die Konfiguration per serieller Verbindung über die Console-Schnittstelle durch.

VLANS für Routing-Schnittstellen

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

6.2.1 Portkonfiguration

Portseparation

Ihr Gerät bietet die Möglichkeit, die vier Switch Ports als eine Schnittstelle zu betreiben

oder diese logisch voneinander zu trennen und wie vier eigenständige Ethernet-Schnittstellen zu konfigurieren.

Standardmäßig gilt für alle Switch Ports die gleiche Konfiguration.

Bei der Konfiguration sollten Sie Folgendes beachten: Die Aufteilung der Switch Ports auf mehrere Ethernet-Schnittstellen trennt diese nur logisch voneinander. Die verfügbare Gesamtbandbreite von 100 Mbit/s Full Duplex für alle entstandenen Schnittstellen bleibt unverändert. Wenn Sie also z. B. alle Switch Ports voneinander trennen, verfügt jede der entstehenden Schnittstellen nur über einen Teil der vollen Bandbreite. Wenn Sie mehrere Switch Ports zu einer Schnittstelle zusammenfassen, so stehen für alle Ports gemeinsam die volle Bandbreite von 100 Mbit/s Full Duplex zur Verfügung.

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

Abb. 78: Physikalische Schnittstellen -> Ethernet-Ports -> Portkonfiguration

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

Felder im Menü Portkonfiguration Switch-Konfiguration

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

Feld	Beschreibung
	<p>Zur Auswahl stehen vier Schnittstellen, <i>en1-0</i> bis <i>en1-3</i>. In der Grundeinstellung ist allen Switch Ports die Schnittstelle <i>en1-0</i> zugeordnet.</p>
<p>Konfigurierte Geschwindigkeit/konfigurierter Modus</p>	<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 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>Deaktiviert</i> : Die Schnittstelle wird angelegt, bleibt aber inaktiv.
<p>Aktuelle Geschwindigkeit/Aktueller Modus</p>	<p>Zeigt den tatsächlichen Modus und die tatsächliche Geschwindigkeit der Schnittstelle an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>100 MBit/s/Full Duplex</i> • <i>100 MBit/s/Half Duplex</i> • <i>10 MBit/s/Full Duplex</i> • <i>10 MBit/s/Half Duplex</i> • <i>Inaktiv</i>

6.3 ISDN-Ports

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

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

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

6.3.1 ISDN-Konfiguration




Hinweis

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


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

6.3.1.1 Bearbeiten mit

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

ISDN-BRI-Schnittstelle

Die ISDN-BRI-Schnittstellen Ihres Gateways können Sie sowohl für Wähl- als auch für Festverbindungen über ISDN nutzen.

Abb. 79: Physikalische Schnittstellen -> ISDN-Ports -> ISDN-Konfiguration -> 

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

Felder im Menü ISDN-Konfiguration Basisparameter

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Automatische Konfiguration beim Start	Wählen Sie aus, ob der ISDN Switch Typ (D-Kanalerkennung für Wählverbindungen) automatisch erkannt werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Ergebnis der automatischen Konfiguration	Zeigt den Status der ISDN-Autokonfiguration an. Die automatische D-Kanal-Erkennung läuft, bis eine Einstellung gefunden wird bzw. bis das ISDN-Protokoll unter ISDN-Protokoll manuell ausgewählt ist. Das Feld kann nicht editiert werden. Mögliche Werte: <ul style="list-style-type: none"> • <i>ISDN Configtype Point-to-Point</i>: Siehe ISDN-Protokoll und ISDN-Konfigurationstyp

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>ISDN Configtype Point-to-Multipoint</i>: Siehe ISDN-Protokoll und ISDN-Konfigurationstyp • <i>Autoconfiguration Deaktiviert</i>: Manuelle Einstellung von ISDN Protokoll und ISDN-Konfigurationstyp. • <i>Wird ausgeführt</i>: Erkennung läuft noch.
Port-Verwendung	<p>Nur wenn Automatische Konfiguration beim Start deaktiviert ist.</p> <p>Wählen Sie das Protokoll aus, das für den ISDN-Port verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i>: Der ISDN-Anschluss wird nicht genutzt. • <i>Euro-ISDN</i>
ISDN-Konfigurationstyp	<p>Nur wenn Automatische Konfiguration beim Start deaktiviert ist.</p> <p>Wählen Sie die ISDN-Anschlussart aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Punkt-zu-Mehrpunkt</i> (Standardwert): Mehrgeräteanschluss. • <i>Punkt-zu-Punkt</i>: Anlagenanschluss.
ISDN-Switch-Typ	<p>Wählen Sie das ISDN-Protokoll, das Ihnen Ihr Provider zur Verfügung stellt:</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standleitung B1 64S</i>: Festverbindung über B-Kanal 1 (64 kbit/s) • <i>Standleitung B1+B2 64S2</i>: Festverbindung über beide B-Kanäle (128 kbit/s) • <i>Standleitung D+B1+B2 TS02</i>: Festverbindung über D-Kanal und beide B-Kanäle (144 kbit/s) • <i>Standleitung B1+B2 Unterschiedliche Endpunkte</i>: Festverbindung zu zwei verschiedenen Endpunkten. • <i>Standleitung B1+D TS01</i>: Festverbindung über B-Kanal

Feld	Beschreibung
	<p>1 und D-Kanal (80 kbit/s)</p> <ul style="list-style-type: none"> • <i>Standleitung B2+D TS01</i>: Festverbindung über B-Kanal 2 und D-Kanal (80 kbit/s) • <i>Standleitung B2 64S</i>: Festverbindung über B-Kanal 2 (64 kbit/s)

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


Felder im Menü Erweiterte Einstellungen

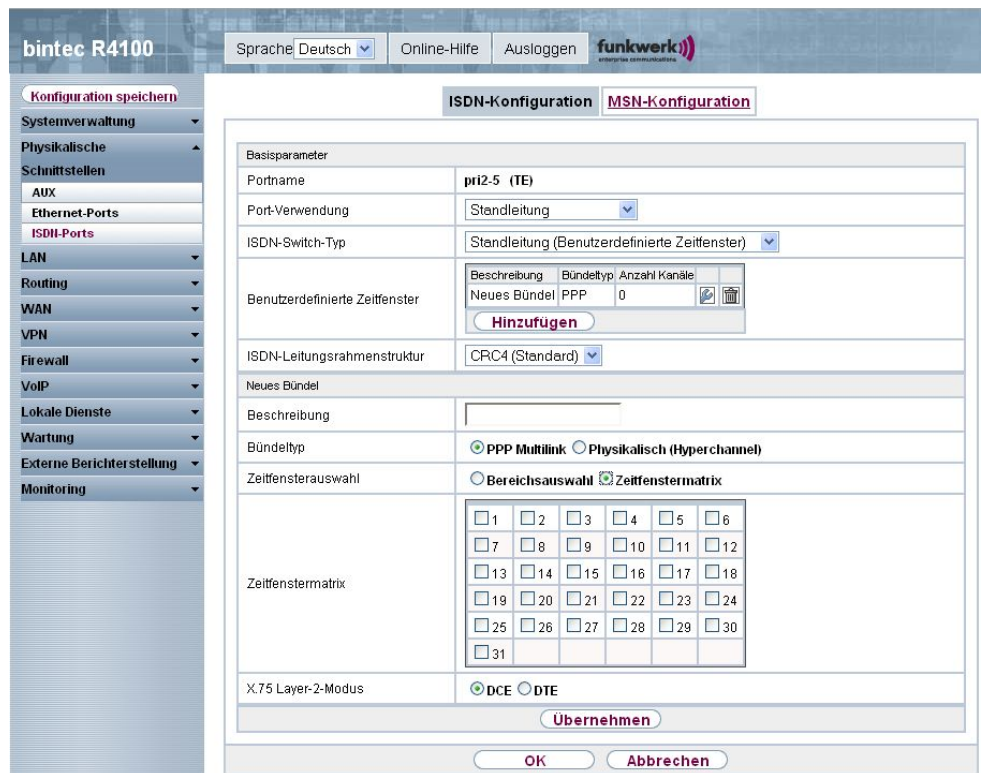
Feld	Beschreibung
X.31 (X.25 im D-Kanal)	<p>Wählen Sie aus, ob Sie X.31 (X.25 im D-Kanal) z. B. für CAPI-Applikationen nutzen wollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
X.31 TEI-Wert	<p>Nur wenn X.31 (X.25 im D-Kanal) aktiviert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

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


ISDN-PRI-Schnittstelle

Bei Primärmultiplexanschluss (PRI, auch S2M genannt) werden die Kanäle nacheinander in so genannten Zeitschlitzen übertragen.

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



The screenshot shows the configuration interface for a bintec R4100 device. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstattung', and 'Monitoring'. Under 'Physikalische Schnittstellen', 'ISDN-Ports' is selected. The main area is titled 'ISDN-Konfiguration' and 'MSN-Konfiguration'. The 'Basisparameter' section includes fields for 'Portname' (pri2-5 (TE)), 'Port-Verwendung' (Standleitung), 'ISDN-Switch-Typ' (Standleitung (Benutzerdefinierte Zeitsfenster)), and 'ISDN-Leitungsrahmenstruktur' (CRC4 (Standard)). A table for 'Benutzerdefinierte Zeitsfenster' shows a 'Neues Bündel' with 'PPP' type and '0' channels. Below this is a 'Zeitsfenstermatrix' grid with 31 slots (1-31) and checkboxes. The 'X.75 Layer-2-Modus' section has radio buttons for 'DCE' (selected) and 'DTE'. Buttons for 'Übernehmen', 'OK', and 'Abbrechen' are at the bottom.

Abb. 80: **Physikalische Schnittstellen** -> **ISDN-Ports** -> **ISDN-Konfiguration** -> 

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

Felder im Menü ISDN-Konfiguration Basisparameter

Feld	Beschreibung
Portname	Zeigt den Namen des ISDN-Ports an.
Port-Verwendung	<p>Wählen Sie aus, ob der ISDN Switch Typ (D-Kanalerkennung für Wählverbindungen) automatisch erkannt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): ISDN-Anschluss wird nicht genutzt. • <i>EURO ISDN S2M (TE)</i>: EURO ISDN S2M User Profile • <i>EURO ISDN S2M (NT)</i>: EURO ISDN S2M Network Profile • <i>Back to Back (dialup)</i>: Zwei S2M-Anschlüsse werden direkt gekoppelt. • <i>Standleitung</i>: Sie können eine Standleitung auswählen.
ISDN-Leitungsrahmenstruktur	<p>Nur wenn eine Port-Verwendung ausgewählt ist.</p> <p>Wählen Sie den Framing-Typ für Layer 1 aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>CRC4 (Standard)</i> (Standardwert) • <i>Ohne CRC</i> <p>Der Standardwert kann in den meisten Anwendungsfällen beibehalten werden. Gegebenenfalls (z. B. in Schweden und Frankreich) können Sie die Option <i>Ohne CRC</i> verwenden, wenn das Gerät an eine TK-Anlage angeschlossen werden soll.</p>
Rufnummer	<p>Nur wenn Port-Verwendung = <i>EURO ISDN S2m (TE)</i> oder <i>EURO ISDN S2m (NT)</i> Tragen Sie die Rufnummer für die Verbindung ein.</p>
Kanalauswahl	<p>Nur wenn Port-Verwendung = <i>EURO ISDN S2m (TE)</i></p> <p>Um die Kompatibilität auch mit speziellen Dienst Anbietern zu gewährleisten, ist für Port-Verwendung = <i>EURO ISDN S2m (TE)</i> eine weitere Option vorgesehen: Wenn Sie den Switch Type entsprechend setzen, können Sie einen Wert für die Variable Kanalauswahl wählen. Diese definiert, wie der B-Kanal für einen abgehenden Ruf ausgewählt wird.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebiger Kanal</i> (Standardwert): Das Gerät meldet der TK-Anlage, dass jeder Kanal möglich ist. Die Vermittlungsstelle der TK-Anlage wählt den zu verwendenden Kanal. • <i>Keine Kanalidentifizierung</i> : Das Gerät sendet keine IE-Kanalidentifizierung (IE = information element). Die Vermittlungsstelle wählt den zu verwendenden Kanal. • <i>Bevorzugten Kanal senden</i> : Das Gerät wählt den zu verwendenden Kanal und signalisiert diesen der Vermittlungsstelle. <p>In der Regel können Sie den Standardwert verwenden. Lediglich in wenigen Sonderfällen ist eine Anpassung der Einstellung notwendig.</p> <p>Sollten Sie Probleme mit abgehenden Rufen haben, fragen Sie Ihren Provider, ob ein spezieller Wert eingestellt werden muss.</p>
Taktsignal-Modus	<p>Nur wenn Port-Verwendung = <i>Back to Back (dialup)</i></p> <p>Legen Sie fest, welcher der Verbindungspartner das Taktsignal für die Synchronisation zwischen Sender und Empfänger senden soll. Wenn das Taktsignal nicht von der Vermittlungsstelle selber gesendet wird, muss einer der Verbindungspartner das Signal senden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Extern</i>: Das Gerät erhält das Taktsignal. • <i>Intern</i>: Das Gerät sendet das Taktsignal.
ISDN-Switch-Typ	<p>Nur wenn Port-Verwendung = <i>Standleitung</i> Wählen Sie die ISDN-Anschlussart aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standleitung (Benutzerdefinierte Zeitschlitzze)</i>: Bis zu 31 PPP-Schnittstellen können für Festverbindungen zu unterschiedlichen Zielen konfiguriert werden • <i>Standleitung, 1 Hyperchannel (G.703 +</i>

Feld	Beschreibung
	:1984 kBit/s, strukturiert <ul style="list-style-type: none"> • <i>Standleitung Unstrukturiert G.703</i>: 2048 kBit/s, nicht strukturiert
Benutzerdefinierte Zeitschlitz	<p>Nur wenn Port-Verwendung = <i>Standleitung</i> und ISDN-Switch-Typ = <i>Standleitung (Benutzerdefinierte Zeitschlitz)</i></p> <p>Sie haben die Möglichkeit, Kanäle beliebig auf dem physikalischen Layer als sogenannte Hyper Channel zu bündeln. Sie können aber auch Kanäle als PPP-Multilink-Kanalbündel zusammenfassen.</p> <p>Timeslots (sogenannte Zeitscheiben oder Zeitschlitz) unterteilen die zur Verfügung stehenden 2 MBit Bandbreite einer S2M-Verbindung in logische Kanäle. Im Folgenden wird nicht zwischen Timeslots und Kanälen unterschieden, da der Unterschied für die Konfiguration ohne Belang ist.</p> <p>Sie sehen eine Aufstellung der bereits konfigurierten Kanalbündel.</p> <p>Klicken Sie auf Hinzufügen um neue Kanalbündel zu konfigurieren.</p>

Über die Schaltfläche **Hinzufügen** bei **Benutzerdefinierte Zeitschlitz** können Sie weitere Bündel konfigurieren.



Hinweis

Diese Funktion steht nur für Standleitungen zur Verfügung.

Felder im Menü ISDN-Konfiguration Neues Bündel

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Kanalbündels an.
Bündeltyp	Zeigt die Art des Kanalbündels an. Mögliche Werte: <ul style="list-style-type: none"> • <i>PPP Multilink</i>: Die Kanäle werden als PPP-Multilink-Kanäle gebündelt. • <i>Physikalisch (Hyperchannel)</i>: Die Kanäle werden als

Feld	Beschreibung
	physikalische Hyperchannels gebündelt.
Zeitschlitzauswahl	Wählen Sie zwischen <i>Bereichsauswahl</i> und <i>Zeitschlitzmatrix</i> aus.
Zeitschlitzbereich	<p>Nur wenn Zeitschlitzauswahl = <i>Bereichsauswahl</i></p> <p>Zeigt die logischen Kanäle (Timeslots) an, die zu diesem Kanalbündel zusammengefügt werden.</p> <ul style="list-style-type: none"> • <i>Von</i>: Zeigt den ersten der für dieses Kanalbündel verwendeten Kanal an. Mögliche Werte: 1 bis 31. • <i>Bis</i>: Zeigt den letzten der für dieses Kanalbündel verwendeten Kanal an. Mögliche Werte: 1 bis 31. • <i>Specify Selection</i>: Hier können Sie eine differenzierte Zuweisung vornehmen.
Zeitschlitzmatrix	Nur wenn Zeitschlitzauswahl = <i>Zeitschlitzmatrix</i> Zeigt eine Liste aller Kanäle im einzelnen an. Wenn Sie nicht alle Kanäle zwischen einem bestimmten Start- und einem bestimmten Endkanal für ein Kanalbündel verwenden wollen, können Sie hier eine differenzierte Zuweisung vornehmen.
X.75 Layer-2-Modus	<p>Definieren Sie, wie sich die Schnittstelle, die durch dieses Kanalbündel entsteht, beim Verbindungsaufbau verhält. Diesen Parameter brauchen Sie nur dann zu konfigurieren, wenn Sie X.75 im Layer 2 verwenden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DCE</i> • <i>DTE</i>

6.3.2 MSN-Konfiguration

In diesem Menü teilen Sie die zur Verfügung stehenden ISDN-Rufnummern den gewünschten Diensten (z. B. PPP-Routing, ISDN-Login) zu.

Falls Sie die ISDN-Schnittstelle für aus- und eingehende Wählverbindungen verwenden, sind in diesem Menü die eigenen Rufnummern für diese Schnittstelle einzutragen (für Festverbindungen sind diese Einstellungen nicht möglich). Entsprechend den Einstellungen in diesem Menü verteilt Ihr Gerät die eingehenden Rufe auf die internen Dienste. Ausgehenden Rufen wird die eigene Rufnummer als Nummer des Anrufers (Calling Party Number)

mitgegeben.

Das Gerät unterstützt die Dienste:

- **PPP (routing):** Der Dienst PPP (routing) ist der allgemeine Routing-Dienst Ihres Geräts. Damit werden u. a. ISDN-Gegenstellen Datenverbindungen mit Ihrem LAN ermöglicht. So können Sie es Partnern außerhalb Ihres lokalen Netzwerkes ermöglichen, auf Hosts in Ihrem LAN zuzugreifen. Genauso ist es möglich, ausgehende Datenverbindungen zu ISDN-Gegenstellen aufzubauen.
- **ISDN-Login:** Der Dienst ISDN-Login ermöglicht sowohl eingehende Datenverbindungen mit Zugang zur SNMP-Shell Ihres Geräts, als auch ausgehende Datenverbindungen zu anderen **bintec**-Geräten. So kann Ihr Gerät aus der Ferne konfiguriert und gewartet werden.
- **IPSec:** Um Hosts, die nicht über feste IP-Adressen verfügen, dennoch eine sichere Verbindung über das Internet zu ermöglichen, unterstützen **bintec**-Geräte den DynDNS-Dienst. Durch die Funktion IPSec Callback kann mit Hilfe eines direkten ISDN-Rufs bei einem IPSec Peer mit dynamischer IP-Adresse diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.
- **X.25 PAD:** Mit X.25 PAD wird ein Protokollkonverter zur Verfügung gestellt, der nicht-paketorientierte Protokolle in paketorientierte Kommunikationsprotokolle und umgekehrt konvertiert. Datenendeinrichtungen, die ihre Daten nicht datenpaketorientiert senden bzw. empfangen, können so an Datex-P (öffentliches Datenpaketnetz nach dem Prinzip der Datenpaketvermittlung) angepasst werden.

Wenn ein Ruf eingeht, überprüft Ihr Gerät zunächst anhand der Einträge in diesem Menü die Art des Anrufs (Daten- oder Sprachruf) und die Called Party Number, wobei nur der Teil der Called Party Number das Gerät erreicht, der von der Ortsvermittlung bzw., falls vorhanden, von der TK-Anlage weitergeleitet wird. Anschließend wird der Ruf dem passenden Dienst zugewiesen.



Hinweis

Wenn kein Eintrag vorhanden ist (Auslieferungszustand) wird jeder über ISDN eingehende Ruf vom Dienst ISDN-Login angenommen. Um dies zu vermeiden, machen Sie hier auf jeden Fall die erforderlichen Eintragungen. Sobald ein Eintrag vorhanden ist, werden eingehende Rufe, die keinem Eintrag zugeordnet werden können, an den Dienst CAPI weitergeleitet.

Im Menü **Physikalische Schnittstellen** -> **ISDN-Ports** -> **MSN-Konfiguration** wird eine

Liste aller MSNs angezeigt.

6.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um die MSNs zu bearbeiten.

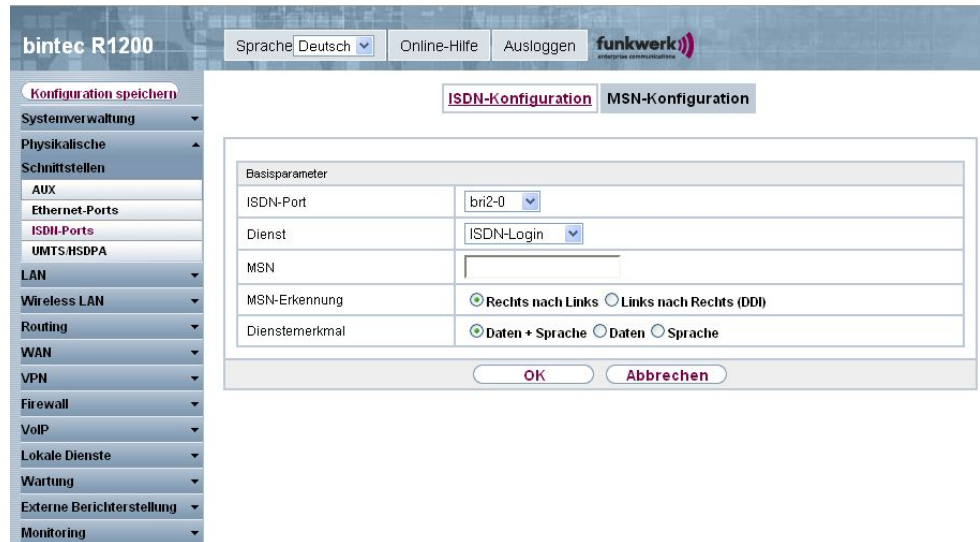


Abb. 81: Physikalische Schnittstellen -> ISDN-Ports -> MSN-Konfiguration -> Neu

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

Felder im Menü MSN-Konfiguration Basisparameter

Feld	Beschreibung
ISDN-Port	Wählen Sie den ISDN-Port aus, für den die MSN konfiguriert werden soll.
Dienst	<p>Wählen Sie den Dienst aus, dem ein Ruf auf die untenstehende MSN zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>ISDN-Login</i> (Standardwert): Ermöglicht Einloggen mit <i>ISDN-Login</i>. • <i>PPP (Routing)</i>: Standardeinstellung für PPP-Routing. Enthält die automatische Erkennung der unten genannten PPP-Verbindungen außer <i>PPP DOVB</i>. • <i>IPSec</i>: Ermöglicht die Festlegung einer Rufnummer für IP-

Feld	Beschreibung
	<p>Sec-Callback.</p> <ul style="list-style-type: none"> • <i>Andere (PPP)</i>: Weitere Dienste können ausgewählt werden: <i>PPP 64k</i> (Ermöglicht 64 kBit/s PPP-Datenverbindungen), <i>PPP 56k</i> (Ermöglicht 56 kBit/s PPP-Datenverbindungen), <i>PPP V.110 (9600...38400)</i> (Ermöglicht PPP-Verbindungen mit V.110 und mit Bit-Raten von 1200 Bit/s, 2400 Bit/s,..., 38400 Bit/s), <i>PPP V.120</i> (Ermöglicht eingehende PPP-Verbindungen mit V.120).
MSN	<p>Geben Sie die Rufnummer ein, die zur Überprüfung der Called Party Number verwendet wird, wobei zur Rufannahme eine Übereinstimmung einzelner Ziffern im Eintrag unter Berücksichtigung der Konfiguration in MSN-Erkennung genügt.</p>
MSN-Erkennung	<p>Wählen Sie den Modus aus, mit dem Ihr Gerät den Ziffernvergleich von MSN mit der "Called Party Number" des eingehenden Rufes durchführt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Rechts nach links</i> (Standardwert) • <i>Links nach rechts (DDI)</i>: Immer auswählen, wenn Ihr Gerät mit einem Point-to-Point-Anschluss (Anlagenanschluss) verbunden ist.
Dienstmerkmal	<p>Wählen Sie die Art des eingehenden Rufes (Diensterkennung) aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Daten + Sprache</i> (Standardwert): sowohl Daten- als auch Sprachruf. • <i>Daten</i>: Datenruf • <i>Sprache</i>: Sprachruf (Modem, Sprache, analoges Fax).

6.4 ADSL-Modem

6.4.1 ADSL-Konfiguration

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

R3000 und **R3000w** sind ADSL Multiprotokoll Router mit integrierten ADSL(2+) Modem und automatischem ISDN Backup. Das ADSL Modem des **R3000 / R3000w** ist für die Standards ANNEX-A und ANNEX-B geeignet und somit in vielen Ländern universell einsetzbar. Er eignet sich besonders für den High-Speed Internet Zugang und den Remote-Access Einsatz in kleinen bis mittleren Unternehmen oder Remote-Offices. Das Gerät verfügt ab Werk bereits über 10 IPsec Tunnel inklusive Hardwarebeschleunigung. Bis zu 100 zusätzliche IPsec Tunnel lassen sich per Lizenz frei schalten. Die integrierte zweite ISDN S0 Schnittstelle kann ebenfalls optional per Lizenz aktiviert werden.

Abb. 82: Physikalische Schnittstellen -> ADSL-Modem -> ADSL-Konfiguration

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

Felder im Menü ADSL-Konfiguration ADSL-Portstatus

Feld	Beschreibung
ADSL-Chipsatz	Zeigt die Kennung des eingebauten Chipsatzes an.
Physikalische Verbindung	<p>Zeigt den aktuellen ADSL-Betriebsmodus an. Der Wert kann nicht verändert werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Unbekannt</i>: Der ADSL Link ist nicht aktiv. • <i>ANSI T1.413</i>: ANSI T1.413 • <i>ADSL1</i>: ADSL classic, G.DMT, ITU G.992.1

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>G.Lite</i>: Splitterless ADSL, ITU G.992.2 • <i>ADSL2</i>: G.DMT.Bis, ITU G.992.3 • <i>ADSL2 DELT</i>: ADSL2 Double Ended Line Test • <i>ADSL2 Plus</i>: ADSL2 Plus, ITU G.992.5 • <i>ADSL2 Plus DELT</i>: ADSL2 Plus Double Ended Line Test • <i>READSL2</i>: Reach Extended ADSL2 • <i>READSL2 DELT</i>: Reach Extended ADSL2 Double Ended Line Test. • <i>ADSL2 ITU-T G.992.3 Annex M</i> • <i>ADSL2+ ITU-T G.992.5 Annex M</i>

Felder im Menü ADSL-Konfiguration Aktuelle Leitungsgeschwindigkeit

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

Felder im Menü ADSL-Konfiguration ADSL-Parameter

Feld	Beschreibung
ADSL-Modus	<p>Definieren Sie, gemäß welchem Annex der ITU-T-Empfehlung G.991.2 die Verbindung realisiert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Annex A</i>: Zum Beispiel für Anwendungsgebiete in Nordamerika (Provider-abhängig). • <i>Annex B</i>(Standardwert): Zum Beispiel für Anwendungsgebiete in Europa (Provider-abhängig).
ADSL-Sync-Typ	<p>Wählen Sie den ADSL-Synchronisierungstyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatischer Modus</i> (Standardwert): Der ADSL-Modus

Feld	Beschreibung
	<p>wird dem der Gegenstelle automatisch angepasst.</p> <ul style="list-style-type: none"> • <i>ADSL1</i>: ADSL1 / G.DMT wird angewendet. • <i>ADSL2</i>: ADSL2 / G.992.3 wird angewendet. • <i>ADSL2 Plus</i>: ADSL2 Plus / G.992.5 wird angewendet. • <i>Automatischer Modus (Annex-M)</i>: Nur für ADSL-Modus = Annex A. Der ADSL-Modus wird dem der Gegenstelle automatisch angepasst unter Einbeziehung von G.992.3 Annex M. • <i>ADSL2 Plus (Annex-M)</i>: Nur für ADSL-Modus = Annex A. ADSL2 Plus / G.992.3 Annex M wird angewendet. • <i>Keiner</i>: Die ADSL-Schnittstelle ist nicht aktiv.
Transmit Shaping	<p>Wählen Sie aus, ob die Datenrate in Senderichtung reduziert werden soll. Dies ist nur in wenigen Fällen an speziellen DSLAMs notwendig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard (Leitungsgeschwindigkeit)</i>: Die Datenrate in Senderichtung wird nicht reduziert. • <i>128.000 Bit/s bis 2.048.000 Bit/s</i>: Die Datenrate in Senderichtung wird reduziert auf maximal 128.000 Bit/s bis 2.048.000 Bit/s in festgesetzten Schritten. • <i>Benutzerdefiniert</i>: Die Datenrate wird reduziert auf den in Maximale Upstream-Bandbreite eingegebenen Wert. <p>Standardwert ist <i>Standard (Leitungsgeschwindigkeit)</i>.</p>
Maximale Upstream-Bandbreite	<p>Nur für Transmit Shaping = Benutzerdefiniert</p> <p>Geben Sie die maximale Datenrate in Senderichtung in Bits pro Sekunde ein.</p>

6.5 SHDSL

6.5.1 SHDSL-Konfiguration

Im Menü **SHDSL** konfigurieren Sie die SHDSL-Schnittstelle Ihres Geräts.

R3400 und **R3800** verfügen über ein integriertes SHDSL-Modem. Die Geräte unterstützen die ITU-T-Empfehlungen G.991.2. Je nach Gerätetyp und Konfiguration überträgt das Gateway die Daten über ein Adernpaar mit bis zu 2312 kBit/s, über zwei Adernpaare mit bis zu 4624 kBit/s, über drei Adernpaare mit bis zu 6936 kBit/s oder über vier Adernpaare mit bis zu 9248 kBit/s.



Hinweis

Erkundigen Sie sich gegebenenfalls bei Ihrem Provider nach den Besonderheiten Ihres SHDSL-Anschlusses.



Hinweis

Verständigen Sie sich bei Back-to-Back-Verbindungen (Campus-Connect) mit Ihrer Gegenstelle über die Anschlussbedingungen.

Die SHDSL-Schnittstellen können separat oder als Bündel konfiguriert werden.

Wählen Sie die Schaltfläche , um die Konfiguration der SHDSL-Profile zu bearbeiten.

Abb. 83: Physikalische Schnittstellen -> SHDSL -> SHDSL-Konfiguration ->

Felder im Menü SHDSL SHDSL-Parameter

Feld	Beschreibung
ATM-Schnittstelle	Zeigt den Namen der ATM-Schnittstelle an.

Feld	Beschreibung
Gerätemodus	<p>Definieren Sie die Rolle innerhalb der Verbindung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>CPE (Customer Premises Equipment)</i> (Standardwert): Modus für die Benutzerseite der SHDSL-Verbindung. • <i>CO (Central Office)</i>: Modus für die Provider-Seite der SHDSL-Verbindung. <p>Beachten Sie: Bei einer SHDSL-Verbindung muss immer auf einer Seite CPE und auf der anderen Seite CO eingestellt sein.</p>
SHDSL-Typ	<p>Definieren Sie, gemäß welchem Annex der ITU-T-Empfehlung G.991.2 die Verbindung realisiert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Annex A</i>: Zum Beispiel für Anwendungsgebiete in Nordamerika (Provider-abhängig). • <i>Annex B</i>(Standardwert): Zum Beispiel für Anwendungsgebiete in Europa (Provider-abhängig).
Übertragungsrate	<p>Definieren Sie, ob die Übertragungsrate ausgehandelt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Fest eingestellt</i>: Die Übertragungsrate ist vorgegeben. • <i>Adaptiv</i>(Standardwert): Die Übertragungsrate wird abhängig von der Leitungsqualität ausgehandelt.
Leitungsmodus	<p>Definieren Sie die Anzahl und Kombination der Adern (abhängig vom Gerätetyp), die für die SHDSL-Verbindung genutzt werden sollen.</p> <p>Nur für R3400:</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2-Draht</i>(Standardwert): Zwei Adern werden mit m-pair Bonding für eine Übertragungsrate von 192 kBit/s bis 2312 kBit/s genutzt. • <i>4-Draht</i>: Vier Adern werden mit m-pair Bonding für eine Übertragungsrate von 384k Bit/s bis 4624 kBit/s genutzt. Die-

Feld	Beschreibung
	<p>se Option unterstützt den 4-Wire-Mode nach G991.2 und den Globespan Enhanced Mode.</p> <p>Nur für R3800:</p> <ul style="list-style-type: none"> • <i>2-Draht</i>: 2 Adern werden mit m-pair Bonding für eine Übertragungsrate von 192 kBit/s bis 2312 kBit/s genutzt. • <i>4-Draht</i>: 4 Adern werden mit m-pair Bonding für eine Übertragungsrate von 384k Bit/s bis 4624 kBit/s genutzt. Diese Option unterstützt den 4-Wire-Mode nach G991.2 und den Globespan Enhanced Mode. • <i>4-Draht-Standard</i>: 4 Adern werden für m-pair Bonding mit eine Übertragungsrate von 384 kBit/s bis 4624 kBit/s genutzt. Diese Option unterstützt den 4-Wire-Mode nach G991.2, nicht aber den Globespan Enhanced Mode. • <i>4-Draht-IMA</i>: 4 Adern werden mit IMA für eine Übertragungsrate von 384 kBit/s bis 4624 kBit/s genutzt. • <i>6-Draht</i>: 6 Adern werden mit m-pair Bonding für eine Übertragungsrate von 576 kBit/s bis 6936 kBit/s genutzt. • <i>6-Draht-IMA</i>: 6 Adern werden mit IMA für eine Übertragungsrate von 576 kBit/s bis 6936 kBit/s genutzt. • <i>8-Draht</i>: 8 Adern werden mit m-pair Bonding für eine Übertragungsrate von 768 kBit/s bis 9248 kBit/s genutzt. • <i>8-Draht-IMA</i>: 8 Adern werden mit IMA für eine Übertragungsrate von 768 kBit/s bis 9248 kBit/s genutzt.
Zusätzliche Aderpaare	<p>Nur für Leitungsmodus = <i>4-Draht</i>, <i>4-Draht-Standard</i>, <i>4-Draht-IMA</i>, <i>6-Draht</i>, <i>6-Draht-IMA</i>.</p> <p>Für Leitungsmodus = <i>4-Draht</i>, <i>4-Draht-Standard</i> oder <i>4-Draht-IMA</i> wird hier das zweite Aderpaar festgelegt.</p> <p>Für Leitungsmodus = <i>6-Draht</i> oder <i>6-Draht-IMA</i> wird hier das zweite und das dritte Aderpaar festgelegt.</p> <p>Aderpaare, die in bereits definierten Verbänden verwendet werden, stehen nicht zur Wahl. Sollen solche dennoch für diese SHDSL-Verbindung genutzt werden, muss zunächst der bestehende Verbund aufgelöst werden.</p>
Vorgegebene Übertragungsrate	Nur für Übertragungsrate = <i>Fest eingestellt</i> .

Feld	Beschreibung
	Wählen Sie aus, welche Geschwindigkeit verwendet werden soll.
Leitungsgeschwindigkeitsintervall	Nur für Übertragungsrate = <i>Adaptiv</i> . Wählen Sie in Minimum die minimale Übertragungsrate und in Maximum die maximale Übertragungsrate der Verbindung aus.

6.6 Serielle Ports

6.6.1 Optionen

Im Menü **Serielle Ports** konfigurieren Sie die serielle WAN Schnittstelle Ihres Gateways.

Ihr Gateway bietet eine integrierte X.21/V.35-Schnittstelle.

Die Schnittstelle kann gemäß verschiedener elektrischer Standards (X.21, V.35, ...) betrieben werden. Anhand des eingesteckten Kabels kann der zu verwendende elektrische Standard und der Schicht-1-Betriebsmodus (DTE oder DCE) automatisch erkannt werden. Beide Parameter können Sie aber auch manuell einstellen. Geeignete Kabel können Sie über Ihren Händler beziehen.

Wählen Sie die Schaltfläche , um die Konfiguration des Serial Ports zu bearbeiten.



The screenshot shows the configuration page for the bintec R4300 gateway. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'Serielle Ports' option is highlighted. The main content area is titled 'Optionen' and contains a table for 'Serielle Parameter'.

Serielle Parameter	
Schnittstelle	Serial0
Erkennungsmodus	Schnittstelle und Anschluss
Schnittstellentyp	Unbekannt (Automatisch ermittelt)
Verbindungstyp	Unbekannt (Automatisch ermittelt)
Layer-2-Modus	<input type="radio"/> DTE <input type="radio"/> DCE <input checked="" type="radio"/> Automatisch
Interface Leads	<input type="checkbox"/> Aktiviert

At the bottom of the configuration area, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 84: Physikalische Schnittstellen -> Serielle Ports -> Optionen -> 

Das Menü **Physikalische Schnittstellen** -> **Serielle Ports** -> **Optionen** ->  besteht aus folgenden Feldern:

Felder im Menü Optionen Serielle Parameter

Feld	Beschreibung
Schnittstelle	Zeigt den Namen der seriellen Schnittstelle an.
Erkennungsmodus	<p>Definieren Sie, ob die verwendeten Schnittstellen und Verbindungstypen automatisch erkannt (autodetected) oder manuell gesetzt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Schnittstelle und Anschluss</i> (Standardwert): Schnittstellen und Verbindungstypen werden automatisch erkannt. • <i>Schnittstelle</i>: Nur der Schnittstellentyp wird automatisch erkannt. Der Verbindungstyp muß manuell gesetzt werden. • <i>Anschluss</i>: Nur der Verbindungstyp wird automatisch erkannt. Der Schnittstellentyp muß manuell gesetzt werden. • <i>Manuell</i>: Sowohl Schnittstellen- als auch Verbindungstyp müssen manuell gesetzt werden.
Schnittstellentyp	<p>Definieren Sie den Schnittstellentyp des genutzten Ports.</p> <p>Wenn Sie im Feld Erkennungsmodus <i>Schnittstelle und Anschluss</i> oder <i>Schnittstelle</i> wählen, wird der Schnittstellentyp automatisch erkannt. Der erkannte Wert wird angezeigt, z. B. <i>V.35 (autodetected)</i>.</p> <p>Wenn Sie im Feld Erkennungsmodus <i>Anschluss</i> oder <i>Manuell</i> wählen, müssen Sie das Feld Schnittstellentyp manuell setzen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i>: Der Port wird nicht genutzt. • <i>X.21 mit Abschluss</i>: V.11 auf allen Leitungen, 120 Ohm Abschlußwiderstand an kritischen Eingangsleitungen. • <i>V.35</i>: V.35 auf kritischen Leitungen, V.28 auf unkritischen Leitungen. • <i>V.36</i>: V.11 auf kritischen Leitungen, V.10 auf unkritischen Leitungen. • <i>X.21 bis</i>: V.28 auf allen Leitungen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>X.21 ohne Abschluss</i>: Nicht terminiertes V.11 auf allen Leitungen. • <i>RS-449</i>: V.11 auf kritischen Leitungen, V.10 auf unkritischen Leitungen (9-polige oder 37-polige Sub- D-Steckverbindung). • <i>RS-530</i>: V.11 auf kritischen Leitungen, V.10 auf unkritischen Leitungen (25-polige Sub-D-Steckverbindung). • <i>RS-530a</i>: V.11 auf kritischen Leitungen, V.10 auf unkritischen Leitungen inkl. DTR und DSR (25-polige Sub-D-Steckverbindung).
Verbindungstyp	<p>Definieren Sie den Verbindungstyp des genutzten Ports.</p> <p>Wenn Sie im Feld Erkennungsmodus <i>Schnittstelle und Anschluss</i> oder <i>Anschluss</i> wählen, wird der Verbindungstyp automatisch erkannt. Der erkannte Wert wird angezeigt, z. B. <i>Unbekannt (Automatisch ermittelt)</i>.</p> <p>Wenn Sie im Feld Erkennungsmodus <i>Schnittstelle</i> oder <i>Manuell</i> wählen, müssen Sie das Feld Verbindungstyp manuell setzen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DTE</i>: Die Pins sind als DTE-Schnittstelle belegt. Diese Einstellung ist z. B. notwendig, wenn der Router an ein öffentliches Datennetz wie Datex-P angeschlossen ist. • <i>DCE</i>: Die Pins sind als DCE-Schnittstelle belegt.
Layer-2-Modus	<p>Definieren Sie den Wert des HDLC-Adressfelds in gesendeten Kommando-Frames (Schicht 2).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch</i> (Standardwert): Die für Anschluss getroffene Auswahl wird übernommen. In der Regel können Sie diese Einstellung übernehmen, z. B. auch bei Zugang zu einem öffentlichen Datennetz (z. B. Datex-P). • <i>DTE</i>: Das Adressfeld hat den Wert für DTE. • <i>DCE</i>: Das Adressfeld hat den Wert für DCE.
Interface Leads	<p>Legen Sie fest, ob das Gateway den Status der Schnittstellenleitung überprüft. Bei beiden Verbindungspartnern sollte der</p>

Feld	Beschreibung
	<p>gleiche Wert eingestellt sein.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktiviert</i>: Auf der Signalleitung (I bei X.21, CTS bei V.35) wird die Schicht-1-Signalisierung der Gegenstelle überprüft. Die Überprüfung beeinflusst die Variable L1State entsprechend. • <i>Deaktiviert</i> (Standardwert): Die Schicht-1-Signalisierung der Gegenstelle wird nicht überprüft; Ihr Gateway geht davon aus, dass die physikalische Leitung immer "up" ist. Bei dieser Einstellung sollten Sie die Schnittstellenleitung auf andere Weise überwachen, z. B. durch PPP-Keepalive.

6.7 UMTS / HSDPA

6.7.1 UMTS / HSDPA / HSUPA

Im Menü UMTS / HSDPA / HSUPA konfigurieren Sie die Anbindung eines UMTS-Card-Bus-Modems.

R1200wu ist mit automatischem ISDN Backup und UMTS / HSDPA Option ausgestattet.

The screenshot shows the configuration interface for a bintec R1200 device. The top navigation bar includes 'Sprache' (Deutsch), 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. A sidebar on the left lists various configuration categories, with 'UMTS/HSDPA' selected. The main content area is titled 'UMTS/HSDPA/HSUPA' and contains a 'Grundeinstellungen' section with the following parameters:

Grundeinstellungen	
UMTS/HSDPA/HSUPA-Status	<input checked="" type="checkbox"/> Aktiviert
Netzwerkqualität	-113 dBm
Eingehender Dienstyp	<input type="radio"/> Deaktiviert <input type="radio"/> ISDN-Login <input checked="" type="radio"/> PPP-Einwahl
SIM-Karte verwendet PIN:	<input type="text"/>
Initialisierungssequenz des Modems	<input type="text"/>
APN (Name des Access-Points)	<input type="text"/>

At the bottom of the configuration area are two buttons: 'OK' and 'Abbrechen'.

Abb. 85: Physikalische Schnittstellen ->UMTS / HSDPA -> UMTS / HSDPA / HSUPA

Das Menü **Physikalische Schnittstellen** -> **UMTS / HSDPA** -> **UMTS / HSDPA / HSUPA** besteht aus folgenden Feldern:

Felder im Menü **UMTS / HSDPA / HSUPA** Grundeinstellungen

Feld	Beschreibung
UMTS/HSD-PA/HSUPA-Status	<p>Wählen Sie aus, ob UMTS/HSDPA/HSUPA auf Ihrem Gerät aktiviert werden soll oder nicht.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Netzwerkqualität	<p>Nur für UMTS/HSDPA/HSUPA-Status = <i>Aktiviert</i></p> <p>Zeigt die aktuelle Qualität der UMTS-Verbindung an. Der Wert kann nicht verändert werden.</p>
Eingehender Dienstyp	<p>Nur für UMTS/HSDPA/HSUPA-Status = <i>Aktiviert</i></p> <p>Wählen Sie aus, welchem Subsystem des Gateways ein über das Modem eingehender Ruf zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>ISDN Login</i>(Standardwert): Der Ruf wird dem ISDN-Login-Subsystem zugewiesen. • <i>PPP-Einwahl</i>: Der Ruf wird dem PPP-Subsystem zugewiesen. • <i>Deaktiviert</i>: Es erfolgt keine Rufannahme.
SIM-Karte verwendet PIN	<p>Nur für UMTS/HSDPA/HSUPA-Status = Init Sequence <i>Aktiviert</i></p> <p>Geben Sie die PIN Ihrer UMTS-Modemkarte ein.</p> <p>Beachten Sie: Die Eingabe einer falschen PIN unterbindet die Kommunikation bis der Eintrag korrigiert wird.</p>
Initialisierungssequenz des Modems	<p>Nur für UMTS/HSDPA/HSUPA-Status = <i>Aktiviert</i></p> <p>Sie können einen Initialisierungsstring für Ihr Modem eingeben. Bei Bedarf können Sie weitere AT-Befehle durch Semikola getrennt anhängen. Die Eingabe ist auf 80 Zeichen begrenzt.</p>
APN (Name des Access	<p>Nur für UMTS/HSDPA/HSUPA-Status = <i>Aktiviert</i></p>

Feld	Beschreibung
Points)	<p>Wenn GPRS/UMTS benutzt werden soll, müssen Sie hier den sogenannten Access Point Name eintragen, den Sie von Ihrem Provider erhalten haben. Maximal können 80 Zeichen eingegeben werden.</p> <p>Wird hier nichts oder ein falscher APN angegeben, so funktioniert eine konfigurierte GPRS/UMTS-Verbindung nicht.</p>

Kapitel 7 LAN


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

7.1 IP-Konfiguration

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

7.1.1 Schnittstellen

In Menü **LAN IP-Konfiguration Schnittstellen** werden die vorhandenen IP-Schnittstellen aufgelistet. Sie haben die Möglichkeit, die IP-Konfiguration der Schnittstellen zu bearbeiten oder virtuelle Schnittstelle für Spezialanwendungen anzulegen. Hier werden auch Schnittstellen, nachdem sie in den Subsystemen erstellt (Drahtlosnetzwerke, Bridge-Links, WDS-Links), und dann im Menü **Systemverwaltung Schnittstellenmodus/Bridge-Gruppen Schnittstellen** in den Routing-Modus gesetzt wurden, 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.

Standardmäßig sind alle vorhandenen Schnittstellen Ihres Geräts im Bridging-Modus. Die Bridge-Gruppe **br0** ist mit der IP-Adresse `192.168.0.254` mit Netzmaske `255.255.255.0` vorbelegt ist.

Beispiel Teilnetze

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

7.1.1.1 Bearbeiten/Neu


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



Abb. 86: LAN -> IP-Konfiguration -> Schnittstellen -> Bearbeiten/Neu

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

Felder im Menü Schnittstellen Basisparameter

Feld	Beschreibung
Basierend auf Ethernet-Schnittstelle	<p>Dieses Feld wird nur angezeigt, wenn eine virtuelle Routing-Schnittstelle bearbeitet wird.</p> <p>Wählen Sie die Ethernet-Schnittstelle aus, zu der die virtuelle Schnittstelle konfiguriert werden soll.</p>
Adressmodus	<p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse/Netzmaske zugewiesen. • <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-

Feld	Beschreibung
	Adresse.
IP-Adresse / Netzmaske	<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>Wählen Sie den Konfigurationsmodus der Schnittstelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Manuell</i> (Standardwert): Die Schnittstelle wird keinem speziellen Verwendungszweck zugeordnet. • <i>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>Manuell</i></p> <p>Ist Voreingestellte verwenden aktiviert (Standardeinstellung) wird die mit der Schnittstelle verbundene MAC-Adresse verwendet. 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 (sie können jedoch geändert werden). Mit übernehmen Sie die vorgegebene MAC-Adresse.</p>
VLAN ID	<p>Nur für Schnittstellenmodus = <i>VLAN</i></p> <p>Diese Option gilt nur für Routing-Schnittstellen. Weisen Sie die Schnittstelle einem VLAN zu, indem Sie die VLAN-ID des entsprechenden VLANs eingeben.</p> <p>Mögliche Werte sind 0 (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>
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>

7.2 VLAN

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

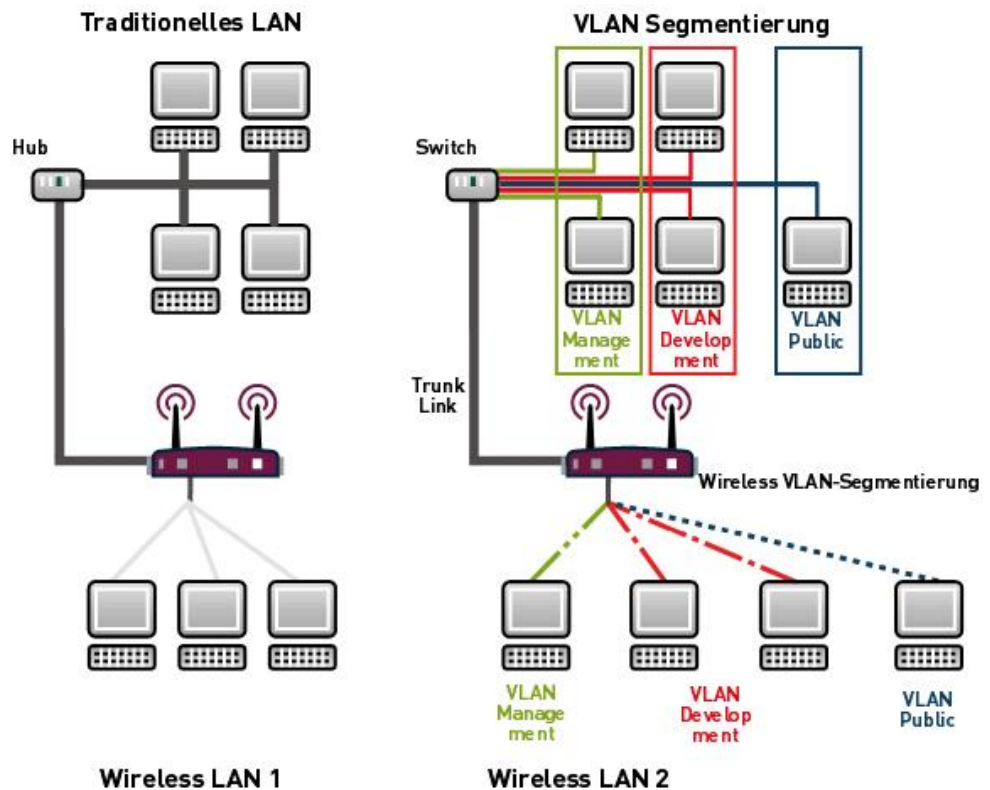


Abb. 87: VLAN-Segmentierung

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. Dieses definieren Sie über die Parameter **Schnittstellenmodus** = *VLAN* und das Feld **VLAN ID** VLANs im Menü **LAN** -> **IP-Konfiguration** -> **Schnittstellen** -> **Neu**.

7.2.1 VLANs

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

7.2.1.1 Bearbeiten/Neu


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



Abb. 88: LAN ->VLAN-> VLANs -> Bearbeiten/Neu

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

Felder im Menü VLANs VLAN konfigurieren

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

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

7.2.2 Portkonfiguration

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

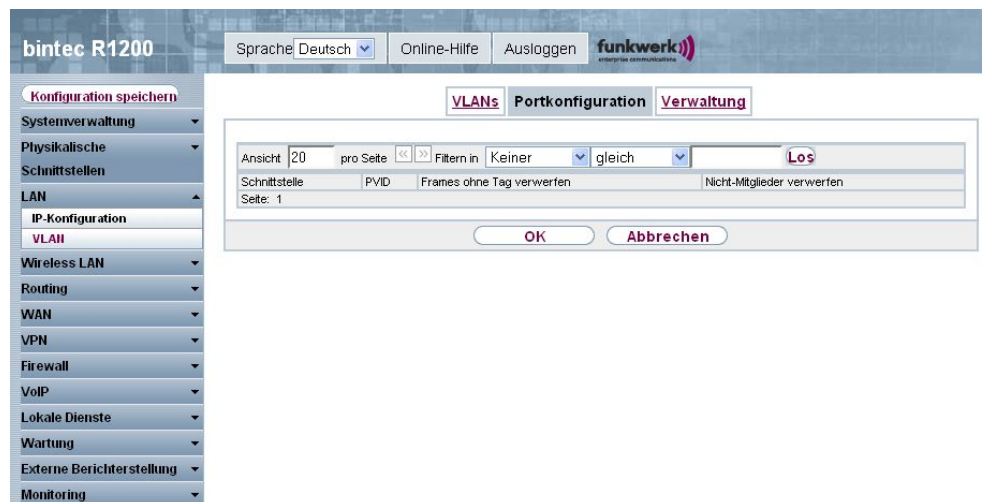


Abb. 89: LAN -> VLAN -> Portkonfiguration

Das Menü LAN -> VLAN -> 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.

7.2.3 Verwaltung

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

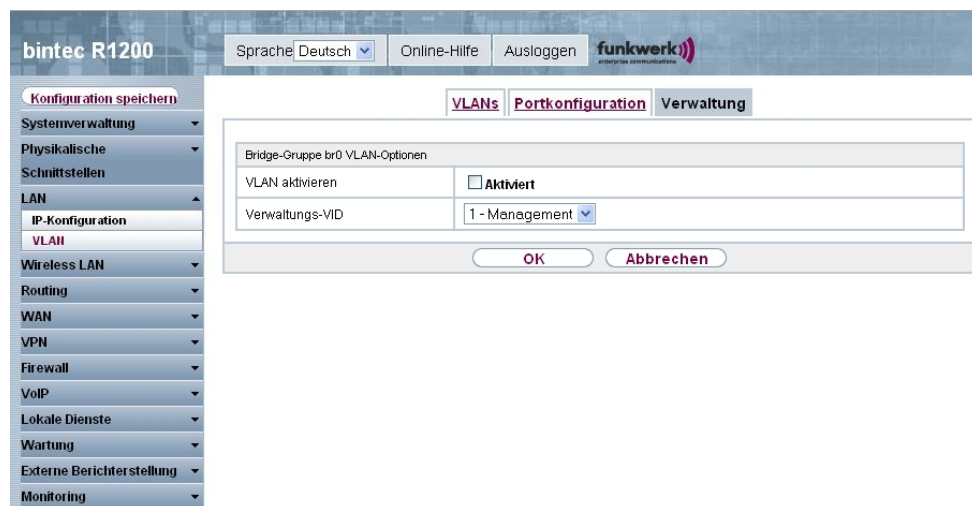


Abb. 90: LAN -> VLAN -> Verwaltung

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

Felder im Menü Verwaltung 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>Geben Sie die VLAN ID des VLANs an, in dem Ihr Gerät arbeiten soll.</p>

Kapitel 8 Wireless LAN

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

Netzwerkfunktionen

Ein WLAN ermöglicht genauso wie ein kabelgebundenes Netzwerk alle wesentlichen Netzwerkfunktionen. Somit steht der Zugriff auf Server, Dateien, Drucker, 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 Frequenzbereich 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.

8.1 WLAN1

Im Menü **Wireless LAN** -> **WLAN1** können Sie alle WLAN-Module Ihres Geräts konfigurieren.

Je nach Modellvariante sind ein oder zwei WLAN-Module, **WLAN1** und ggf. **WLAN2**, verfügbar.

8.1.1 Einstellungen Funkmodul

Im Menü **Wireless LAN** -> **WLAN1** -> **Einstellungen Funkmodul** wird eine Übersicht über alle Konfigurationsoptionen des WLAN-Moduls angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with 'Wireless LAN' expanded to show 'WLAN1' and 'Verwaltung'. The main content area is titled 'Einstellungen Funkmodul' and contains a table with the following data:


Einstellungen Funkmodul						
MAC-Adresse	Betriebsmodus	Frequenzband	Kanal	Maximale Bitrate	Sendeleistung	Status
	Aus	2,4 GHz	Auto	Auto	17 dBm	

Abb. 91: **Wireless LAN** -> **WLAN1** -> **Einstellungen Funkmodul**

8.1.1.1 Einstellungen Funkmodul

In diesem Menü ändern Sie die Einstellungen des Funkmoduls.

Wählen Sie die Schaltfläche , um die Konfiguration zu bearbeiten.

bintec R1200 Sprache Deutsch 

Konfiguration speichern

Einstellungen Funkmodul

WLAN-Einstellungen


Funkmodul	<input checked="" type="checkbox"/> Aktiviert
Betriebsmodus	Einen auswählen <input type="button" value="v"/>
Frequenzband	2.4 GHz In/Outdoor <input type="button" value="v"/>
Kanal	Auto <input type="button" value="v"/>
Antenna Diversity	<input checked="" type="checkbox"/> Aktiviert
Max. Link-Entfernung	<input checked="" type="checkbox"/> Benutze Standard
Sendeleistung	Max. <input type="button" value="v"/>

Performance-Einstellungen

Drahtloser Modus	802.11 mixed <input type="button" value="v"/>
Max. Übertragungsrate	Auto <input type="button" value="v"/>
Nitro Modus	<input checked="" type="checkbox"/> Aktiviert
Nitro XM	<input type="checkbox"/> Frame Compression <input checked="" type="checkbox"/> Frame Concatenation <input checked="" type="checkbox"/> Piggyback Acknowledge <input checked="" type="checkbox"/> Direct Link

Erweiterte Einstellungen

Beacon Period	100 <input type="text"/> ms
DTIM Period	2 <input type="text"/>
RTS Threshold	Immer inaktiv <input type="button" value="v"/>
Short Retry Limit	7 <input type="text"/>
Long Retry Limit	4 <input type="text"/>
Fragmentation Threshold	2346 <input type="text"/> Bytes
ED Threshold	0 <input type="text"/>
CW Min.	15 <input type="text"/>
CW Max.	1023 <input type="text"/>
Max. Receive Lifetime	512 <input type="text"/> ms
Max. Transmit MSDU Lifetime	512 <input type="text"/> ms

Abb. 92: Wireless LAN -> WLAN1 -> Einstellungen Funkmodul -> 

Das Menü **Wireless LAN -> WLAN1 -> Einstellungen Funkmodul ->**  besteht aus den folgenden Feldern:

Felder im Menü Einstellungen Funkmodul WLAN-Einstellungen

Feld	Beschreibung
Funkmodul	Wählen Sie aus, ob Sie das Funkmodul aktivieren möchten. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

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>Einen auswählen</i> (Standardwert): Das Funkmodul ist ausgeschaltet. • <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.
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</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 In/Outdoor</i>: Ihr Gerät wird mit 5 GHz (Mode

Feld	Beschreibung
	<p>802.11a/h) innerhalb oder außerhalb von Gebäuden betrieben.</p> <p>Für Betriebsmodus = <i>Access Client</i></p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>2.4 und 5 GHz</i> • <i>5 und 2.4 GHz</i>(Standardwert) • <i>5 GHz</i> • <i>2.4 GHz</i>
Nutzungsbereich	<p>Nur für Betriebsmodus = <i>Access Client</i>, Client-Modus = <i>Infrastruktur</i> und Frequenzband = <i>2.4 und 5 GHz, 5 und 2.4 GHz</i> oder <i>5 GHz</i></p> <p>Wählen Sie aus, an welchem Standort das Gerät betrieben wird.</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>

Feld	Beschreibung
	<p>Access Point Modus:</p> <p>Durch das Einstellen des Netzwerknamens (SSID) im Access Point Modus werden Funknetze zwar logisch voneinander getrennt, können sich aber physisch immer noch behindern, falls sie auf denselben bzw. zu nah nebeneinander liegenden Funkkanälen arbeiten. Falls Sie also zwei oder mehr Funknetze mit geringem Abstand betreiben, ist es ratsam, den Netzen verschiedene Kanäle zuzuweisen. Diese sollten jeweils mindestens 4 Kanäle auseinanderliegen, da ein Netz auch die benachbarten Kanäle teilweise mitbelegt.</p> <p>Im Falle der manuellen Kanalauswahl vergewissern Sie sich bitte vorher, ob die entsprechenden Clients diese Kanäle auch unterstützen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>2.4 GHz In/Outdoor</i> Mögliche Werte sind <i>1</i> bis <i>13</i> und <i>Auto</i>(Standardwert). • Für Frequenzband = <i>5 GHz Indoor</i> Mögliche Werte sind <i>36, 40, 44, 48</i> und <i>Auto</i> (Standardwert) • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz Indoor</i> Hier ist nur die Option <i>Auto</i> möglich. <p>Access Client Modus:</p> <p>Im Access Client Modus können Sie nur im Client-Modus = Ad-Hoc den erforderlichen Kanal auswählen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • Für Frequenzband = <i>2.4 GHz In/Outdoor</i> Mögliche Werte sind <i>1</i> bis <i>13</i> und <i>Auto</i>(Standardwert). • Für Frequenzband = <i>5 GHz Indoor</i> Mögliche Werte sind <i>36, 40, 44, 48</i> und <i>Auto</i> (Standardwert) • Für Frequenzband = <i>5 GHz In/Outdoor</i> und <i>5 GHz In-</i>

Feld	Beschreibung
	<p><i>door</i></p> <p>Hier ist nur die Option <i>Auto</i> möglich.</p>
Antenna Diversity	<p>Wählen Sie aus, wieviele und welche Antennen zum Senden und Empfangen verwendet werden.</p> <p>Ist die Funktion deaktiviert, sendet und empfängt nur die Hauptantenne.</p> <p>Ist die Funktion aktiviert, empfangen zwei Antennen und das bessere Signal wird ausgewertet.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiviert.</p>
Max. Link-Entfernung	<p>Geben Sie die maximale Link-Entfernung ein.</p> <p>Ist die Option <i>Benutze Standard</i> aktiviert, wird die automatisch generierte Entfernung übernommen.</p> <p>Ist die Option nicht aktiviert, geben Sie den gewünschten Maximalwert in das Eingabefeld in m ein.</p> <p>Standardmäßig ist die Option <i>Benutze Standard</i> aktiviert.</p>
Sendeleistung	<p>Wählen Sie den Maximalwert der abgestrahlten Antennenleistung. Die tatsächlich abgestrahlte Antennenleistung kann abhängig von der übertragenen Datenrate auch niedriger liegen als der eingestellte Maximalwert. Der Maximalwert der verfügbaren Sendeleistung ist länderabhängig.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>max.</i> (Standardwert): Die maximale Antennenleistung wird verwendet. • <i>Benutzerdefiniert</i>: Geben Sie den gewünschten Maximalwert in das Eingabefeld in dBm ein. • <i>2 mW 3 dBm</i> • <i>5 mW 7 dBm</i> • <i>10 mW 10 dBm</i> • <i>40 mW 16 dBm</i>

Felder im Menü Einstellungen Funkmodul Performance-Einstellungen

Feld	Beschreibung
Drahtloser Modus	<p>Nur für Frequenzband = 2,4 GHz In/Outdoor</p> <p>Wählen Sie die Wireless-Technologie aus, die der Access-Point anwenden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>11g</i>: Ihr Gerät arbeitet ausschließlich nach 802.11g. 802.11b-Clients können nicht zugreifen. • <i>11b</i>: Ihr Gerät arbeitet ausschließlich nach 802.11b und zwingt alle Clients dazu, sich anzupassen. • <i>802.11 mixed</i> (Standardwert) / <i>802.11 mixed-short</i>: Ihr Gerät passt sich der Technologie der Clients an. Für mixed-short gilt: Die Datenraten 5.5 und 11 Mbit/s müssen von allen Clients unterstützt werden (Basic Rates). • <i>802.11 mixed-long</i>: Ihr Gerät passt sich der Technologie der Clients an. 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.
Max. Übertragungsrate	<p>Wählen Sie die Übertragungsgeschwindigkeit aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Automatisch erkennen</i> (Standardwert): Die Übertragungsgeschwindigkeit wird automatisch ermittelt. • <i>1, 2, 5, 6, 9, 11, 12, 18, 24, 36, 48, 54 MBit/s</i>
Nitro Modus	<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>

Feld	Beschreibung
Nitro XM	<p>Die Funktion Nitro XM (eXtreme Multimedia) kann durch Kombination von Protection (vermeidet Kollisionen in Funkzellen mit 11g- und 11b-Clients), Packet Bursting (Senden mehrerer Datenpakete in einem Rutsch; unter dem Namen Nitro bereits eingeführt), Kompression und Concatenation (kombiniert mehrere kleine zu einem größeren WLAN-Paket) den Durchsatz steigern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Frame Compression</i>: Wenn diese Funktion eingeschaltet ist, werden gesendete Daten komprimiert. Das funktioniert nur in Verbindung mit Clients, die Conexant-Funkkarten benutzen. Der erzielte Gewinn an Übertragungsgeschwindigkeit ist stark von der Art der übertragenen Daten abhängig. • <i>Frame Concatenation</i>: Wenn diese Funktion eingeschaltet ist, werden mehrere kurze Datenpakete zu längeren zusammengefasst. Das funktioniert nur in Verbindung mit Clients, die Conexant-Funkkarten benutzen. • <i>Piggyback Acknowledge</i>: Wenn diese Funktion eingeschaltet ist, wird die Bestätigung für empfangene Pakete ("ACK") mit anderen gesendeten Paketen kombiniert. Das funktioniert nur in Verbindung mit Clients, die Conexant-Funkkarten benutzen. • <i>Direct Link</i>: Wenn "Direct link" eingeschaltet ist, können angemeldete Clients direkt, ohne Umweg über den Access Point, Daten austauschen. Das funktioniert nur in Verbindung mit Clients, die Conexant-Funkkarten benutzen. <p>Standardmäßig sind <i>Frame Concatenation</i>, <i>Piggyback Acknowledge</i> und <i>Direct Link</i> aktiviert.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Beacon Period	<p>Nur für Betriebsmodus = <i>Access-Point</i> oder <i>Select one</i>.</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 über-</p>

Feld	Beschreibung
	<p>mittelt.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Standardwert ist 100 msec.</p>
DTIM Period	<p>Nur für Betriebsmodus = <i>Access-Point</i> oder <i>Einen auswählen</i>.</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- 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) 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 werden, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.</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</p>

Feld	Beschreibung
	<p>Datenpakets ein, der länger ist als der in RTS Threshold definierten 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 maximale Grösse an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Wert 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>
ED Threshold	<p>Legen Sie den Energy Detection Schwellenwert für CCA (Clear Channel Assessment) fest.</p> <p>Mögliche Werte sind -2147483648 bis 2147483647</p> <p>Der Standardwert ist 0.</p>
CW Min	<p>Legen Sie die maximale Größe des Contention Window fest.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 15 .</p>
CW Max	<p>Legen Sie die Mindestgröße des Contention Window fest.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 1023 .</p>
Max Receive Lifetime	<p>Geben Sie die Zeit nach dem initialen Empfangen des ersten Fragments eines Datenpakets ein, nach deren Ablauf keine weiteren Versuche unternommen werden. Das Datenpaket wird verworfen.</p> <p>Mögliche Werte sind 1 bis 4294967295.</p> <p>Der Standardwert ist 512 msec.</p>
Max Transmit MSDU Li-	<p>Geben Sie die Zeit nach dem initialen Senden des ersten Frag-</p>

Feld	Beschreibung
fetime	<p>ments eines Datenpakets ein, nach deren Ablauf keine weiteren Senderversuche unternommen werden. Das Datenpaket wird verworfen.</p> <p>Mögliche Werte sind 1 bis 4294967295.</p> <p>Der Standardwert ist 512 msec.</p>

Felder im Menü Erweiterte Einstellungen Client Mode

Feld	Beschreibung
Kanäle scannen	<p>Nur für Betriebsmodus = <i>Access Client</i></p> <p>Wählen Sie aus, auf welchen Kanälen der WLAN-Client automatisch nach verfügbaren Drahtlosnetzwerken scannen soll.</p> <p>Standardmäßig ist die Funktion aktiv. Damit wird auf allen Kanälen gescannt. Wird die Funktion deaktiviert, können unter Ausgewählte Kanäle die gewünschten Kanäle festgelegt werden.</p>
Ausgewählte Kanäle	<p>Nur für Kanäle scannen = <i>deaktiviert</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



Feld	Beschreibung
	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 ms</i>.</p>
Channel Sweep	<p>Zeigt an, wieviele Frequenzen im Hintergrund gescannt werden sollen.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>2</i>. Der Wert <i>0</i> deaktiviert den Scan im Hintergrund. Der Wert <i>-1</i> aktiviert den Scan aller verfügbarer Frequenzen.</p>
Min. Zeitraum aktiver Scan	<p>Zeigt an, wieviel Zeit in Millisekunden eine Frequenz mindestens aktiv gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>10 ms</i>.</p>
Max. Zeitraum aktiver Scan	<p>Zeigt an, wieviel Zeit in Millisekunden eine Frequenz maximal aktiv gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>40 ms</i>.</p>
Min. Zeitraum passiver Scan	<p>Zeigt an, wieviel Zeit in Millisekunden eine Frequenz mindestens passiv gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>20 ms</i>.</p>
Max. Zeitraum passiver Scan	<p>Zeigt an, wieviel Zeit in Millisekunden eine Frequenz maximal aktiv gescannt wird.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist <i>120 ms</i>.</p>

Feld	Beschreibung
Association Advantage	<p>Zeigt an, welche Priorität das BSS hat, mit dem der WLAN-Client aktuell verbunden ist.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 10.</p>
RSSI Advantage	<p>Zeigt an, welche Priorität der Indikator für die Signalstärke (RSSI) des BSS hat.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 10.</p>
Weight of Age	<p>Zeigt die Priorität des Alters des BSS an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 5.</p>
Weight of Penalty	<p>Zeigt die Priorität des Penalty des BSS an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 10.</p>
Penalty-Wert	<p>Zeigt den Wert des Penalty des BSS an.</p> <p>Der Wert kann nur für Roaming-Profil = <i>Benutzerdefiniertes Roaming</i> verändert werden. Der Standardwert ist 50.</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 das 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 werden, indem die Werte <i>Immer aktiv</i> bzw. <i>Immer inaktiv</i> (Standardwert) ausgewählt werden.</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>

Feld	Beschreibung
Long Retry Limit	<p>Geben Sie die maximale Anzahl von Sendeversuchen eines Datenpakets ein, der länger ist als der in RTS Threshold definierten 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 maximale Grösse an, ab der Datenpakete fragmentiert (d.h. in kleinere Einheiten aufgeteilt) werden. Niedrige Wert 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>
ED Threshold	<p>Legen Sie den Energy Detection Schwellenwert für CCA (Clear Channel Assessment) fest.</p> <p>Mögliche Werte sind -2147483648 bis 2147483647</p> <p>Der Standardwert ist 0.</p>
CW Min.	<p>Legen Sie die maximale Größe des Contention Window fest.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 15 .</p>
CW Max.	<p>Legen Sie die Mindestgröße des Contention Window fest.</p> <p>Mögliche Werte sind 1 bis 65535.</p> <p>Der Standardwert ist 1023 .</p>
Max. Receive Lifetime	<p>Geben Sie die Zeit nach dem initialen Empfangen des ersten Fragments eines Datenpakets ein, nach deren Ablauf keine weiteren Versuche unternommen werden. Das Datenpaket wird verworfen.</p> <p>Mögliche Werte sind 1 bis 4294967295.</p> <p>Der Standardwert ist 512 msec.</p>

Feld	Beschreibung
Max. Transmit MSDU Lifetime	<p>Geben Sie die Zeit nach dem initialen Senden des ersten Fragments eines Datenpakets ein, nach deren Ablauf keine weiteren Sendeveruche unternommen werden. Das Datenpaket wird verworfen.</p> <p>Mögliche Werte sind 1 bis 4294967295.</p> <p>Der Standardwert ist 512 msec.</p>

8.1.2 Drahtlosnetzwerke (VSS)

Wenn Sie Ihr Gerät im Access Point Modus betreiben (**Wireless LAN** -> **WLAN1** -> **Einstellungen Funkmodul** ->  -> **Betriebsmodus** = *Access Point*), können Sie im Menü **Wireless LAN** -> **WLAN1** -> **Drahtlosnetzwerke (VSS)** ->  -> **Neu** die gewünschten Drahtlosnetzwerke bearbeiten oder neue einrichten.

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 = Verschlüsse-

lung 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 von 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.


WPA2

Die Erweiterung von WPA ist WPA2. In WPA2 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 (**ACL Modus** oder **MAC-Filter**). In der Access Control List tragen Sie die MAC-Adressen der Clients ein, die Zugriff auf Ihr Wireless LAN haben dürfen. Alle anderen Clients haben keinen Zugriff.

Sicherheitsmaßnahmen

Zur Absicherung der auf dem WLAN übertragenen Daten sollten Sie im Menü **Wireless LAN** -> **WLAN1** -> **Drahtlosnetzwerke (VSS)** -> **Neu**-> gegebenenfalls folgende Konfigurationsschritte vornehmen:

- Ändern Sie die Zugangspasswörter Ihres Geräts.
- Ändern Sie die Standard-SSID, **Netzwerkname (SSID)** = *Funkwerk-ec*, 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* oder beidem, und tragen Sie den entsprechenden Schlüssel im Access-Point unter **WEP-Schlüssel 1 - 4** oder **Preshared Key** und in den WLAN-Clients ein.
- Der WEP-Schlüssel sollte regelmäßig geändert werden. Wechseln Sie dazu **Übertragungsschlüssel**. Wählen Sie den längeren 104 Bit WEP-Schlüssel.
- Für die Übertragung von extrem sicherheitsrelevanten Informationen sollte **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 auf das 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 Drahtlosnetzwerke (VSS) MAC-Filter* auf Seite 222).

Im Menü **Wireless LAN** -> **WLAN1** -> **Drahtlosnetzwerke (VSS)** wird eine Liste aller WLAN-Netzwerke angezeigt.

8.1.2.1 Drahtlosnetzwerke (VSS) -> Neu/


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

Abb. 93: Wireless LAN -> WLAN1 -> Drahtlosnetzwerke (VSS) -> /Neu

Das Menü **Wireless LAN** -> **WLAN1** -> **Drahtlosnetzwerke (VSS)** -> /Neu besteht aus folgenden Feldern:

Felder im Menü Drahtlosnetzwerke (VSS) 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>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</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 umgewandelt ARP-Broadcasts an die intern bekannten IP-Adressen weitergeleitet werden. Uni-</p>

Feld	Beschreibung
	<p>casts 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>

Felder im Menü Drahtlosnetzwerke (VSS) Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	<p>Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Key • <i>WPA-Enterprise</i>: 802.11i/TKIP
Übertragungsschlüssel	<p>Nur für Sicherheitsmodus = <i>WEP 40</i>, <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>



Feld	Beschreibung
WEP-Schlüssel 1-4	<p>Nur für Sicherheitsmodus = <i>WEP 40</i> , <i>WEP 104</i></p> <p>Geben Sie den WEP-Schlüssel ein.</p> <p>Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen. Z. B. <i>hallo</i> für <i>WEP 40</i>, <i>funkwerk-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 WPA2 wird angewendet.
WPA Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i> und WPA-Modus = <i>WPA</i> oder <i>WPA</i> und <i>WPA2</i></p> <p>Wählen Sie aus welche Verschlüsselungsmethode angewendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): Temporal Key Integrity Protocol. • <i>AES</i>: Advanced Encryption Standard. • <i>AES</i> und <i>TKIP</i> <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als "performanter" gilt.</p>
WPA2 Cipher	<p>Nur für Sicherheitsmodus = <i>WPA-PSK</i></p> <p>und WPA-Modus = <i>WPA2</i> oder <i>WPA</i> und <i>WPA2</i></p> <p>Wählen Sie aus welche Verschlüsselungsmethode angewendet werden soll.</p>

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (Standardwert): Temporal Key Integrity Protocol. • <i>AES</i>: Advanced Encryption Standard. • <i>AES und TKIP</i> <p>Beide Verschlüsselungsmethoden werden als sicher eingestuft, wobei AES als "performanter" gilt.</p>
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>

Felder im Menü Drahtlosnetzwerke (VSS) MAC-Filter

Feld	Beschreibung
ACL-Modus	<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 hier Einträge mit Hinzufügen an und geben Sie die MAC-Adressen der Clients (MAC-Adresse) ein, die zugelassen werden sollen.</p>

8.1.3 WDS Links

Wenn Sie Ihr Gerät im Access Point Modus betreiben (**Wireless LAN** -> **WLANx** -> **Einstellungen Funkmodul** ->  -> **Betriebsmodus** = *Access Point*), können Sie im Menü **Wireless LAN** -> **WLANx** -> **WDS Links** ->  -> **Neu** die gewünschten WDS Links bearbeiten oder neue einrichten.



Wichtig

Wählen Sie den Kanal aus, der verwendet werden soll. Der WDS Link ist nur im 2.4 GHz Band 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 Sicherheitsmethode (WEP40 bzw. WEP104) 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.

8.1.3.1 WDS Links -> Neu


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



Abb. 94: Wireless LAN -> WLANx -> WDS Links ->  ->/Neu

Das Menü **Wireless LAN** -> **WLANx** -> **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> <p>Standardmäßig ist die Option <i>Benutze Standard</i> aktiviert.</p>

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>WEP40</i>: Der Datenverkehr auf diesem WDS Link wird mit

Feld	Beschreibung
	<p>WEP40 verschlüsselt. Geben Sie in WEP Schlüssel 1 - 4 die Schlüssel für diesen WDS-Link ein und wählen Sie in Übertragungsschlüssel den Standard-Schlüssel aus.</p> <ul style="list-style-type: none"> • <i>WEP104</i>: Der Datenverkehr auf diesem WDS Link wird mit WEP104 verschlüsselt. Geben Sie in WEP Schlüssel 1 - 4 die Schlüssel für diesen WDS-Link ein und wählen Sie in Übertragungsschlüssel den Standard-Schlüssel aus.
Übertragungsschlüssel	<p>Nur für Schutz = WEP40 , <i>WEP104</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 Schutz = WEP40 , <i>WEP104</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 <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>WEP40</i> oder 26 Zeichen für <i>WEP104</i> z. B. <i>WEP40: 0xA0B23574C5</i>, <i>WEP104: 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>WEP40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP104</i> mit 13 Zeichen z. B. <i>hallo</i> für <i>WEP40</i>, <i>funkwerk-wep1</i> für <i>WEP104</i>.</p>

Felder im Menü Entfernter Partner

Feld	Beschreibung
Entfernte MAC-Adresse	Geben Sie die MAC-Adresse des WDS-Partners ein.

8.1.4 Client Link


Wenn Sie Ihr Gerät im Access Client Modus betreiben (**Wireless LAN -> WLAN1 -> Einstellungen Funkmodul ->  -> Betriebsmodus = Access Client**), können Sie im Menü **Wireless LAN -> WLAN1 -> Client Links ->  ->** die vorhandenen Client Links bearbeiten.

Der Client-Modus kann im Infrastruktur Modus oder im Ad-Hoc-Modus betri In einem Netz im Infrastruktur Modus kommunizieren alle Clients ausschließlich über Access Points miteinander. Es läuft keine Kommunikation zwischen den einzelnen Clients direkt ab.

eben werden.

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

8.1.4.1 Client Link ->

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten.



The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Wireless LAN', with 'WLAN1' selected and 'Client Link' highlighted. The main content area displays the 'Einstellungen Funkmodul' and 'Client Link' configuration page. The 'Client Link' section contains a form with the following fields:

- Basisparameter**
 - Netzwerkname (SSID):
 - Sicherheitsmodus:

At the bottom of the form are two buttons: 'OK' and 'Abbrechen'.

Abb. 95: **Wireless LAN -> WLAN1 -> Client Link ->  ->**

Das Menü **Wireless LAN -> WLAN1 -> Client Link ->  ->** besteht aus folgenden Feldern:

Felder im Menü Client Link 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 Client Link Sicherheitseinstellungen

Feld	Beschreibung
Sicherheitsmodus	Wählen Sie den Sicherheitsmodus (Verschlüsselung und Authentifizierung) des Drahtlosnetzwerkes aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Weder Verschlüsselung noch Authentifizierung • <i>WEP 40</i>: WEP 40 Bit • <i>WEP 104</i>: WEP 104 Bit • <i>WPA-PSK</i>: WPA Preshared Key
Übertragungsschlüssel	Nur für Sicherheitsmodus = <i>WEP 40</i> , <i>WEP 104</i> Wählen Sie einen der in WEP-Schlüssel <1 - 4> konfigurierten Schlüssel als Standardschlüssel aus. Standardwert ist <i>Schlüssel 1</i> .
WEP-Schlüssel 1-4	Nur für Sicherheitsmodus = <i>WEP 40</i> , <i>WEP 104</i> Geben Sie den WEP-Schlüssel ein. Geben Sie eine Zeichenfolge mit der für den gewählten WEP-Modus passenden Zeichenanzahl ein. Für <i>WEP 40</i> benötigen Sie eine Zeichenfolge mit 5 Zeichen, für <i>WEP 104</i> mit 13 Zeichen z. B. <i>hallo</i> für <i>WEP 40</i> , <i>funkwerk-wep1</i> für <i>WEP 104</i> .
WPA-Modus	Nur für Sicherheitsmodus = <i>WPA-PSK</i> und <i>WPA-Enterprise</i> Wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA 2 (mit AES-Verschlüsselung) oder beides anwenden wollen. Mögliche Werte: <ul style="list-style-type: none"> • <i>WPA</i> (Standardwert): Nur WPA wird angewendet. • <i>WPA 2</i>: Nur WPA2 wird angewendet.

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

8.1.4.2 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**.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar has a menu with 'Wireless LAN' expanded to 'WLAN1'. The main content area is titled 'Einstellungen Funkmodul' and 'Client Link'. It features a 'Scan' button and a table with the following structure:

Scan							
Beschreibung des Client Links		sta1-0					
Aktion		[Scan]					
AP-MAC-Adresse	Netzwerkname (SSID)	Kanal	Modus	Signal	SNR	Verbunden	Aktion

Below the table is a 'Zurück' button.

Abb. 96: **Wireless LAN -> WLAN1 -> 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 lokale 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 -> WLAN1 -> Client Link -> Scan** besteht aus den folgenden Feldern:

Felder im Menü Client Link Scan

Feld	Beschreibung
Beschreibung des Client Links	Zeigt den Namen des von Ihnen konfigurierten Client-Links an.
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.

Feld	Beschreibung
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.
SNR	Zeigt die Qualität des Signals in dBm an.
Verbunden	Zeigt den Status des Links auf Ihrem Client an.
Aktion	Sie können den Status der Client-Links verändern. In diesem Feld werden die zur Verfügung stehenden Aktionen angezeigt.

8.2 Verwaltung

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

8.2.1 Grundeinstellungen

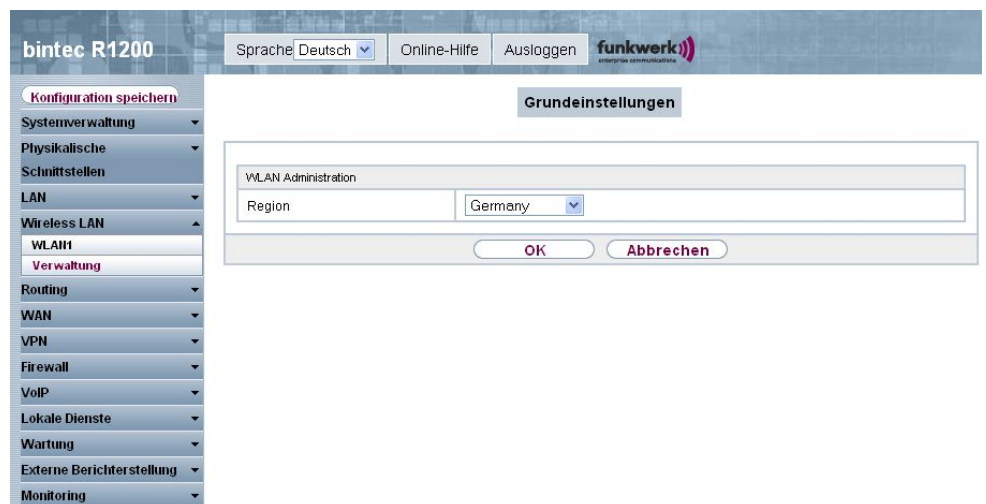


Abb. 97: Wireless LAN -> Verwaltung -> Grundeinstellungen

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

Felder im Menü Grundeinstellungen WLAN Administration

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

Kapitel 9 Routing

9.1 Routen

9.1.1 IP-Routen

Im Menü **Routing** -> **Routen** -> **IP-Routen** wird eine Liste aller konfigurierten Routen angezeigt.

9.1.1.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 router. The left sidebar contains a menu with options like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'HAT', 'RIP', 'Lastverteilung', 'Multicast', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'Routing' menu is expanded, showing 'Routen' as the selected option. The main content area is titled 'IP-Routen' and contains a form for configuring a new route. The form has the following fields:

- Routenklasse:** Includes an 'Erweiterte Route' checkbox (unchecked) and an 'Aktiviert' checkbox (unchecked).
- Routenparameter:**
 - Routentyp:** A dropdown menu set to 'Netzwerkroute'.
 - Ziel-IP-Adresse/Netzmaske:** Two input fields separated by a slash, both empty.
 - Schnittstelle:** A dropdown menu set to 'Keine'.
 - Netzwerktyp:** A dropdown menu set to 'Direkt'.
 - Lokale IP-Adresse:** An input field containing '0.0.0.0'.
 - Metrik:** A dropdown menu set to '1'.

At the bottom of the form are two buttons: 'OK' and 'Abbrechen'.

Abb. 98: **Routing** -> **Routen** -> **IP-Routen** -> **Neu mit Erweiterte Route** = *Nicht aktiviert*

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

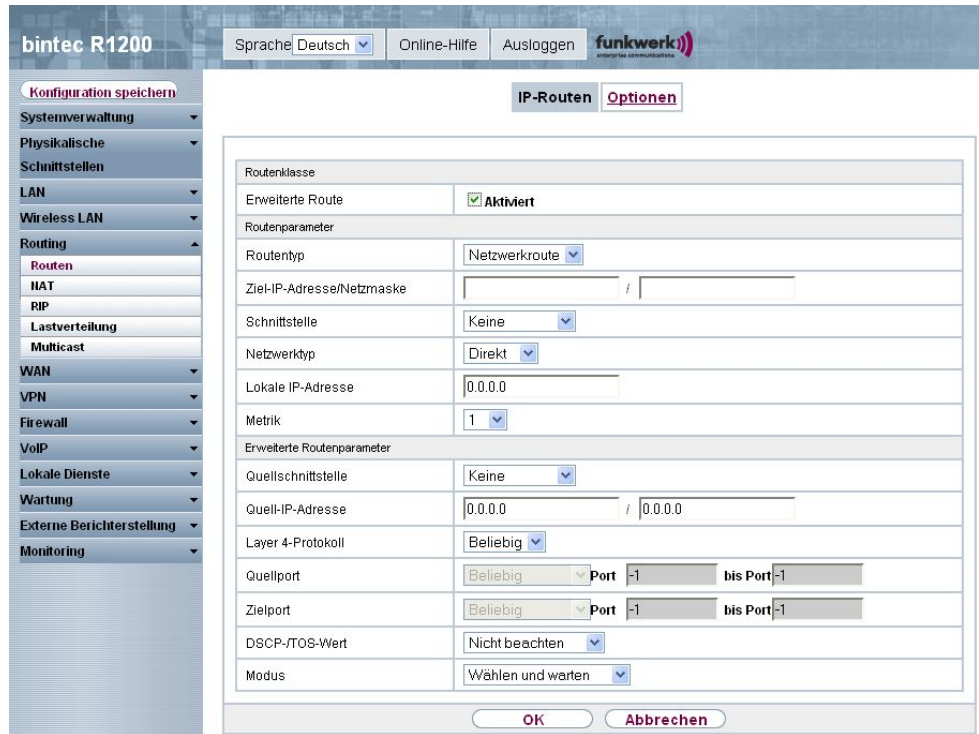


Abb. 99: Routing -> Routen -> IP-Routen -> Neu mit **Erweiterte Route** = *Aktiviert*

Das Menü **Routing -> Routen -> IP-Routen -> Neu** besteht aus folgenden Feldern:

Felder im Menü IP-Routen Routenklasse

Feld	Beschreibung
Erweiterte Route	<p>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 Geräteschnittstelle angelegt.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü IP-Routen Routenparameter

Feld	Beschreibung
Routentyp	Wählen Sie die Art der Route aus.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Netzwerkroute</i> (Standardwert): Route zu einem Netzwerk. • <i>Standardroute</i> : Wird benutzt, wenn keine andere passende Route verfügbar ist. • <i>Hostroute</i> : Route zu einem einzelnen Host.
Ziel-IP-Adresse/Netzmaske	<p>Nur für Routentyp <i>Hostroute</i> oder <i>Netzwerkroute</i></p> <p>Geben Sie die IP-Adresse des Ziel-Hosts ein.</p> <p>Bei Routentyp = <i>Netzwerkroute</i> Geben Sie in das zweite Feld zusätzlich die entsprechende Netzmaske ein. Wenn kein Eintrag erfolgt, benutzt Ihr Gerät eine Standardnetzmaske.</p>
Schnittstelle	<p>Wählen Sie ggf. die Schnittstelle aus, welche für diese Route verwendet werden soll.</p>
Netzwerktyp	<p>Nicht für Routentyp = <i>Standardroute</i></p> <p>Wählen Sie zusätzlich den Netzwerktyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Direkt</i>(Standardwert): <ul style="list-style-type: none"> • im LAN: Sie definieren eine weitere IP-Adresse für die Schnittstelle. • im WAN: Sie definieren eine Route ohne Transitnetzwerk. • <i>Indirekt</i>: <ul style="list-style-type: none"> • im LAN: Sie definieren eine Gateway-Route. • im WAN: Sie definieren eine Route mit Transitnetzwerk.
Lokale IP-Adresse	<p>Nur für Netzwerktyp = <i>Direkt</i></p> <p>Geben Sie die IP-Adresse des Gateways ein, an den Ihr Gerät die IP-Pakete weitergeben soll.</p>
Gateway	<p>Nur für Netzwerktyp = <i>Indirekt</i></p> <p>Geben Sie die IP-Adresse des Hosts ein, an den Ihr Gerät die IP-Pakete weitergeben soll.</p>

Feld	Beschreibung
Metrik	<p>Wählen Sie die Priorität der Route aus.</p> <p>Je niedriger Sie den Wert setzen, desto höhere Priorität besitzt die Route.</p> <p>Wertebereich von 0 bis 15 . Standardwert ist 1</p>

Felder im Menü IP-Routen Erweiterte Routenparameter

Feld	Beschreibung
Quellschnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die Datenpakete das Gerät erreichen sollen.</p> <p>Standardwert ist <i>Keiner</i></p>
Quell-IP-Adresse	Geben Sie die IP-Adresse und Netzmaske des Quell-Hosts bzw. Quell-Netzwerks ein.
Layer 4-Protokoll	<p>Wählen Sie ein Protokoll aus.</p> <p>Mögliche Werte: <i>ICMP , TCP , UDP , GRE , ESP , AH , OSPF , L2TP , BELIEBIG .</i></p> <p>Standardwert ist <i>BELIEBIG</i></p>
Quellport	<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>Priviligiert</i>: Eingabe von privilegierten Port-Nummern: 0 ... 1023. • <i>Server</i>: Eingabe von Server Port-Nummern: 5000 ... 32767. • <i>Clients 1</i>: Eingabe von Client Port-Nummern: 1024 ... 4999.

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

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>DSCP</i>: Es handelt sich um einen Differentiated Services Code Point nach RFC 3260. • <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. <p>Geben Sie für <i>DSCP</i>, <i>TOS-Binärwert</i> und <i>TOS Dezimalwert</i> den entsprechenden Wert ein.</p>
Modus	<p>Wählen Sie aus, wann die in Routenparameter -> Schnittstelle definierte Schnittstelle benutzt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Wählen und warten</i> (Standardwert): Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und warten, bis die Schnittstelle "aktiv" ist. • <i>Verbindlich</i>: Die Route ist immer benutzbar. • <i>Wählen und fortfahren</i>: Die Route ist benutzbar, wenn die Schnittstelle "aktiv" ist. Ist die Schnittstelle "ruhend", dann wählen und solange die Alternative Route benutzen (rerouting), bis die Schnittstelle "aktiv" ist. • <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.

9.1.2 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.

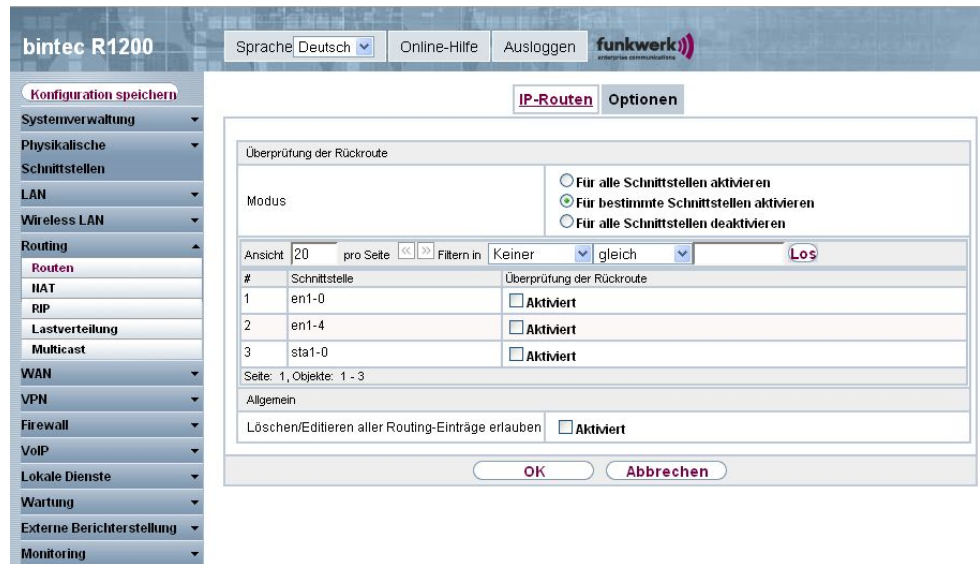


Abb. 100: Routing -> Routen -> Optionen

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

Felder im Menü Optionen 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.
#	<p>Nur für Modus = Für bestimmte Schnittstellen aktivieren</p> <p>Zeigt die laufende Nummer des Listeneintrags an.</p>

Feld	Beschreibung
Schnittstelle	Nür für Modus = <i>Für bestimmte Schnittstellen aktivieren</i> Zeigt den Namen der Schnittstelle an.
Überprüfung der Rückroute	Nür für Modus = <i>Für bestimmte Schnittstellen aktivieren</i> Wählen Sie aus, ob Überprüfung der Rückroute für diese Schnittstelle aktiviert werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion für alle Schnittstellen deaktiviert.

Felder im Menü Optionen Allgemein

Feld	Beschreibung
Löschen/Editieren von allen Routing-Einträgen erlauben	Legen Sie fest, ob alle auf Ihrem Gerät eingetragenen Routen im Menü Routing -> Routen -> Routen editierbar und löschar sein sollen. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion für alle Schnittstellen deaktiviert.

9.2 NAT

9.2.1 NAT-Schnittstellen

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 [Portweiterleitung](#) auf Seite 241).

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

The screenshot shows the configuration page for NAT interfaces on a bintec R1200 router. The interface includes a navigation sidebar on the left and a main configuration area. The main area has a title bar with 'NAT-Schnittstellen' and 'Portweiterleitung'. Below this is a table with the following data:

Schnittstelle	NAT aktiv	Automatische Ablehnung	PPTP-Passthrough	Portweiterleitungen
LAN_EN1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_STA1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Below the table, there are 'OK' and 'Abbrechen' buttons. The page also shows a search filter set to 'Keiner' and a 'Los' button.

Abb. 101: Routing -> NAT -> NAT-Schnittstellen

Für jede NAT-Schnittstelle sind die Optionen *NAT aktiv*, *Automatische Ablehnung* und *PPTP-Passthrough* auswählbar.

Außerdem wird in *Portweiterleitungen* angezeigt, wieviele 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.
Automatische Ablehnung	Wählen Sie aus, ob IP-Pakete stillschweigend durch NAT abgelehnt werden sollen. Ist diese Funktion deaktiviert, wird der Absender der abgelehnten IP-Pakete mit einer entsprechenden ICMP oder TCP RST Nachricht informiert. Standardmäßig ist die Funktion nicht aktiv.
PPTP-Passthrough	Wählen Sie aus, ob auch bei aktiviertem NAT der Aufbau und Betrieb mehrerer gleichzeitiger ausgehender PPTP-Verbindungen von Hosts im Netzwerk erlaubt sein soll. Standardmäßig ist die Funktion nicht aktiv.

Feld	Beschreibung
	Wenn PPTP-Passthrough aktiviert ist, darf Ihr Gerät selber nicht als Tunnel-Endpoint konfiguriert werden.
Portweiterleitungen	Zeigt die Anzahl der in Routing -> NAT -> Portweiterleitung konfigurierten Portweiterleitungsregeln an.

9.2.2 Portweiterleitung

Im Menü **Routing -> NAT -> Portweiterleitung** wird eine Liste aller NAT-Schnittstellen angezeigt, für die Portweiterleitung konfiguriert wurde.

9.2.2.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 router. The left sidebar contains a navigation menu with options like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'Routing' menu is expanded, showing 'Routen', 'NAT', 'RIP', 'Lastverteilung', and 'Multicast'. The 'NAT' menu is further expanded to show 'NAT-Schnittstellen' and 'Portweiterleitung'. The 'Portweiterleitung' configuration page is displayed, featuring a 'Basisparameter' section with the following fields:

- Schnittstelle: Keine
- Datenverkehr auswählen: Dienst: Benutzerdefiniert, Protokoll: Beliebig
- Entsprechender NAT-Eintrag für ausgehende Verbindung: Aktiviert
- Externe IP-Adresse: Auto 255.255.255.255
- Port: -Alle- -1 bis -1
- Entferntes Netzwerk: Aktiviert
- Weiterleiten an: Host zuweisen: IP-Adresse 255.255.255.255
- Zielport: Original -1

At the bottom of the configuration area, there are 'OK' and 'Abbrechen' buttons.

Abb. 102: Routing -> NAT -> Portweiterleitung -> Neu

Das Menü **Routing -> NAT -> Portweiterleitung -> Neu** besteht aus folgenden Feldern:

Felder im Menü Portweiterleitung Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, für die Portweiterleitung konfiguriert werden soll.

Felder im Menü Portweiterleitung Datenverkehr auswählen

Feld	Beschreibung
Dienst	<p>Wählen Sie den Dienst aus, für den bei eingehenden Verbindungen das Adress-Mapping definiert wird.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Benutzerdefiniert</i> (Standardwert) • <i>DNS (UDP)</i> • <i>DNS (TCP)</i> • <i>FTP</i> • <i>HTTP</i> • <i>HTTPS</i> • <i>IMAP</i> • <i>NNTP</i> • <i>POP3</i> • <i>SMTP</i> • <i>SSH</i> • <i>TELNET</i>
Protokoll	<p>Nur für Dienst = <i>Benutzerdefiniert</i></p> <p>Wählen Sie das Protokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> • <i>ICMP</i> • <i>GGP</i> • <i>IP</i> • <i>TCP</i> • <i>EGP</i> • <i>IGP</i> • <i>PUP</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Chaos</i> • <i>UDP</i> • <i>HMP</i> • <i>XNS-IDP</i> • <i>RDP</i> • <i>IPv6</i> • RSVP • <i>GRE</i> • <i>ESP</i> • <i>AH</i> • <i>TLSP</i> • <i>Skip</i> • <i>Kryptolan</i> • <i>ISO-IP</i> • <i>IGRP</i> • <i>OSPF</i> • <i>IPinIP</i> • <i>IPXinIP</i> • <i>VRRP</i> • <i>L2TP</i>
Entsprechender NAT-Eintrag für ausgehende Verbindung	<p>Wählen Sie aus, ob für das Portforwarding ein NAT-Eintrag für ausgehende Verbindungen angelegt werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiviert.</p>
Externe IP-Adresse	<p>Wählen Sie die nach außen hin wirksame (externe) Host- bzw. Netz-IP-Adresse der gewählten Schnittstelle aus.</p> <p>In Standard-Szenarien steht nur eine externe IP-Adresse zur Verfügung. Wählen Sie in diesem Fall die Option Auto.</p> <p>Die Option Auto ist standardmäßig nicht aktiv, sodass Sie die IP-Adresse manuell eingeben können.</p>
Port	Nur für Dienst = <i>Benutzerdefiniert</i>

Feld	Beschreibung
	<p>Wählen Sie zunächst, ob alle Verbindungen zugelassen werden sollen, oder ein bestimmter Port oder Portbereich definiert werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle</i> (Standardwert): Es wird keine Port-Umsetzung durchgeführt. In diesem Fall ist in den Eingabefeldern der Wert <i>-1</i> eingetragen. • <i>Port angeben</i>: Ermöglicht die Eingabe einer Port-Nummer. • <i>Portbereich angeben</i>: Ermöglicht die Eingabe eines Port-Nummern-Bereichs. <p>Geben Sie nun den ursprünglichen Zielport oder Zielport-Bereich (...bis...) der eingehenden IP-Verbindung ein.</p>
Entfernetes Netzwerk	<p>Wählen Sie aus, ob die IP-Pakete an ein Entferntes Netzwerk weitergeleitet werden sollen.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Mit <i>Ja</i> wird die Funktion aktiv.</p>
Entfernte IP-Adresse / Netzmaske	<p>Nur für Entfernetes Netzwerk = <i>Ja</i></p> <p>Geben Sie nun die Remote-IP-Adresse und Netzmaske des Entfernten Netzwerks an.</p>

Felder im Menü Portweiterleitung Weiterleiten an

Feld	Beschreibung
Host zuweisen	<p>Geben Sie die IP-Adresse des internen Hosts oder Netzes ein.</p> <p>Sie haben auch die Möglichkeit, die Option <i>Lokal</i> auszuwählen, wobei dann auf Ihr Gerät selber gemappt wird.</p>
Zielport	<p>Geben Sie den neu gesetzten Zielport der eingehenden IP-Verbindung ein.</p> <p>Wählen Sie aus, ob der Quellport verwendet werden soll, indem Sie die Option Original aktivieren. In diesem Fall ist im Eingabefeld der Portnummer der Wert <i>-1</i> eingetragen. Oder deaktivieren Sie die Option Original und geben Sie eine Portnummer</p>

Feld	Beschreibung
	ein.

9.3 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.

9.3.1 RIP-Schnittstellen

Im Menü **Routing** -> **RIP** -> **RIP-Schnittstellen** wird eine Liste aller RIP-Schnittstellen angezeigt.

bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Systemverwaltung
 Physikalische
 Schnittstellen
 LAN
 Wireless LAN
 Routing
 Routen
 IAT
 RIP
 Lastverteilung
 Multicast
 WAN
 VPN
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

RIP-Schnittstellen RIP-Filter RIP-Optionen

Ansicht 20 pro Seite Filtern in Keiner gleich Los

#	Schnittstelle	Version in Senderichtung	Version in Empfangsrichtung	Routenankündigung
1	en1-0	Keine	Keine	Nur aktiv
2	en1-4	Keine	Keine	Nur aktiv
3	sta1-0	Keine	Keine	Nur aktiv

Seite: 1, Objekte: 1 - 3

Abb. 103: Routing -> RIP -> RIP-Schnittstellen

9.3.1.1 Bearbeiten

Für jede RIP-Schnittstelle sind über das -Menü die Optionen *Version in Senderichtung*, *Version in Empfangsrichtung* und *Routenankündigung* auswählbar.

bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Systemverwaltung
 Physikalische
 Schnittstellen
 LAN
 Wireless LAN
 Routing
 Routen
 IAT
 RIP
 Lastverteilung
 Multicast
 WAN
 VPN
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

RIP-Schnittstellen RIP-Filter RIP-Optionen

RIP-Parameter für: en1-0

Version in Senderichtung	Keine
Version in Empfangsrichtung	Keine
Routenankündigung	Nur aktiv

OK Abbrechen

Abb. 104: Routing -> RIP -> RIP-Schnittstellen ->

Das Menü **Routing** -> **RIP** -> **RIP-Schnittstellen** ->  besteht aus folgenden Feldern:

Felder im Menü RIP-Parameter für: <Schnittstelle>

Feld	Beschreibung
Version in Senderrichtung	<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 (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

Feld	Beschreibung
	<p>RFC 2091 gesendet bzw. empfangen und verarbeitet (Triggered RIP).</p> <ul style="list-style-type: none"> • <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 interface-spezifische RIP-Konfiguration.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <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.

9.3.2 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** = kein Eintrag (dies entspricht der IP-Adresse 0.0.0.0) mit **Netzmaske** = kein Eintrag (dies entspricht 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** = keine Eintrag (dies entspricht der IP-Adresse 0.0.0.0) mit **Netzmaske** = 255.255.255.255


Im Menü **Routing** -> **RIP** -> **RIP-Filter** wird eine Liste aller RIP-Filter angezeigt.


The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische', 'Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. Under 'Routing', 'RIP' is selected. The main content area has three tabs: 'RIP-Schnittstellen', 'RIP-Filter', and 'RIP-Optionen'. Below the tabs is a table with the following structure:

#	Schnittstelle	Richtung	IP-Adresse	Netzmaske	Filterstatus

At the bottom of the table are three buttons: 'Neu', 'OK', and 'Abbrechen'.

Abb. 105: Routing -> 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.

9.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere RIP-Filter einzurichten.

The screenshot shows the configuration interface for the bintec R1200. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Routing' -> 'RIP' -> 'RIP-Filter'. The main content area displays the 'Basisparameter' section with the following fields:

- Schnittstelle:** A dropdown menu currently set to 'Keine'.
- IP-Adresse/Netzmaske:** Two input fields separated by a slash, currently empty.
- Richtung:** Radio buttons for 'Importieren' (selected) and 'Exportieren'.
- Metrik-Offset für Aktive Schnittstellen:** A dropdown menu set to '0'.
- Metrik-Offset für Inaktive Schnittstellen:** A dropdown menu set to '0'.

At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 106: Routing -> RIP -> RIP-Filter -> Neu

Das Menü **Routing -> RIP -> RIP-Filter -> Neu** besteht aus folgenden Feldern:

Felder im Menü RIP-Filter Basisparameter

Feld	Beschreibung
Schnittstelle	Wählen Sie aus, für welche Schnittstelle die zu konfigurierende Regel gilt.
IP-Adresse / Netzmaske	Geben Sie die IP-Adresse und Netzmaske ein, auf welche die Regel angewendet werden soll. Die Adresse kann sowohl im LAN als auch im WAN liegen. Die Regeln für eingehende und ausgehende RIP-Pakete (Importieren oder Exportieren) müssen für dieselbe IP-Adresse getrennt konfiguriert werden. Sie können einzelne Host-Adressen ebenso angeben wie Netz-adressen.
Richtung	Wählen Sie aus, ob das Filter für das Exportieren oder das Im-portieren von Routen gilt. Mögliche Werte: <ul style="list-style-type: none"> • <i>Importieren</i> (Standardwert) • <i>Exportieren</i>

Feld	Beschreibung
Metrik-Offset für Aktive Schnittstellen	<p>Wählen Sie den Wert aus, der der Metrik der Route beim Import hinzugefügt werden soll, wenn der Status der Schnittstelle "Aktiv" ist. Beim Export wird der Wert der exportierten Metrik hinzugefügt, wenn der Status der Schnittstelle "Aktiv" ist.</p> <p>Mögliche Werte sind -16 bis 16.</p> <p>Standardwert ist 0</p>
Metrik-Offset für Inaktive Schnittstellen	<p>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.</p> <p>Mögliche Werte sind -16 bis 16.</p> <p>Standardwert ist 0</p>

9.3.3 RIP-Optionen

The screenshot shows the configuration interface for a bintec R1200 device. The top navigation bar includes the language set to 'Deutsch', 'Online-Hilfe', and 'Ausloggen'. The main menu on the left lists various configuration categories, with 'Routing' expanded to show 'RIP' selected. The 'RIP-Optionen' sub-menu is active, displaying the following settings:

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

Buttons for 'OK' and 'Abbrechen' are located at the bottom of the configuration window.

Abb. 107: Routing-> RIP -> RIP-Optionen

Das Menü **Routing** -> **RIP** -> **RIP-Optionen** besteht aus folgenden Feldern:

Felder im Menü RIP-Optionen Globale RIP-Parameter

Feld	Beschreibung
RIP-UDP-Port	<p>Die Einstellungsmöglichkeit des UDP-Ports, der für das Senden und Empfangen von RIP-Updates verwendet wird, ist lediglich für Testzwecke von Bedeutung. Eine Veränderung der Einstellung kann dazu führen, dass Ihr Gerät auf einem Port sendet und lauscht, den keine weiteren Geräte benutzen. Der Standardwert 520 sollte eingestellt bleiben.</p>
Standardmäßige Routenverteilung	<p>Wählen Sie aus, ob die Standard-Route Ihres Geräts über RIP-Updates propagiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Poisoned Reverse	<p>Wählen Sie das Verfahren zur Verhinderung von Routing-Schleifen.</p> <p>Bei Standard RIP werden die gelernten Routen über alle Schnittstellen mit aktiviertem RIP SENDEN propagiert. Bei Poisoned Reverse propagiert Ihr Gerät jedoch über die Schnittstelle, über die es die Routen gelernt hat, diese mit der Metrik (Next Hop Count) 16 ("Netz ist nicht erreichbar").</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
RFC 2453-Variabler Timer	<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>
RFC 2091-Variabler Timer	<p>Wählen Sie aus, ob für die in RFC 2091 beschriebenen Timer diejenigen Werte verwendet werden sollen, die Sie im Menü Timer für Triggered RIP (RFC 2091) konfigurieren können.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
	Wenn die Funktion nicht aktiv ist, werden für die Timeouts die im RFC vorgesehenen Zeiträume eingehalten.

Felder im Menü RIP-Optionen Timer für RIP V2 (RFC 2453)

Feld	Beschreibung
Aktualisierungstimer	Nur für RFC 2453-Variabler Timer = Aktiviert Nach Ablauf dieses Zeitraums wird ein RIP-Aktualisierung gesendet. Der Standardwert ist 30 (Sekunden).
Routentimeout	Nur für RFC 2453-Variabler Timer = Aktiviert Nach der letzten Aktualisierung einer Route wird der Routentimeout aktiv. Nach dessen Ablauf wird die Route deaktiviert und der Garbage Collection Timer gestartet. Der Standardwert ist 180 (Sekunden).
Garbage Collection Timer	Nur für RFC 2453-Variabler Timer = Aktiviert Der Garbage Collection Timer wird gestartet, sobald der Routentimeout abgelaufen ist. Nach Ablauf dieses Zeitraums wird die ungültige Route aus der IPROUTETABLE gelöscht, sofern keine Aktualisierung für die Route erfolgt. Der Standardwert ist 120 (Sekunden).

Felder im Menü RIP-Optionen Timer für Triggered RIP (RFC 2091)

Feld	Beschreibung
Hold Down Timer	Nur für RFC 2091-Variabler Timer = Aktiviert Der Hold Down Timer wird aktiv, sobald Ihr Gerät eine unerreichbare Route (Metric 16) erhält. Nach Ablauf dieses Zeitraums wird die Route ggf. gelöscht. Der Standardwert ist 120 (in Sekunden).

Feld	Beschreibung
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> <p>Der Standardwert ist 5 (in Sekunden).</p>

9.4 Lastverteilung

9.4.1 Lastverteilungsgruppen

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

- 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 **Routing** -> **Lastverteilung** -> **Lastverteilungsgruppen** wird eine Liste aller konfigurierten Lastenausgleichs-Gruppen angezeigt.

9.4.1.1 Neu

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

The screenshot shows the configuration interface for 'Lastverteilungsgruppen' (Load Distribution Groups) on a bintec R1200 device. The interface is in German. The top bar includes 'Sprache: Deutsch', 'Online-Hilfe', and 'Ausloggen'. The left navigation menu is expanded to 'Routing' -> 'Lastverteilung' -> 'Lastverteilungsgruppen'. The main configuration area is titled 'Lastverteilungsgruppen' and contains the following fields:

- Basisparameter** (Basic Parameters):
 - Gruppenbeschreibung (Group Description): A text input field.
 - Verteilungsrichtlinie (Distribution Policy): A dropdown menu set to 'Sitzungs-Round-Robin'.
 - Verteilungsmodus (Distribution Mode): A checkbox that is checked.
- Schnittstellenauswahl für Verteilung** (Interface Selection for Distribution):
 - Schnittstelle (Interface): A dropdown menu.
 - Verteilungsverhältnis (Distribution Ratio): A text input field.

At the bottom of the configuration area, there is a 'Hinzufügen' (Add) button and three buttons: 'OK', 'Abbrechen' (Cancel), and 'Zurück' (Back).

Abb. 108: Routing -> Lastverteilung -> Lastverteilungsgruppen -> Neu

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

Felder im Menü Lastverteilungs-Gruppen 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.

Feld	Beschreibung
Berücksichtigen	<p>Nur für Verteilungsrichtlinie = <i>Bandbreite lastabhängig</i></p> <p>Wählen Sie aus, in welcher Richtung die aktuelle Datenrate berücksichtigt werden soll.</p> <p>Optionen:</p> <ul style="list-style-type: none"> • <i>Download</i>: Nur die Datenrate in Empfangsrichtung wird berücksichtigt. • <i>Upload</i>: Nur die Datenrate in Senderichtung wird berücksichtigt. <p>Standardmäßig sind die Optionen <i>Download</i> und <i>Upload</i> deaktiviert.</p>
Verteilungsmodus	<p>Wählen Sie aus, welchen Zustand die Schnittstellen der Gruppe haben dürfen, damit sie in die Lastverteilung einbezogen werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Immer</i>(Standardwert): Auch Schnittstellen im Zustand ruhend werden einbezogen. • <i>Nur aktive Schnittstellen verwenden</i>: Es werden nur Schnittstellen im Zustand aktiv berücksichtigt.

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

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

Felder im Menü Lastverteilungs-Gruppen Schnittstellenauswahl für Verteilung

Feld	Beschreibung
Schnittstelle	<p>Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, die der Gruppe angehören sollen.</p>
Verteilungsverhältnis	<p>Geben Sie an, welchen Prozentsatz des Datenverkehrs eine Schnittstelle übernehmen soll.</p> <p>Die Bedeutung unterscheidet sich je nach verwendeter Verteilungsrichtlinie:</p>

Feld	Beschreibung
	<ul style="list-style-type: none">• für <i>Sitzungs-Round-Robin</i> wird die Anzahl verteilten Sessions zugrunde gelegt.• für <i>Bandbreite lastabhängig</i> ist die Datenrate maßgeblich.

9.5 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 Einsatzbereiche 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 benutzt. 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.

9.5.1 Weiterleiten

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

9.5.1.1 Neu

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

The screenshot shows the web interface for a bintec R1200 router. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstattung', and 'Monitoring'. The 'Routing' category is expanded, showing sub-items: 'Routen', 'HAT', 'RIP', 'Lastverteilung', 'Multicast', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstattung', and 'Monitoring'. The 'Multicast' item is selected. The main content area shows the 'Weiterleiten' (Forwarding) configuration page. At the top, there are tabs for 'Weiterleiten', 'IGMP', and 'Optionen'. Below the tabs is a 'Basisparameter' (Basic Parameters) section with the following fields:

Basisparameter	
Alle Multicast-Gruppen	<input type="checkbox"/> Aktiviert
Multicast-Gruppen-Adresse	<input type="text"/>
Quellschnittstelle	Keine <input type="button" value="v"/>
Zielschnittstelle	Keine <input type="button" value="v"/>

At the bottom of the configuration area are two buttons: 'OK' and 'Abbrechen'.

Abb. 109: Routing -> Multicast -> Weiterleiten -> /Neu

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

Felder im Menü Weiterleiten 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 Aktiviert.</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 = <i>nicht aktiv</i></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.

9.5.2 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.

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

9.5.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um IGMP auf weiteren Schnittstellen zu konfigurieren.

The screenshot shows the configuration interface for a bintec R1200 device. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, and Multicast. The 'Routing' menu is expanded, showing options like Routen, IAT, RIP, Lastverteilung, and Multicast. The 'Multicast' menu is further expanded to show 'IGMP'. The main content area displays the 'IGMP-Einstellungen' (IGMP Settings) for a selected interface (currently 'Keine'). The settings include:

- Schnittstelle: Keine
- Abfrage Intervall: 125 Sekunden
- Maximale Antwortzeit: 10 Sekunden
- Robustheit: 2
- Antwortintervall (Letztes Mitglied): 1 Sekunden
- Maximale Anzahl der IGMP-Statusmeldungen: 0 Meldungen pro Sekunde
- Modus: Nur Host Host und Routing

 Below the main settings is an 'Erweiterte Einstellungen' (Advanced Settings) section with an 'IGMP Proxy' checkbox, which is currently unchecked. At the bottom are 'OK' and 'Abbrechen' buttons.

Abb. 110: **Routing -> Multicast -> IGMP -> /Neu**

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

Felder im Menü IGMP IGMP-Einstellungen

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der IGMP aktiviert werden soll, d.h. Queries werden versendet und Antworten akzeptiert.
Abfrage Intervall	Geben Sie das Intervall in Sekunden ein, in dem IGMP Queries versendet werden sollen. Möglich Werte sind 0 bis 600. Der Standardwert ist 125.
Maximale Antwortzeit	Geben Sie für das Senden von Queries an, in welchem Zeitintervall in Sekunden Hosts auf jeden Fall antworten müssen. Die Hosts wählen aus diesem Intervall zufällig eine Verzögerung, bis die Antwort gesendet wird. Damit können Sie bei Netzen mit vielen Hosts eine Streuung und somit eine Entlastung errei-

Feld	Beschreibung
	<p>chen.</p> <p>Möglich Werte sind <i>0</i> bis <i>100</i>.</p> <p>Der Standardwert ist <i>100</i>.</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 <i>2</i> bis <i>8</i>.</p> <p>Der Standardwert ist <i>2</i>.</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 dieses Schnittstelle weitergeleitet werden müssen.</p>
Maximale Anzahl der IGMP-Statusmeldungen	<p>Limitieren Sie die Anzahl der Reports/Queries pro Sekunde für die gewählte Schnittstelle.</p>
Modus	<p>Wählen Sie aus, ob die hier definierte Schnittstelle nur im Host-Modus oder auch im Routing Modus arbeitet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Host und Routing</i> (Standardwert): Die Schnittstelle wird im Routing- und im Host-Modus betrieben. • <i>Nur Host</i>: Die Schnittstelle wird nur im Host-Modus betrieben.

IGMP Proxy

Mit IGMP Proxy können mehrere lokal angeschlossene Schnittstellen als ein Subnetz zu einem benachbarten Router simuliert werden. Auf der IGMP-Proxy-Schnittstelle eingehende Queries werden in die lokalen Subnetze weitergeleitet. Lokale Reports werden auf der IPGM-Proxy-Schnittstelle weitergeleitet.

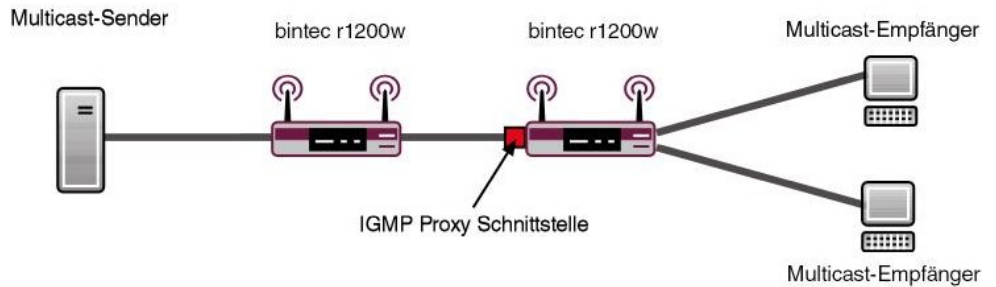


Abb. 111: IGMP Proxy

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	Wählen Sie die Schnittstelle Ihres Geräts aus, über die Queries angenommen und gesammelt werden sollen.

9.5.3 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.



Abb. 112: Routing -> Multicast -> Optionen

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

Felder im Menü Optionen Basiseinstellungen

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

Feld	Beschreibung
	<ul style="list-style-type: none">• <i>Nur Version 3</i>: Nur IGMP Version 3 wird verwendet.
Maximale Gruppen	Geben Sie ein, wieviele 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	Geben Sie die maximale Anzahl der insgesamt möglichen eingehenden Queries bzw. Meldungen pro Sekunde ein. Der Standardwert ist 0, d.h die Anzahl der IGMP-Statusmeldungen ist nicht begrenzt.

Kapitel 10 WAN

10.1 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), PPP-over-PPTP und PPP-over-ATM (PPPoA) zur Verfügung. Ein Internetzugang mittels ISDN ist ebenfalls konfigurierbar.



Hinweis





Beachten Sie die Vorgaben Ihres Providers!

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

Alle eingetragenen Verbindungen werden in der entsprechenden Liste angezeigt, welche die **Beschreibung**, den **Benutzername**, 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 über den ISDN-D-Kanal die Nummer des Anrufers mitgegeben. Anhand dieser Nummer kann Ihr Gerät den Anrufer identifizieren (CLID), wenn dieser auf Ihrem Gerät eingetragen ist. Nach der Identifizierung mit CLID kann Ihr Gerät zusätzlich eine PPP-Authentisierung mit dem Verbindungspartner durchführen, bevor der Ruf angenommen wird. Dazu benötigt Ihr Gerät Vergleichsdaten, die Sie hier eintragen. Zunächst legen Sie fest, welche Authentisierungsverhandlung 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.

Callback

Um zusätzliche Sicherheit bezüglich des Verbindungspartners zu erlangen oder die Kosten von Verbindungen eindeutig verteilen zu können, kann für jede Verbindung der Callback-Mechanismus verwendet werden. Damit kommt eine Verbindung erst durch einen Rückruf

zustande, nachdem der Anrufende eindeutig identifiziert wurde. Ihr Gerät kann sowohl einen eingehenden Ruf mit einem Rückruf beantworten, also auch von einem Verbindungspartner einen Rückruf anfordern. Die Identifizierung kann aufgrund der Calling Party Nummer oder aufgrund der PAP/CHAP/MS-CHAP-Authentifizierung erfolgen. Im ersten Fall erfolgt die Identifikation ohne Rufannahme, da die Calling Party Number über den ISDN-D-Kanal übermittelt wird, im zweiten Fall mit Rufannahme.

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 Gebühren ggf. zu sparen.

Blockieren nach Verbindungsfehler

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

Kanalbündelung

Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet.

Dynamisch

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

Statisch

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

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

10.1.1 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.

10.1.1.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. Under 'WAN', 'Internet + Einwählen' is selected, and 'Standleitung' is highlighted. The main configuration area has tabs for 'PPPoE', 'PPTP', 'ISDN', 'GPRS/UMTS', 'AUX', and 'IP Pools'. The 'PPPoE' tab is active, displaying two sections: 'Basisparameter' and 'Erweiterte Einstellungen'.

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	<input type="password" value="••••••••"/>
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	<input type="text" value="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	<input type="text" value="60"/> Sekunden
Maximale Anzahl der erneuten Einwählversuche	<input type="text" value="5"/>
Authentifizierung	PAP <input type="button" value="v"/>
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Ereichbarkeitsprüfung	<input type="checkbox"/> Aktiviert

At the bottom of the configuration area, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 113: WAN -> Internet + Einwählen -> PPPoE -> Neu

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

Felder im Menü PPPoE Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den PPPoE-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPPoE-Modus	<p>Wählen Sie aus, ob Sie eine Standard-Internetverbindung über PPPoE (<i>Standard</i>) nutzen oder ob Ihr Internetzugang über mehrere Schnittstellen aufgebaut werden soll (<i>Mehrfachverbindung</i>). Wählen Sie <i>Mehrfachverbindung</i>, so können Sie mehrere DSL-Verbindungen eines Providers über PPP als statische Bündel koppeln, um mehr Bandbreite zu erhalten. Jede dieser DSL-Verbindungen sollte dafür eine separate Ethernet-Verbindung nutzen. Aktuell ist bei vielen Providern die Funktion PPPoE Multilink erst in Vorbereitung.</p> <p>Wir empfehlen Ihnen, für PPPoE Multilink den Ethernet Switch Ihres Geräts im Split-Port-Modus zu betreiben und für jede PPPoE-Verbindung eine eigene Ethernet-Schnittstelle zu benutzen, z. B. <i>en1-1, 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 Mode = <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> <p>Standardwert ist <i>Nicht spezifiziert</i>.</p>
PPPoE-Schnittstelle für Mehrfachlinks	<p>Nur für PPPoE Mode = <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>

Feld	Beschreibung
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 (Flatrate-Modus) deaktiviert ist</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold.</p> <p>Standardwert ist 300 .</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>

Felder im Menü PPPoE 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>

Feld	Beschreibung
	Standardmäßig ist die Funktion aktiv.
NAT-Eintrag erstellen	Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Lokale IP-Adresse	Nur bei IP-Adressmodus = <i>Statisch</i> Geben Sie die statische IP-Adresse des Verbindungspartners ein.
Routeneinträge	Nur bei IP-Adressmodus = <i>Statisch</i> Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner. Fügen Sie mit Hinzufügen neue Einträge hinzu. <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Remote-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 unternommen werden soll. Standardwert ist 60.
Maximale Anzahl der erneuten Einwählversuche	Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird. Mögliche Werte von 0 bis 100. Standardwert ist 5.

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

10.1.2 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, z. B. in Österreich notwendig.

10.1.2.1 Neu

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

bintec R1200 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk**
ENTERPRISE COMMUNICATIONS GMBH

Konfiguration speichern

Systemverwaltung
 Physikalische Schnittstellen
 LAN
 Wireless LAN
 Routing
 WAN
 Internet + Einwählen
 Standleitung
 Real Time Jitter Control
 VPN
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

PPPoE **PPTP** ISDN GPRS/UMTS AUX IP Pools

Basisparameter	
Beschreibung	<input type="text"/>
PPTP-Schnittstelle	Eine auswählen <input type="button" value="v"/>
Benutzername	<input type="text"/>
Passwort	•••••••• <input type="text"/>
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 <input type="button" value="v"/>
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
PPTP-Adressmodus	Static
Lokale PPTP-IP-Adresse	10.0.0.140
Remote-PPTP-IP-Adresse	10.0.0.138
LCP-Erreichbarkeitsprüfung	<input type="checkbox"/> Aktiviert

Abb. 114: WAN -> Internet + Einwählen -> PPTP -> Neu

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

Felder im Menü PPTP Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um die Internetverbindung eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPTP-Schnittstelle	Wählen Sie die IP-Schnittstelle aus, über die Pakete zur PPTP-Gegenstelle transportiert werden. Bei Verwendung eines externen DSL-Modems, wählen Sie hier den Ethernet-Port aus, an dem das Modem angeschlossen ist.

Feld	Beschreibung
	<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> <p>Standardwert ist <i>Nicht spezifiziert</i>.</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 (Flatrate-Modus) deaktiviert ist</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit 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 Timeout.</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 PPTP 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 Ziel-Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Remote-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 unternommen werden soll. Standardwert ist 60.

Feld	Beschreibung
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte von 0 bis 100 .</p> <p>Standardwert ist 5 .</p>
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i> : Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i> : Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP-Partner geforderte Authentifizierungsprotokoll ausführen (MSCHAP Version 1 oder 2 möglich). • <i>MS-CHAPv2</i>: Nur MS-CHAP Version 2 ausführen.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Feld	Beschreibung
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 IP-Adresse des in PPTP-Schnittstelle ausgewählten Ethernet-Ports wird verwendet.
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 nicht aktiv.</p>

10.1.3 PPPoA

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

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

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

10.1.3.1 Neu

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

bintec R3800 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk**
enterprise communications

Konfiguration speichern

Systemverwaltung
Physikalische Schnittstellen
LAN
Routing
WAN
 Internet + Einwählen
 ATM
 Standleitung
 Real Time Jitter Control
VPN
Firewall
VoIP
Lokale Dienste
Wartung
Externe Berichterstellung
Monitoring

PPPoE **PPTP** **PPPoA** **ISDN** **AUX** **IP Pools**

Basisparameter	
Beschreibung	<input type="text"/>
ATM PVC	Eine auswählen <input type="button" value="v"/>
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 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	<input type="text" value="60"/> Sekunden
Maximale Anzahl der erneuten Einwählversuche	<input type="text" value="5"/>
Authentifizierung	<input type="text" value="PAP"/> <input type="button" value="v"/>
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input type="checkbox"/> Aktiviert

Abb. 115: WAN -> Internet + Einwählen -> PPPoA -> Neu

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

Felder im Menü PPPoA Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungspartner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
ATM PVC	Wählen Sie ein im Menü ATM -> Profile angelegtes ATM-Profil, dargestellt durch die vom Provider vorgegebenen globalen ID VPI und VCI.
Benutzername	Geben Sie den Benutzernamen ein.

Feld	Beschreibung
Passwort	Geben Sie das Passwort für die PPPoA-Verbindung ein.
Immer aktiv	<p>Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Aktivieren Sie diese Option nur, wenn Sie einen Internetzugang mit Flatrate-Tarif haben.</p>
Timeout bei Inaktivität	<p>Nur wenn Immer aktiv (Flatrate-Modus) deaktiviert ist</p> <p>Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen soll.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold.</p> <p>Standardwert ist 300 .</p> <p>Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.</p>

Felder im Menü PPPoA IP-Modus und Routen

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

Feld	Beschreibung
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>statisch</i>.</p> <p>Tragen Sie hier die statische IP-Adresse ein, die Sie von Ihrem Provider erhalten haben.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <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 -LANs. • <i>Netzmaske</i>: Netzmaske zu Remote-IP-Adresse. • <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 unternommen werden soll. Standardwert ist 60 .
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte von 0 bis 100 .</p> <p>Standardwert ist 5 .</p>
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diese Internetverbindung aus. Wählen Sie die Authentifizierung, die von Ihrem Provider spezifiziert ist.

Feld	Beschreibung
	<p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP</i> (Standardwert): Nur <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i> : Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig <i>CHAP</i>, sonst <i>PAP</i> ausführen. • <i>MS-CHAPv1</i>: Nur <i>MS-CHAP</i> Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i> : Vorrangig <i>CHAP</i> ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (<i>MSCHAP</i> Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur <i>MS-CHAP</i> Version 2 ausführen.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primäre Domänennamen Server und Sekundäre Domänennamen Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Diese ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

10.1.4 ISDN

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

In diesem Menü konfigurieren Sie folgende ISDN-Verbindungen:

- Internetzugang über ISDN
- LAN-zu-LAN Kopplung über ISDN
- Remote (Mobile) Dialin
- Nutzung der Funktion ISDN Callback

10.1.4.1 Neu

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

bintec R1200 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Systemverwaltung
 Physikalische Schnittstellen
 LAN
 Wireless LAN
 Routing
WAN
 Internet + Einwählen
 Standleitung
 Real Time Jitter Control
 VPN
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

PPPoE PPTP **ISDN** GPRS/UMTS AUX IP Pools

Basisparameter

Beschreibung:

Verbindungstyp: ISDN 64 kbit/s

Benutzername:

Entfernter Benutzer (nur Einwahl):

Passwort:

Immer aktiv: Aktiviert

Timeout bei Inaktivität: 20 Sekunden

IP-Modus und Routen

IP-Adressmodus: Statisch IP-Adresse bereitstellen IP-Adresse abrufen

Standardroute: Aktiviert

NAT-Eintrag erstellen: Aktiviert

Lokale IP-Adresse:

Routeneinträge

Entfernte IP-Adresse	Netzmaske	Metrik
<input type="text"/>	<input type="text"/>	1

Hinzufügen

Erweiterte Einstellungen

Blockieren nach Verbindungsfehler für: 300 Sekunden

Maximale Anzahl der erneuten Einwählversuche: 5

Nutzungsart: Standard Nur Einwahl Mehrfacheinwahl (Nur Einwahl)

Authentifizierung: PAP/CHAP/MS-CHAP

Callback-Modus: Keiner Aktiv Passiv

Optionen für Bandbreite auf Anforderung

Kanalbündelung: Keine

Wahlnummern

Einträge	Modus	Rufnummer (MSN)	Anzahl Verwendeter Ports
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Hinzufügen

IP-Optionen

OSPF-Modus: Passiv Aktiv Inaktiv

Proxy-ARP-Modus: Inaktiv Aktiv oder Ruhend Nur aktiv

DNS-Aushandlung: Aktiviert

OK **Abbrechen**

Abb. 116: WAN -> Internet + Einwählen -> ISDN -> Neu

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

Felder im Menü ISDN Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den Verbindungs-

Feld	Beschreibung
	<p>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>
Verbindungstyp	<p>Wählen Sie aus, welches Layer-1-Protokoll Ihr Gerät nutzen soll.</p> <p>Diese Einstellung gilt für ausgehende Verbindungen zum Verbindungspartner und nur für eingehende Verbindungen vom Verbindungspartner, wenn sie anhand der Calling Party Number identifiziert werden konnten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>ISDN 64kBit/s</i>: Für ISDN-Datenverbindungen mit 64 kBit/s • <i>ISDN 56kBit/s</i>: Für ISDN-Datenverbindungen mit 56 kBit/s
Benutzername	Geben Sie die Kennung Ihres Geräts (lokaler PPP Benutzername) ein.
Entfernter Benutzer (nur Einwahl)	Geben Sie die Kennung der Gegenstelle (entfernter PPP Benutzername) 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>Geben Sie das Inaktivitätsintervall in Sekunden für den Statischen Short Hold ein. Mit dem Statischen Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Zur Verfügung stehen Werte von <i>-1</i> bis <i>3600</i> (Sekunden). Ein Wert von <i>-1</i> bedeutet, dass die Verbindung nach einem Abbruch sofort wieder aufgebaut wird, <i>0</i> deaktiviert den Shorthold. Standardwert ist <i>20</i>.</p>

Felder im Menü ISDN 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>: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse. • <i>IP-Adresse abrufen</i>: Ihr Gerät erhält dynamisch eine IP-Adresse.
Standardroute	<p>Nur bei IP-Adressmodus = <i>Statisch</i> und <i>IP-Adresse abrufen</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 bei IP-Adressmodus = <i>Statisch</i> und <i>IP-Adresse abrufen</i></p> <p>Wenn eine ISDN-Internetverbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Weisen Sie der ISDN-Schnittstelle die 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>

Feld	Beschreibung
	<p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <i>Netzmaske</i>: Netzmaske zu Ziel IP-Address. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0 . . . 15). Standardwert ist 1.
IP-Zuordnungspool	<p>Nur bei IP-Adressmodus = IP-Adresse bereitstellen</p> <p>Wählen Sie einen im Menü WAN -> Internet + Einwählen -> 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>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Standardwert ist 300 .</p>
Maximale Anzahl der erneuten Einwählversuche	<p>Geben Sie die Anzahl der erfolglosen Versuche für einen Verbindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte von 0 bis 100 .</p> <p>Standardwert ist 5 .</p>
Nutzungsart	<p>Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Kein spezieller Typ ist ausgewählt. • <i>Nur Einwahl</i>: Die Schnittstelle wird für eingehende Wahlverbindungen und für von außen initiierten Callback verwendet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Mehrfacheinwahl (Nur Einwahl)1</i>: Die Schnittstelle wird als Multi-User Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen PPTP Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP/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 <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <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.
Verschlüsselung	<p>Nur für PPP-Authentifizierung = <i>MS-CHAPv2</i></p> <p>Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem Verbindungspartner angewendet werden soll. Dies ist nur möglich, wenn keine Komprimierung mit STAC bzw. MS-STAC für die Verbindung aktiv ist. 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>Keine</i> (Standardwert): Es wird keine MPP-Verschlüsselung angewendet. • <i>Aktiviert</i>: 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.

Feld	Beschreibung
Callback-Modus	<p>Wählen Sie die Funktion Callback-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Ihr Gerät führt keinen Rückruf aus. • <i>Aktiv</i>: Wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> • <i>Keine PPP-Aushandlung</i>: Ihr Gerät ruft den Verbindungspartner an, um einen Rückruf anzufordern. • <i>Windows-Clientmodus</i>: Ihr Gerät ruft den Verbindungspartner an, um über CBCP (Callback Control Protocol) einen Rückruf anzufordern. Wird für Windows Clients benötigt. • <i>Passiv</i>: Wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> • <i>Aktiviert</i> : Ihr Gerät ruft sofort zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert wird. • <i>Windows-Servermodus</i> : Ihr Gerät ruft nach einer vom Microsoft Client vorgeschlagenen Zeit (NT: 10 Sekunden, neuere Systeme: 12 Sekunden) zurück. Es verwendet die Rufnummer (Einträge-> Nummer (MSN)) mit dem Modus Ausgehend oder <i>Beide</i>, die für den Verbindungspartner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP Aushandlung mitgeteilt werden. Diese Einstellung ist aus Sicherheitsgründen möglichst nicht zu verwenden. Bei der Anbindung von mobilen Microsoft-Clients über DFÜ-Netzwerk ist dies derzeit nicht vermeidbar. • <i>Verzögert, nur CLID</i> : Ihr Gerät ruft nach ca. vier Sekunden zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert worden ist. Nur sinnvoll bei CLID. • <i>Windows-Servermodus, Rückruf optional</i> : Wie <i>Windows-Servermodus</i> mit Abbruchoption. Diese Einstellung ist aus Sicherheitsgründen zu vermeiden. Der Microsoft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu Ihrem Gerät ohne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer für den Verbindungspartner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit ABBRECHEN geschlossen wird.

Felder im Menü Erweiterte Einstellungen Optionen für Bandbreite auf Anforderung

Feld	Beschreibung
Kanalbündelung	<p>Wählen Sie aus, ob Kanalbündelung bzw. welche Art von Kanalbündelung für ISDN-Verbindungen mit dem Verbindungspartner genutzt werden soll.</p> <p>Ihr Gerät unterstützt dynamische und statische Kanalbündelung für Wählverbindungen. Bei Aufbau einer Verbindung wird zunächst nur ein B-Kanal geöffnet. Dynamische Kanalbündelung bedeutet, dass Ihr Gerät bei Bedarf, also bei großen Datenraten, weitere ISDN-B-Kanäle zuschaltet, um den Durchsatz zu erhöhen. Sinkt das Datenaufkommen, werden die zusätzlichen B-Kanäle wieder geschlossen. Bei statischer Kanalbündelung legen Sie im Voraus fest, wie viele B-Kanäle Ihr Gerät nutzen soll, unabhängig von der übertragenen Datenrate.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Keine Kanalbündelung, für Verbindungen steht immer nur ein B-Kanal zur Verfügung. • <i>Statisch</i>: Statische Kanalbündelung. • <i>Dynamisch</i>: Dynamische Kanalbündelung.

Felder im Menü **Erweiterte Einstellungen Wahlnummern**

Feld	Beschreibung
Einträge	Fügen Sie weitere Einträge mit Hinzufügen hinzu.

Felder im Menü **Konfiguration der Wahlnummern Eintrag: <1> (erscheint nur für Einträge = Hinzufügen)**

Feld	Beschreibung
Modus	<p>Nur wenn Einträge = Hinzufügen.</p> <p>Wählen Sie aus, ob Rufnummer (MSN) für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): Für eingehende und ausgehende Rufe. • <i>Eingehend</i>: Für eingehende Rufe, wenn der Verbindungspartner sich bei Ihrem Gerät einwählen soll. • <i>Ausgehend</i>: Für ausgehende Rufe, wenn Sie sich beim Verbindungspartner einwählen wollen.

Feld	Beschreibung
	Die Calling Party Number des eingehenden Rufes wird mit der unter Rufnummer (MSN) eingetragenen Nummer verglichen.
Rufnummer	Geben Sie die Rufnummern des Verbindungspartners ein.
Port-Verwendung	Wählen Sie aus welches Port zu verwenden ist.

Felder im Menü Erweiterte Einstellungen IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellen Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, 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 aktiv, 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 und wie ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantwortet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • <i>Aktiv oder ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> 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 Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbin-

Feld	Beschreibung
	dungspartner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server, Sekundärer DNS-Server, Primärer WINS und Sekundärer WINS 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>

10.1.5 GPRS/UMTS



Hinweis

Beachten Sie, dass das Menü **GPRS/UMTS** nur verfügbar ist, wenn eine UMTS-Modemkarte in den CardBus Slot eingeführt und in das System integriert ist! Nicht alle **bintec** Gateways verfügen über eine CardBus-Schnittstelle. Ob Ihr Gateway über diesen Schnittstellentyp verfügt, entnehmen Sie bitte dem Datenblatt.

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

Mit seiner CardBus-Schnittstelle (PCCARD) unterstützt das **bintec** Gateway die Integration eines UMTS-CardBus-Modems in das System. Damit können Sie eine Verbindung in das Internet über UMTS herstellen.

10.1.5.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 device. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Lokale Dienste, and Monitoring. The WAN section is expanded to show 'Internet + Einwählen', 'Standleitung', and 'Real Time Jitter Control'. The main configuration area has tabs for 'PPPoE', 'PPTP', 'ISDN', 'GPRS/UMTS', 'AUX', and 'IP Pools'. The 'GPRS/UMTS' tab is selected, displaying the 'Neu' configuration screen. This screen is divided into 'Basisparameter' and 'Erweiterte Einstellungen' sections. The 'Basisparameter' section includes fields for 'Beschreibung', 'GPRS/UMTS-Schnittstelle' (set to 'Slot 6 Einheit 0 UMTS'), 'Benutzername', 'Passwort', 'Immer aktiv' (checkbox), and 'Timeout bei Inaktivität' (set to 300 Sekunden). The 'Erweiterte Einstellungen' section includes 'Blockieren nach Verbindungsfehler für' (60 Sekunden), 'Maximale Anzahl der erneuten Einwählversuche' (5), 'Authentifizierung' (set to PAP), 'DNS-Aushandlung' (checkbox), 'TCP-ACK-Pakete priorisieren' (checkbox), and 'LCP-Erreichbarkeitsprüfung' (checkbox). 'OK' and 'Abbrechen' buttons are at the bottom.

Abb. 117: WAN -> Internet + Einwählen -> GPRS/UMTS -> Neu

Das Menü **WAN -> Internet + Einwählen -> GPRS/UMTS -> Neu** besteht aus folgenden Feldern:

Felder im Menü GPRS/UMTS Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den WAN-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
GPRS/UMTS-Schnittstelle	Wählen Sie die GPRS/UMTS-Schnittstelle aus.

Feld	Beschreibung
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 für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold.</p> <p>Standardwert ist 300 .</p>

Felder im Menü GPRS/UMTS 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	Wählen Sie aus, ob Network Address Translation (NAT) akti-

Feld	Beschreibung
	<p>viert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die statische IP-Adresse des Verbindungspartners ein.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Remote-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 von 0 bis 100.</p> <p>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 <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig <i>CHAP</i>, sonst <i>PAP</i> ausführen. • <i>MS-CHAPv1</i>: Nur <i>MS-CHAP</i> Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i> : Vorrangig <i>CHAP</i> ausführen, bei Ablehnung anschließend das vom Verbindungspartner geforderte Authentifizierungsprotokoll ausführen. (<i>MSCHAP</i> Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>: Nur <i>MS-CHAP</i> Version 2 ausführen.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

10.1.6 AUX

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

In diesem Menü können Sie unterschiedliche Vorgaben für die Kommunikation zwischen Gateway und Modem definieren. Für den Anschluss eines externen Analogmodems an den AUX Port eines **bintec** Gateways, benötigen Sie ein spezielles Kabel für den Konsolen-Port (z. B. AUX-Backup Cable) Ihres Gateways.

10.1.6.1 Neu

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

bintec R1200 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk**
enterprise communications

Konfiguration speichern

Systemverwaltung
Physikalische Schnittstellen
LAN
Wireless LAN
Routing
WAN
Internet + Einwählen
Standleitung
Real Time Jitter Control
VPN
Firewall
VoIP
Lokale Dienste
Wartung
Externe Berichterstellung
Monitoring

PPPoE PPTP ISDN GPRS/UMTS AUX IP Pools

Basisparameter

Beschreibung	<input type="text"/>
Benutzername	<input type="text"/>
Passwort	••••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	<input type="text" value="600"/> Sekunden

IP-Modus und Routen

IP-Adressmodus	<input type="radio"/> Statisch <input type="radio"/> IP-Adresse bereitstellen <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	<input type="text" value="50"/> Sekunden
Maximale Anzahl der erneuten Einwahlversuche	<input type="text" value="5"/>
Nutzungsart	<input checked="" type="radio"/> Standard <input type="radio"/> Nur Einwahl <input type="radio"/> Mehrfacheinwahl (Nur Einwahl)
Authentifizierung	<input type="text" value="PAP"/>
DNS-Aushandlung	<input checked="" type="checkbox"/> Aktiviert
TCP-ACK-Pakete priorisieren	<input type="checkbox"/> Aktiviert
LCP-Erreichbarkeitsprüfung	<input type="checkbox"/> Aktiviert
Callback-Modus	<input checked="" type="radio"/> Keiner <input type="radio"/> Aktiv <input type="radio"/> Passiv

Wahlnummern

Einträge	Modus <input type="text"/> Rufnummer (MSN) <input type="text"/> Hinzufügen
----------	--

IP-Optionen

Proxy-ARP-Modus	<input checked="" type="radio"/> Inaktiv <input type="radio"/> Aktiv oder Ruhend <input type="radio"/> Nur aktiv
-----------------	--

OK Abbrechen

Abb. 118: WAN -> Internet + Einwählen -> AUX -> Neu

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

Felder im Menü AUX Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen beliebigen Namen ein, um den WAN-Partner eindeutig zu benennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.

Feld	Beschreibung
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 für Statischen Short Hold ein. Mit Statischem Short Hold legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p> <p>Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold.</p> <p>Standardwert ist 600 .</p>

Felder im Menü AUX 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. • <i>IP-Adresse bereitstellen</i>: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse.
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>

Feld	Beschreibung
NAT-Eintrag erstellen	<p>Wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Lokale IP-Adresse	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Geben Sie die statische IP-Adresse des Verbindungspartners ein.</p>
Routeneinträge	<p>Nur bei IP-Adressmodus = <i>Statisch</i></p> <p>Definieren Sie weitere Routing-Einträge für diesen Verbindungspartner.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -Netzwerkes. • <i>Netzmaske</i>: Netzmaske zu Remote-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.
IP-Zuordnungspool	<p>Nur bei IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>Wählen Sie einen im Menü WAN -> Internet + Einwählen -> 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>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	<p>Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll.</p> <p>Standardwert ist 50.</p>
Maximale Anzahl der er-	Geben Sie die Anzahl der erfolglosen Versuche für einen Ver-

Feld	Beschreibung
neuten Einwählversuche	<p>bindungsaufbau ein, nach denen die Schnittstelle blockiert wird.</p> <p>Mögliche Werte von 0 bis 100 .</p> <p>Standardwert ist 5 .</p>
Nutzungsart	<p>Wählen Sie ggf. eine spezielle Nutzung der Schnittstelle.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Kein spezieller Typ ist ausgewählt. • <i>Nur Einwahl</i>: Die Schnittstelle wird für eingehende Wahlverbindungen und für von außen initiierten Callback verwendet. • <i>Mehrfacheinwahl (Nur Einwahl)1</i>: Die Schnittstelle wird als Multi-User Verbindungspartner definiert, d. h. mehrere Clients wählen sich mit gleichem Benutzernamen und Passwort ein.
Authentifizierung	<p>Wählen Sie das Authentifizierungsprotokoll für diesen PPTP Partner aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PAP/CHAP/MS-CHAP</i> : Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>PAP</i>: Nur <i>PAP</i> (Standardwert): (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <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.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server und Sekundärer DNS-Server vom Verbindungspartner</p>

Feld	Beschreibung
	<p>erhält oder diese zum Verbindungspartner schickt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. So ist es möglich, im Falle einer Leitungsstörung schneller auf eine Backup-Verbindung umzuschalten.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Callback-Modus	<p>Wählen Sie die Funktion Callback-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Ihr Gerät führt keinen Rückruf aus. • <i>Aktiv</i>: Wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> • <i>Keine PPP-Aushandlung</i>: Ihr Gerät ruft den Verbindungspartner an, um einen Rückruf anzufordern. • <i>Windows-Clientmodus</i>: Ihr Gerät ruft den Verbindungspartner an, um über CBCP (Callback Control Protocol) einen Rückruf anzufordern. Wird für Windows Clients benötigt. • <i>Passiv</i>: Wählen Sie eine der folgenden Optionen: <ul style="list-style-type: none"> • <i>PPP-Aushandlung oder CLID</i>: Ihr Gerät ruft sofort zurück, wenn Ihr Gerät vom Verbindungspartner dazu aufgefordert wird. • <i>Windows-Servermodus</i>: Ihr Gerät ruft nach einer vom Microsoft Client vorgeschlagenen Zeit (NT: 10 Sekunden, neuere Systeme: 12 Sekunden) zurück. Es verwendet die Rufnummer (Einträge-> Nummer (MSN)) mit dem Modus

Feld	Beschreibung
	<p><i>Ausgehend</i> oder <i>Beide</i>, die für den Verbindungspartner eingetragen ist. Wenn keine Nummer eingetragen ist, kann die erforderliche Nummer vom Anrufer in einer PPP Aus- handlung mitgeteilt werden. Diese Einstellung ist aus Si- cherheitsgründen möglichst nicht zu verwenden. Bei der Anbindung von mobilen Microsoft-Clients über DFÜ- Netzwerk ist dies derzeit nicht vermeidbar.</p> <ul style="list-style-type: none"> • <i>Verzögert, nur CLID</i>: Ihr Gerät ruft nach ca. vier Se- kunden zurück, wenn Ihr Gerät vom Verbindungspartner da- zu aufgefordert worden ist. Nur sinnvoll bei CLID. • <i>Windows-Servermodus, Rückruf optional</i>: Wie <i>Windows-Servermodus</i> mit Abbruchoption. Diese Einstel- lung ist aus Sicherheitsgründen zu vermeiden. Der Micro- soft-Client hat hier zusätzlich die Möglichkeit, den Callback abzubrechen und die initiale Verbindung zu Ihrem Gerät oh- ne Callback aufrechtzuerhalten. Dieses gilt nur, wenn keine feste ausgehende Rufnummer für den Verbindungspartner konfiguriert ist. Dies wird erreicht, indem das erscheinende Dialogfenster mit ABBRECHEN geschlossen wird.

Felder im Menü Erweiterte Einstellungen Wahlnummern

Feld	Beschreibung
Einträge	Fügen Sie weitere Einträge mit Hinzufügen hinzu.

Felder im Menü Konfiguration der Wahlnummern Eintrag: <1> (erscheint nur für Ein- träge = Hinzufügen)

Feld	Beschreibung
Modus	<p>Nur wenn Einträge = Hinzufügen.</p> <p>Wählen Sie aus, ob Rufnummer (MSN) für eingehende oder für ausgehende Rufe oder für beides verwendet werden soll. Mögli- che Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): Für eingehende und ausgehende Ru- fe. • <i>Eingehend</i>: Für eingehende Rufe, wenn der Verbindungs- partner sich bei Ihrem Gerät einwählen soll. • <i>Ausgehend</i>: Für ausgehende Rufe, wenn Sie sich beim Ver- bindungspartner einwählen wollen. <p>Die Calling Party Number des eingehenden Rufes wird mit der</p>

Feld	Beschreibung
	unter Rufnummer (MSN) eingetragenen Nummer verglichen.
Rufnummer	Geben Sie die Rufnummern des Verbindungspartners ein.
Port-Verwendung	Wählen Sie aus welches Port zu verwenden ist.
Felder im Menü Erweiterte Einstellungen IP-Optionen	
Feld	Beschreibung
Proxy-ARP-Modus	<p>Wählen Sie aus, ob und wie ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantwortet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • <i>Aktiv oder ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> 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 Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.

10.1.7 IP Pools

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

Ihr Gerät kann als dynamischer IP-Address-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 Address-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 Address-Pool zuweisen (falls verfügbar). Bei Address-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 Stun-

de wird aber versucht, wieder die zuletzt an diesen Partner vergebene IP-Adresse zuzuweisen.

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere IP Pools einzurichten.

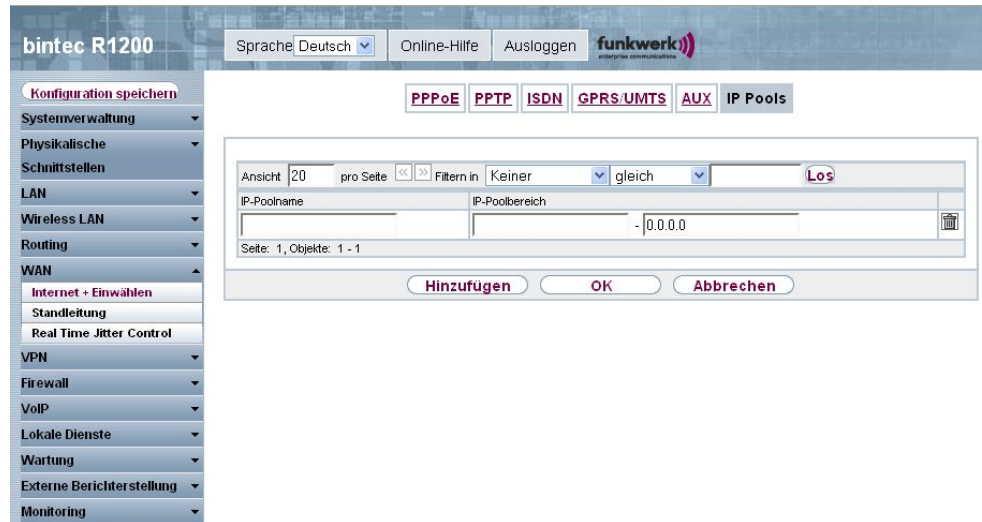


Abb. 119: WAN -> Internet + Einwählen -> IP Pools -> Hinzufügen

Das Menü **WAN -> Internet + Einwählen -> IP Pools -> Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Optionen IP Pools

Feld	Beschreibung
IP-Poolname	Geben Sie die Bezeichnung des IP-Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse des Bereiches ein. Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.

10.2 ATM

10.2.1 Profile

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

Wenn die Verbindung für Ihren Internetzugang über das interne Modem aufgebaut wird, müssen dafür die ATM-Verbindungsparameter eingestellt werden.

Standardmäßig ist ein ATM-Profil mit der Beschreibung *AUTO-CREATED* vorkonfiguriert, dessen Werte (VPI 1 und VCI 32) z. B. für eine ATM-Verbindung der Telekom geeignet sind.



Hinweis

Die ATM-Encapsulierungen sind in den RFCs 1483 und 2684 beschrieben. Sie finden die RFCs auf den entsprechenden Seiten der IETF (www.ietf.org/rfc.html).

10.2.1.1 Neu

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

The screenshot shows the configuration interface for a bintec R3800 device. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'WAN' category is expanded, showing 'Internet + Einwählen', 'ATM', 'Standleitung', and 'Real Time Jitter Control'. The 'ATM' option is selected.

The main content area is titled 'Profile' and has sub-tabs for 'Dienstkategorien' and 'OAM-Regelung'. The 'ATM-Profilparameter' section contains the following fields:

- Provider: - Benutzerdefiniert -
- Beschreibung: (empty text field)
- ATM-Schnittstelle: fcca-3-0
- Typ: Ethernet über ATM
- Virtual Path Identifier (VPI): 8
- Virtual Channel Identifier (VCI): 32
- Encapsulierung: LLC Bridged no FCS
- Einstellungen für Ethernet über ATM:
 - Standard-Ethernet für PPPoE-Schnittstellen: Aktiviert
 - Adressmodus: Statisch DHCP
 - IP-Adresse/Netzmaske: IP-Adresse [] Netzmaske [] with a 'Hinzufügen' button.
 - MAC-Adresse: [] with a checked box for 'Voreingestellte verwenden'.

At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 120: WAN -> ATM -> Profile -> Neu

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

Felder im Menü Profile ATM Profilparameter

Feld	Beschreibung
Provider	Wählen Sie eines der vorkonfigurierten ATM-Profil für Ihren Provider aus der Liste aus oder definieren Sie mit - <i>Benutzerdefiniert</i> - ein Profil.
Beschreibung	Nur für Provider = - <i>Benutzerdefiniert</i> - Geben Sie eine beliebige Beschreibung für die Verbindung ein.
ATM-Schnittstelle	Wählen Sie eine ATM-Schnittstelle aus.
Typ	Nur für Provider = - <i>Benutzerdefiniert</i> - Wählen Sie das Protokoll für die ATM-Verbindung aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Ethernet über ATM</i> (Standardwert): Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Ethernet über ATM (EthoA) verwendet. • <i>Geroutete Protokolle über ATM</i>: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird Geroutete Protokolle über ATM (RPoA) verwendet. • <i>PPP über ATM</i>: Für die ATM-Verbindung (Permanent Virtual Circuit, PVC) wird PPP über ATM (PPPoA) verwendet.
Virtuelle Pfad-Identifizier (VPI)	Nur für Provider = - <i>Benutzerdefiniert</i> - Geben Sie den VPI-Wert der ATM-Verbindung ein. Der VPI ist die Identifikationsnummer des zu verwendenden virtuellen Pfades. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind 0 bis 255. Standardwert ist 8.
Virtuelle Kanal-Identifizier (VCI)	Nur für Provider = - <i>Benutzerdefiniert</i> - Geben Sie den VCI-Wert der ATM-Verbindung ein. Der VCI ist die Identifikationsnummer des virtuellen Kanals. Ein virtueller Kanal ist die logische Verbindung für den Transport von ATM-Zellen zwischen zwei oder mehreren Punkten. Verwenden Sie die Vorgaben Ihres Providers. Mögliche Werte sind 32 bis 65535.

Feld	Beschreibung
	Standardwert ist 32.
Enkapsulierung	<p>Nur für Provider = - <i>Benutzerdefiniert</i> -</p> <p>Wählen Sie die zu verwendende Enkapsulierung aus. Verwenden Sie die Vorgaben Ihres Providers.</p> <p>Mögliche Werte (nach RFC 2684):</p> <ul style="list-style-type: none"> • <i>LLC Bridged no FCS</i> (Standardwert für Ethernet über ATM): Wird nur für Typ = <i>Ethernet über ATM</i> angezeigt. <p>Bridged Ethernet mit LLC/SNAP-Enkapsulierung ohne Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> • <i>LLC Bridged FCS</i> : Wird nur für Typ = <i>Ethernet über ATM</i> angezeigt. <p>Bridged Ethernet mit LLC/SNAP-Enkapsulierung mit Frame Check Sequence (Prüfsummen).</p> <ul style="list-style-type: none"> • <i>VC-Multiplexing</i> (Standardwert für PPP über ATM): Bridged Ethernet ohne zusätzliche Enkapsulierung (Null Einkapselung) mit Frame Check Sequence (Prüfsummen).

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

Feld	Beschreibung
Standard-Ethernet für PPPoE-Schnittstellen	<p>Nur für Typ = <i>Ethernet über ATM</i></p> <p>Wählen Sie aus, ob diese Ethernet-over-ATM-Schnittstelle für alle PPPoE-Verbindungen verwendet werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Adressmodus	<p>Nur für Typ = <i>Ethernet über ATM</i></p> <p>Wählen Sie aus, auf welche Weise der Schnittstelle eine IP-Adresse zugewiesen werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Der Schnittstelle wird eine statische IP-Adresse in IP-Adresse/Netzmaske zugewiesen.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>DHCP</i>: Die Schnittstelle erhält dynamisch per DHCP eine IP-Adresse.
IP-Adresse/Netzmaske	<p>Nur für Adressmodus = <i>Statisch</i></p> <p>Geben Sie die IP-Adressen (IP-Adresse) und die entsprechenden Netzmasken (Netzmaske) der ATM-Schnittstellen ein. Fügen Sie weitere Einträge mit Hinzufügen hinzu.</p>
MAC-Adresse	<p>Geben Sie der routerinternen Schnittstelle der ATM-Verbindung eine MAC-Adresse, z. B. <i>00:a0:f9:06:bf:03</i>. Ein Eintrag wird nur in speziellen Fällen benötigt.</p> <p>Für Internetverbindungen ist es ausreichend, die Option Voreingestellte verwenden (Standardeinstellung) auszuwählen, wobei dann die MAC-Adresse des <i>en1-0</i> verwendet wird.</p>
DHCP-MAC-Adresse	<p>Nur für Adressmodus = <i>DHCP</i>.</p> <p>Geben Sie die MAC-Adresse der routerinternen Schnittstelle der ATM-Verbindung ein, z. B. <i>00:e1:f9:06:bf:03</i>.</p> <p>Sollte Ihnen Ihr Provider eine MAC-Adresse für DHCP zugewiesen haben, so tragen Sie diese hier ein.</p> <p>Sie haben auch die Möglichkeit, die Option Voreingestellte verwenden (Standardeinstellung) auszuwählen, wobei dann die MAC-Adresse des <i>en1-0</i> verwendet wird.</p>
DHCP-Hostname	<p>Nur für Adressmodus = <i>DHCP</i>.</p> <p>Geben Sie ggf. den beim Provider registrierten Host-Namen an, der von Ihrem Gerät für DHCP-Anfragen verwendet werden soll.</p> <p>Die maximale Länge des Eintrags beträgt 45 Zeichen.</p>

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

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

Feld	Beschreibung
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Einstellungen für PPP über ATM (erscheint nur für Typ = PPP über ATM), siehe auch

Feld	Beschreibung
Client-Typ	<p>Wählen Sie aus, ob die PPPoA-Verbindung permanent oder bei Bedarf aufgebaut werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Auf Anforderung</i> (Standardwert): Die PPPoA wird nur bei Bedarf aufgebaut, z. B. für den Internetzugang.

10.2.2 Dienstkategorien

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

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



Achtung

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

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

10.2.2.1 Neu

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

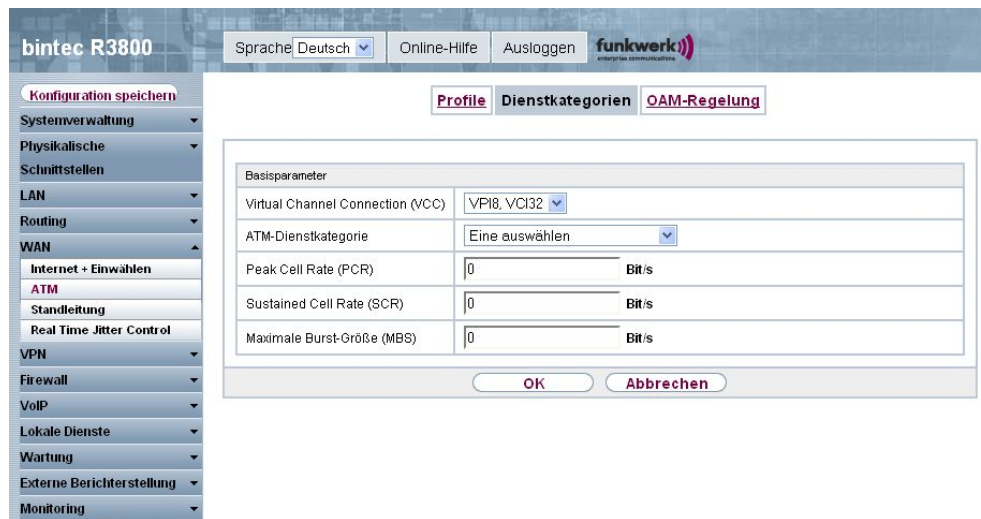


Abb. 121: WAN -> ATM -> Dienstkategorien -> Neu

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

Felder im Menü ATM Dienstkategorien

Feld	Beschreibung
Virtual Channel Connection (VCC)	Wählen Sie die bereits konfigurierte ATM-Verbindung (angezeigt durch die Kombination von VPI und VCI) aus, für welche die Servicekategorie festgelegt werden soll.
ATM-Dienstkategorie	<p>Wählen Sie aus, auf welche Art der Datenverkehr der ATM-Verbindung geregelt werden soll.</p> <p>Durch die Auswahl der ATM-Dienstkategorie wird implizit eine Priorität zugeordnet: von CBR (höchste Priorität) über VBR.1 /VBR.3 bis VBR (niedrigste Priorität).</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Unspecified Bit Rate (UBR)</i> (Standardwert): (Unspecified Bit Rate) Der Verbindung wird keine bestimmte Datenrate garantiert. Die Peak Cell Rate (PCR) legt die Grenze fest, bei deren Überschreiten Daten verworfen werden. Diese Kategorie eignet sich für nicht-kritische Anwendungen. • <i>Constant Bit Rate (CBR)</i>: (Constant Bit Rate) Der Verbindung wird eine garantierte Datenrate zugewiesen, die von

Feld	Beschreibung
	<p>der Peak Cell Rate (PCR) bestimmt wird. Diese Kategorie eignet sich für kritische Anwendungen (Real-Time), die eine garantierte Datenrate voraussetzen.</p> <ul style="list-style-type: none"> • <i>Variable Bit Rate V.1 (VBR.1)</i> : (Variable Bit Rate) Der Verbindung wird eine garantierte Datenrate zugewiesen (Sustained Cell Rate (SCR)). Diese darf insgesamt um das in Maximale Burst Grösse konfigurierte Volumen überschritten werden. Jeglicher weiterer ATM-Traffic wird verworfen. Die Peak Cell Rate (PCR) bildet dabei die maximal mögliche Datenrate. Die Kategorie eignet sich für nicht-kritische Anwendungen mit stoßweisem Datenaufkommen. • <i>Variable Bit Rate V.3 (VBR.3)</i> : (Variable Bit Rate) Der Verbindung wird eine garantierte Datenrate zugewiesen (Sustained Cell Rate (SCR)). Diese darf insgesamt um das in Maximale Burst Grösse (MBS) konfigurierte Volumen überschritten werden. Weiterer ATM-Traffic wird markiert und je nach Auslastung des Zielnetzes mit niedriger Priorität behandelt, d. h. wird bei Bedarf verworfen. Die Peak Cell Rate (PCR) bildet dabei die maximal mögliche Datenrate. Diese Kategorie eignet sich für kritische Anwendungen mit stoßweisem Datenaufkommen.
Peak Cell Rate (PCR)	<p>Geben Sie einen Wert für die maximale Datenrate in Bits pro Sekunde ein.</p> <p>Mögliche Werte: 0 bis 10000000.</p> <p>Der Standardwert ist 0.</p>
Sustained Cell Rate (SCR)	<p>Nur für ATM-Dienstkategorie = <i>Variable Bit Rate V.1 (VBR.1)</i> oder <i>Variable Bit Rate V.3 (VBR.3)</i></p> <p>Geben Sie einen Wert für die mindestens zur Verfügung stehende, garantierte Datenrate in Bits pro Sekunde ein.</p> <p>Mögliche Werte: 0 bis 10000000.</p> <p>Der Standardwert ist 0.</p>
Maximale Burst-Größe (MBS)	<p>Nur für ATM-Dienstkategorie = <i>Variable Bit Rate V.1 (VBR.1)</i> oder <i>Variable Bit Rate V.3 (VBR.3)</i></p> <p>Geben Sie hier einen Wert für die maximale Anzahl in Bits pro</p>

Feld	Beschreibung
	<p>Sekunde ein, um welche die PCR kurzzeitig überschritten werden darf.</p> <p>Mögliche Werte: 0 bis 100000.</p> <p>Der Standardwert ist 0.</p>

10.2.3 OAM-Regelung

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



Hinweis

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

Zur Überwachung der ATM-Verbindung stehen zwei Mechanismen zur Verfügung: Loop-back Tests und OAM Continuity Check (OAM CC). Sie können unabhängig voneinander konfiguriert werden.



Achtung

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

Im Menü **WAN -> ATM -> OAM-Regelung** wird eine Liste aller überwachten OAM-Fluss-Levels angezeigt.

10.2.3.1 Neu

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

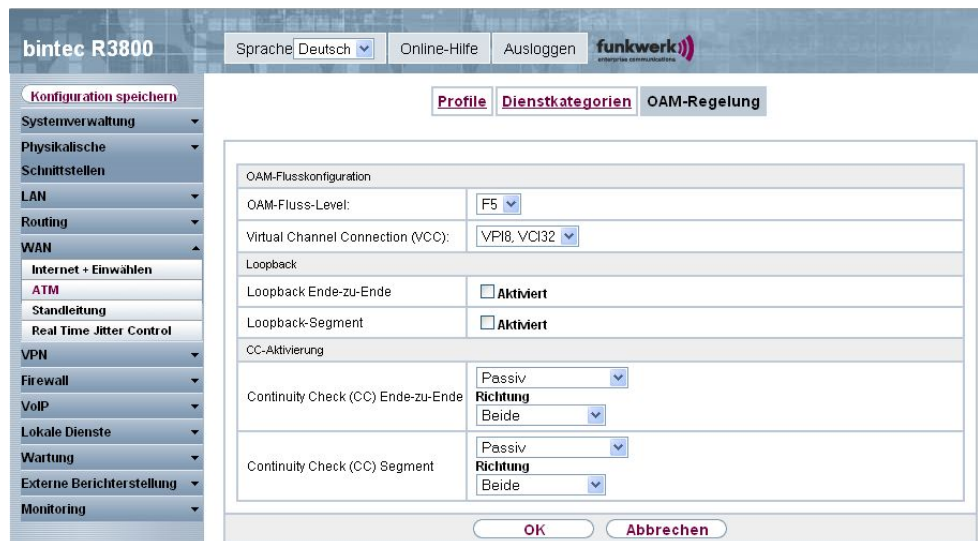


Abb. 122: WAN -> ATM -> OAM-Regelung -> Neu

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

Felder im Menü OAM-Regelung OAM-Flusskonfiguration

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

Felder im Menü OAM-Regelung Loopback

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

Feld	Beschreibung
	<p>Geben Sie ein, wieviele direkt aufeinanderfolgende Loopback-Zellen ausbleiben dürfen, bevor die Verbindung als unterbrochen ("inaktiv") angesehen wird.</p> <p>Mögliche Werte sind 1 bis 99.</p> <p>Standardwert ist 5.</p>

Felder im Menü OAM-Regelung CC-Aktivierung

Feld	Beschreibung
<p>Continuity Check (CC) Ende-zu-Ende</p>	<p>Wählen Sie aus, ob Sie den OAM-CC-Test für die Verbindung zwischen den Endpunkten der VCC bzw. VPC aktivieren wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • <i>Kein Aushandeln</i>: Je nach Einstellung im Feld Richtung werden OAM CC Requests entweder gesendet und/oder beantwortet. Es findet keine CC-Aushandlung statt. • <i>Keiner</i>: Die Funktion ist nicht aktiv. <p>Wählen Sie außerdem aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • <i>Sink</i>: CC-Daten werden empfangen. • <i>Quelle</i>: CC-Daten werden generiert. • <i>Keiner</i>: Die Funktion ist nicht aktiv.
<p>Continuity Check (CC) Segment</p>	<p>Wählen Sie aus, ob Sie den OAM-CC-Test für die Segment-Verbindung (Segment=Verbindung des lokalen Endpunkts bis zum nächsten Verbindungspunkt) der VCC bzw. VPC aktivieren</p>

Feld	Beschreibung
	<p>wollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) beantwortet. • <i>Aktiv</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet. • <i>Beide</i>: OAM CC Requests werden nach der CC-Aushandlung (CC activation negotiation) gesendet und beantwortet. • <i>Kein Aushandeln</i>: Je nach Einstellung im Feld Richtung werden OAM CC Requests entweder gesendet und/oder beantwortet, es findet keine CC-Aushandlung statt. • <i>Keiner</i>: Die Funktion ist nicht aktiv. <p>Wählen Sie weiterhin aus, ob die Testzellen des OAM CC gesendet bzw. empfangen werden sollen.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): CC-Daten werden sowohl empfangen als auch generiert. • <i>Sink</i>: CC-Daten werden empfangen. • <i>Quelle</i>: CC-Daten werden generiert. • <i>Keiner</i>: Die Funktion ist nicht aktiv.

10.3 Standleitung

Standleitung ist eine permanente (stehende) Verbindung zweier Kommunikationspartner über ein Telekommunikationsnetzwerk. Im Gegensatz zu einer Wählleitung steht der gesamte Übertragungsweg immer zur Verfügung. Die Standleitung kann nicht vom Teilnehmer über ein Wahlverfahren aufgebaut werden und hat daher keine Rufnummer. Die Verbindung muss vom Netzbetreiber hergestellt werden.

10.3.1 Schnittstellen

Im Menü **WAN** -> **Standleitung** -> **Schnittstellen** wird eine Liste aller automatisch generierter Standleitungsverbindungen angezeigt. Zur automatischen Generierung ist die Konfiguration der entsprechenden ISDN-Schnittstelle nötig.

bintec R4100 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Schnittstellen

Automatisch generiert von BRI (ISDN-S0)

Beschreibung	Typ	Protokoll	Port	Status	Aktion

Automatisch generiert von PRI (ISDN-S2M)

Beschreibung	Typ	Protokoll	Port	Status	Aktion


Automatisch generiert von Seriell

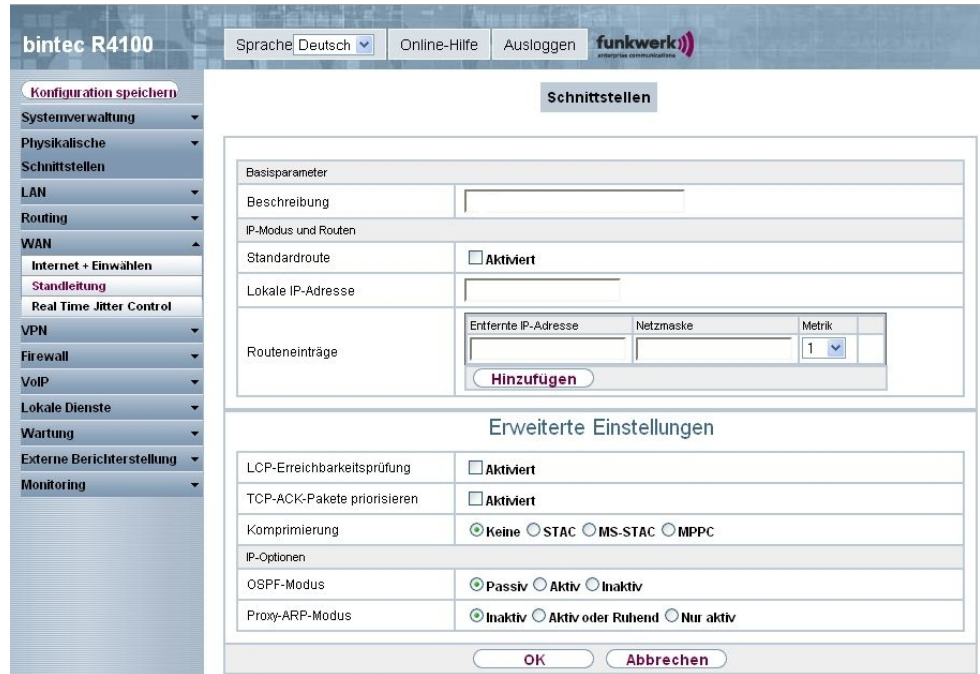
Beschreibung	Typ	Protokoll	Port	Status	Aktion
si4-0	Keiner	PPP		+	⬆️⬆️
si4-1	Keiner	PPP		+	⬆️⬆️

Systemverwaltung
 Physikalische
 Schnittstellen
 LAN
 Routing
 WAN
 Internet + Einwählen
 Standleitung
 Real Time Jitter Control
 VPN
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

Abb. 123: WAN -> Standleitung -> Schnittstellen

10.3.1.1 Bearbeiten

Wählen Sie die Schaltfläche  um die Konfiguration der entsprechenden Standleitung zu bearbeiten.



The screenshot shows the configuration page for a WAN interface on a bintec R4100 device. The page is titled 'Schnittstellen' and is divided into two main sections: 'Basisparameter' and 'Erweiterte Einstellungen'.

Basisparameter:

- Beschreibung:** A text input field.
- IP-Modus und Routen:**
 - Standardroute:** A checkbox labeled 'Aktiviert'.
 - Lokale IP-Adresse:** A text input field.
 - Routeneinträge:** A table with columns for 'Entfernte IP-Adresse', 'Netzmaske', and 'Metrik'. The 'Metrik' column has a dropdown menu set to '1'. Below the table is a 'Hinzufügen' button.

Erweiterte Einstellungen:

- LCP-Erreichbarkeitsprüfung:** A checkbox labeled 'Aktiviert'.
- TCP-ACK-Pakete priorisieren:** A checkbox labeled 'Aktiviert'.
- Komprimierung:** Radio buttons for 'Keine' (selected), 'STAC', 'MS-STAC', and 'MPPC'.
- IP-Optionen:**
 - OSPF-Modus:** Radio buttons for 'Passiv' (selected), 'Aktiv', and 'Inaktiv'.
 - Proxy-ARP-Modus:** Radio buttons for 'Inaktiv' (selected), 'Aktiv oder Ruhend', and 'Nur aktiv'.

At the bottom of the page are 'OK' and 'Abbrechen' buttons.

Abb. 124: WAN -> Standleitung -> Schnittstellen -> Automatisch generiert von BRI (ISDN-S0) -> 

Das Menü WAN -> Standleitung -> Schnittstellen -> Automatisch generiert von BRI (ISDN-S0) ->  besteht aus folgenden Feldern:

Felder im Menü Standleitung Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung für die Verbindung ein.

Felder im Menü Schnittstellen IP-Modus und Routen

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

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Tragen Sie hier die IP-Adresse ein, die Sie von Ihrem Netzbetreiber erhalten haben.
Routeneinträge	Definieren Sie weitere Routeneinträge für diesen Verbindungsparten. Fügen Sie mit Hinzufügen neue Einträge hinzu.

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
LCP-Erreichbarkeitsprüfung	Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle überprüft werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
TCP-ACK-Pakete priorisieren	Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Komprimierung	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. Mögliche Werte: <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

Felder im Menü Erweiterte Einstellungen IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus ob über die Schnittstelle OSPF-Protokoll-Pakete gesendet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine 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 aktiv, d. h. über diese Schnittstelle werden OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob und wie die ARP-Requests für diesen spezifischen Verbindungspartner beantwortet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>(Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • <i>Aktiv oder ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> 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 Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.

The screenshot shows the configuration interface for a bintec R4100 device. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische, Schnittstellen, LAN, Routing, WAN, Internet + Einwählen, Standleitung, Real Time Jitter Control, VPN, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The main content area is titled 'Schnittstellen' and is divided into two sections: 'Basisparameter' and 'Erweiterte Einstellungen'.

Basisparameter:

- Beschreibung: [Text input field]
- IP-Modus und Routen:
 - Standardroute: Aktiviert
 - Lokale IP-Adresse: [Text input field]
- Routeneinträge:

Entfernte IP-Adresse	Netzmaske	Metrik
[Text input field]	[Text input field]	1

Erweiterte Einstellungen:

- LCP-Erreichbarkeitsprüfung: Aktiviert
- TCP-ACK-Pakete priorisieren: Aktiviert
- Komprimierung: Keine STAC MS-STAC MPPC
- IP-Optionen:
 - OSPF-Modus: Passiv Aktiv Inaktiv
 - Proxy-ARP-Modus: Inaktiv Aktiv oder Ruhend Nur aktiv

Buttons: OK, Abbrechen

Abb. 125: WAN -> Standleitung -> Schnittstellen -> Automatisch generiert von PRI (ISDN-S2M) ->

Das Menü WAN -> Standleitung -> Schnittstellen -> Automatisch generiert von PRI (ISDN-S2M) -> besteht aus folgenden Feldern:

Felder im Menü Schnittstellen Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung für die Verbindung ein.

Felder im Menü Schnittstellen IP-Modus und Routen

Feld	Beschreibung
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Tragen Sie hier die IP-Adresse ein, die Sie von Ihrem Netzbetreiber erhalten haben.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbin-

Feld	Beschreibung
	<p>dungsparten.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle überprüft werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
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

Felder im Menü Erweiterte Einstellungen IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus ob über die Schnittstelle OSPF-Protokoll-Pakete gesendet werden.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none">• <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine 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 aktiv, d. h. über diese Schnittstelle werden OSPF-Protokoll-Pakete gesendet.• <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob und wie die ARP-Requests für diesen spezifischen Verbindungspartner beantwortet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Inaktiv</i>(Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner.• <i>Aktiv oder ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> 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 Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.

The screenshot shows the configuration page for 'Schnittstellen' (Interfaces) under the 'WAN' section. The left sidebar contains a navigation menu with options like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Routing', 'WAN', 'Internet + Einwählen', 'Standleitung', 'Real Time Jitter Control', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The main content area is titled 'Schnittstellen' and is divided into two sections: 'Basisparameter' and 'Erweiterte Einstellungen'.

Basisparameter

- Beschreibung: si4-0
- IP-Modus und Routen
 - Standardroute: Aktiviert
 - Lokale IP-Adresse: [Empty field]
- Routeneinträge:

Entfernte IP-Adresse	Netzmaske	Metrik
[Empty field]	[Empty field]	1

Erweiterte Einstellungen

- LCP-Erreichbarkeitsprüfung: Aktiviert
- TCP-ACK-Pakete priorisieren: Aktiviert
- Komprimierung: Keine STAC MS-STAC MPPC
- IP-Optionen
 - OSPF-Modus: Passiv Aktiv Inaktiv
 - Proxy-ARP-Modus: Inaktiv Aktiv oder Ruhend Nur aktiv

Buttons: OK, Abbrechen

Abb. 126: WAN -> Standleitung -> Schnittstellen -> Automatisch generiert von Seriell ->

Das Menü WAN -> Standleitung -> Schnittstellen -> Automatisch generiert von Seriell -> besteht aus folgenden Feldern:

Felder im Menü Schnittstellen Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Beschreibung für die Verbindung ein.

Felder im Menü Schnittstellen IP-Modus und Routen

Feld	Beschreibung
Standardroute	Wählen Sie aus, ob die Route zu diesem Verbindungspartner als Standard-Route festgelegt werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Lokale IP-Adresse	Tragen Sie hier die IP-Adresse ein, die Sie von Ihrem Netzbetreiber erhalten haben.
Routeneinträge	Definieren Sie weitere Routing-Einträge für diesen Verbin-

Feld	Beschreibung
	<p>dungsparten.</p> <p>Fügen Sie mit Hinzufügen neue Einträge hinzu.</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle überprüft werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
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

Felder im Menü Erweiterte Einstellungen IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus ob über die Schnittstelle OSPF-Protokoll-Pakete gesendet werden.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiv, d. h. über diese Schnittstelle werden keine 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 aktiv, d. h. über diese Schnittstelle werden OSPFProtokoll- Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob und wie die ARP-Requests für diesen spezifischen Verbindungspartner beantwortet werden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i>(Standardwert): Deaktiviert Proxy-ARP für diesen Verbindungspartner. • <i>Aktiv oder ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum Verbindungspartner <i>aktiv</i> oder <i>ruhend</i> 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 Verbindungspartner <i>aktiv</i> ist, wenn also bereits eine Verbindung zum Verbindungspartner besteht.

10.4 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.

10.4.1 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.

10.4.1.1 Neu

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



Abb. 127: **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 Regulierte Schnittstellen Grundeinstellungen

Feld	Beschreibung
Schnittstelle	Legen Sie fest, für welche Schnittstellen die Sprachübertragung optimiert werden soll.
Kontrollmodus	Wählen Sie den Modus für die Optimierung aus. Mögliche Werte: <ul style="list-style-type: none"> <i>Nur kontrollierte RTP-Streams</i>(Standardwert): Anhand der Daten, die über das Media Gateway geroutet wer-

Feld	Beschreibung
	<p>den, erkennt das System Sprachdaten-Verkehr und optimiert die Sprachübertragung.</p> <ul style="list-style-type: none">• <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 11 VPN

11.1 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) integriert werden. Die funkwerk-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.

11.1.1 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.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes the language set to 'Deutsch', links for 'Online-Hilfe' and 'Ausloggen', and the 'funkwerk' logo. A left-hand menu lists various system management categories, with 'VPN' expanded to show 'IPSec' as the selected option. The main content area is titled 'IPSec-Peers' and contains sub-tabs for 'Phase-1-Profil', 'Phase-2-Profil', 'IP Pools', and 'Optionen'. Below these tabs is a table with columns for 'Prio', 'Beschreibung', 'Peer-Adresse', 'Peer-ID', 'Phase-1-Profil', 'Phase-2-Profil', and 'Status'. The table is currently empty, and a 'Neu' button is visible below it. Search and filter controls are present at the top of the table area.

Abb. 128: 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 524.

11.1.1.1 Neu

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

bintec R1200 Sprache: Deutsch

Konfiguration speichern

Systemverwaltung **Physikalische Schnittstellen**

LAN **Wireless LAN** **Routing** **WAN** **VPN**

IPSec **L2TP** **PPTP** **GRE** **Zertifikate** **Firewall** **VoIP** **Lokale Dienste** **Wartung** **Externe Berichterstellung** **Monitoring**

IPSec-Peers **Phase-1-Profil** **Phase-2-Profil** **IP Pools** **Optionen**

Peer-Parameter

Administrativer Status: Aktiv Inaktiv

Beschreibung: Peer-1

Peer-Adresse:

Peer-ID: Fully Qualified Domain Name (FQDN)

Preshared Key:

Schnittstellenrouten

IP-Adressenvergabe: Statisch IKE-Konfigurationsmodus

Standardroute: Aktiviert

Lokale IP-Adresse:

Routeneinträge:

Entfernte IP-Adresse	Netzmaske	Metrik
<input type="text"/>	<input type="text"/>	1 <input type="button" value="↓"/>

Erweiterte Einstellungen

Erweiterte IPSec-Optionen

Phase-1-Profil: * PSK Multiproposal

Phase-2-Profil: * Multi-Proposal

Startmodus: Auf Anforderung Immer aktiv

Erweiterte IP-Optionen

Überprüfung der Rückroute: Aktiviert

Proxy ARP: Inaktiv Aktiv oder Ruhend Nur aktiv

IPSec-Callback

Modus: Inaktiv

Abb. 129: VPN -> IPSec -> IPSec-Peers -> Neu

Das Menü VPN -> IPSec -> IPSec-Peers -> Neu besteht aus folgenden Feldern:

Felder im Menü IPSec-Peers Pee-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

Feld	Beschreibung
	ration zunächst nicht zur Verfügung.
Beschreibung	Geben Sie eine Beschreibung des Peers ein, die diesen identifiziert. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Peer-Adresse	Geben Sie die offizielle IP-Adresse des Peers bzw. seinen auflösbaren Host-Namen ein. Die Eingabe kann in bestimmten Konfigurationen entfallen, wobei Ihr Gerät dann keine IPSec-Verbindung initiieren kann.
Peer-ID	Wählen Sie den ID-Typ aus und geben Sie die ID des Peers ein. Die Eingabe kann in bestimmten Konfigurationen entfallen. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen. Mögliche ID-Typen: <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> Auf dem Peer-Gerät entspricht diese ID dem Parameter Lokaler ID-Wert .
Preshared Key	Geben Sie das mit dem Peer vereinbarte Passwort ein. Die maximal mögliche Länge des Eintrags beträgt 50 Zeichen. Alle Zeichen sind möglich außer <i>0x</i> am Anfang des Eintrags.

Felder im Menü IPSec-Peers Schnittstellenrouten

Feld	Beschreibung
IP-Adressenvergabe	Wählen Sie den Konfigurationsmodus der Schnittstelle aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>Statisch</i> (Standardwert): Sie geben eine Statische IP-Adresse ein.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>IKE-Konfigurationsmodus</i>: Sie wählen eine IP-Adresse aus dem konfigurierten IP-Pool aus.
IP-Zuordnungspool	<p>Nur bei IP-Adressenvergabe = <i>IKE-Konfigurationsmodus</i></p> <p>Wählen Sie einen im Menü VPN -> 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-Adressvergabe = <i>Statisch</i></p> <p>Wählen Sie aus, ob die Route zu diesem IPSec Peer als Standard-Route 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 wenn Standardroute <i>nicht aktiviert</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>
Routeneinträge	<p>Definieren Sie Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <i>Netzmaske</i>: Netzmaske zu Ziel IP-Address. • <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 Erweiterte IPSec-Optionen

Feld	Beschreibung
Phase-1-Profil	<p>Wählen Sie ein schon im Menü Phase-1-Profile konfiguriertes Profil für die Phase 1 aus. Sie haben auch die Möglichkeit, das in Phase-1-Profile als Standard markierte Profil auszuwählen: <i>Keines (Standardprofil verwenden)</i>.</p>
Phase-2-Profil	<p>Wählen Sie ein schon im Menü Phase-2-Profile konfiguriertes Profil für die Phase 2 aus. Sie haben auch die Möglichkeit, das</p>

Feld	Beschreibung
	in Phase-2-Profil als Standard markierte Profil auszuwählen: <i>Keines (Standardprofil verwenden).</i>
Startmodus	Wählen Sie aus, wie der Peer in den aktiven Zustand versetzt werden soll. Mögliche Werte: <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 Einstellungen** **Erweiterte IP-Optionen**

Feld	Beschreibung
Überprüfung der Rückroute	Wählen Sie aus, ob für die Schnittstelle zum Verbindungspartner eine Überprüfung der Rückroute aktiviert werden soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Proxy-ARP	Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen Verbindungspartner beantworten soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen IPsec Peer. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPsec Peer <i>aktiv</i> (aktiv) oder <i>ruhend</i> (ruhend) ist. Bei <i>ruhend</i> beantwortet Ihr Gerät lediglich den ARP-Request, der Verbindungsaufbau erfolgt erst, wenn jemand tatsächlich die Route nutzen will. • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum IPsec Peer <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum IPsec Peer besteht.

IPsec-Callback

Um Hosts, die nicht über feste IP-Adressen verfügen, eine sichere Verbindung über das In-

ternet zu ermöglichen, unterstützen **bintec**-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: Mit Hilfe eines direkten ISDN-Rufs bei einem Peer kann diesem signalisiert werden, dass man online ist und den Aufbau eines IPSec-Tunnels über das Internet erwartet. Sollte der gerufene Peer derzeit keine Verbindung zum Internet haben, wird er durch den ISDN-Ruf veranlasst, eine Verbindung aufzubauen. Dieser ISDN-Ruf verursacht (je nach Einsatzland) keine Kosten, da der ISDN-Ruf von Ihrem Gerät nicht angenommen werden muss. Die Identifikation des Anrufers durch dessen ISDN-Rufnummer genügt als Information, um einen Tunnelaufbau zu initiieren.

Um diesen Dienst einzurichten, muß zunächst auf der passiven Seite im Menü **Physikalische Schnittstellen -> ISDN-Ports -> MSN-Konfiguration -> Neu** eine Rufnummer für den IPSec-Callback konfiguriert werden. Dazu steht für das Feld **Dienst** der Wert *IPSec* zur Verfügung. Dieser Eintrag sorgt dafür, dass auf dieser Nummer eingehende Rufe an den IPSec-Dienst geleitet werden.

Bei aktivem Callback wird, sobald ein IPSec-Tunnel benötigt wird, der Peer durch einen ISDN-Ruf veranlasst, diesen zu initiieren. Bei passivem Callback wird immer dann ein Tunnelaufbau zum Peer initiiert, wenn ein ISDN-Ruf auf der entsprechenden Nummer (**MSN** im Menü **Physikalische Schnittstellen -> ISDN-Ports -> MSN-Konfiguration -> Neu** für **Dienst** *IPSec*) eingeht. Auf diese Weise wird sichergestellt, dass beide Peers erreichbar sind und die Verbindung über das Internet zustande kommen kann. Es wird lediglich dann kein Callback ausgeführt, wenn bereits SAs (Security Associations) vorhanden sind, der Tunnel zum Peer also bereits besteht.



Hinweis

Wenn ein Tunnel zu einem Peer aufgebaut werden soll, wird vom IPSec- Daemon zunächst die Schnittstelle aktiviert, über die der Tunnel realisiert werden soll. Sofern auf dem lokalen Gerät IPSec mit DynDNS konfiguriert ist, wird die eigene IP-Adresse propagiert und erst dann der ISDN-Ruf an das entfernte Gerät abgesetzt. Auf diese Art ist sichergestellt, dass das entfernte Gerät das lokale auch tatsächlich erreichen kann, wenn es den Tunnelaufbau initiiert.

Übermittlung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Geräts über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs. Einschrän-

kungen, 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.funkwerk-ec.com. Bitte folgen Sie den Anweisungen der Online-Lizenzierung.

Vor Systemsoftware Release 7.1.4 unterstützte der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Auslösers auf indirektem Wege (z. B. über DynDNS) ermittelt werden konnte. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse über ISDN umgangen. Darüber hinaus ermöglicht es diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus (Haupt Modus) für den Tunnelaufbau zu verwenden.

Funktionsweise: Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht. Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in *Felder im Menü Erweiterte Einstellungen IPSec-Callback* auf Seite 339 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 des gerufenen Peers die Informationen 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 der Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.
- (6) Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.



Hinweis

In manchen Ländern (z. B. in der Schweiz) kann auch der Ruf im D-Kanal Kosten verursachen. Eine falsche Konfiguration der angerufenen Seite kann dazu führen, dass die angerufene Seite den B-Kanal öffnet und somit Kosten für die anrufende Seite verursacht werden.

Felder im Menü Erweiterte Einstellungen 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

Feld	Beschreibung
	<p>zum Peer. Es werden keine ISDN-Rufe an das entfernte Gerät abgesetzt, um dieses zum Aufbau eines IPSec-Tunnels zu veranlassen.</p> <ul style="list-style-type: none"> • <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).
Eingehende ISDN-Nummer	<p>Nur für Modus = <i>Passiv</i> oder <i>Beide</i> .</p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number). Es können auch Wildcards verwendet werden.</p>
Ausgehende ISDN-Nummer	<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 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 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.)

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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 des D-Kanals 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 des D-Kanals 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 und auf B-Kanal zurückgehen</i></p> <p>Wählen Sie aus, in welchem D-Kanal-Modus Ihr Gerät versuchen soll, die IP-Adresse zu übertragen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LLC</i> (Standardwert): Die IP-Adresse wird in den "LLC Information Elements" des D-Kanals übertragen. • <i>SUBADDR</i>: Die IP-Adresse wird in den Subaddress "Information Elements" des D-Kanals übertragen. • <i>LLC und SUBADDR</i>: Die IP-Adresse wird sowohl in den "LLC-" als auch in den "Subaddress Information Elements" übertragen.

11.1.2 Phase-1-Profile

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

The screenshot shows the configuration interface for a bintec R1200 device. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The VPN section is expanded to show sub-options: IPsec, L2TP, PPTP, GRE, and Zertifikate. The main content area is titled 'IPSec-Peers' and 'Phase-1-Profile'. It features a table with columns for 'Standard', 'Beschreibung', 'Proposals', 'Authentifizierung', 'Modus', 'DH-Gruppe', and 'Lebensdauer'. The table is currently empty. Above the table, there are controls for 'Ansicht' (20 pro Seite), 'Filtern in' (Keiner), and 'gleich'. Below the table are three buttons: 'Neu', 'OK', and 'Abbrechen'.

Abb. 130: VPN -> IPsec -> Phase-1-Profile

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

11.1.2.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 device. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN, IPsec, L2TP, PPTP, GRE, Zertifikate, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The main area is titled 'Phase-1-Profile' and contains the following fields:

- Phase-1-Parameter (IKE)**
 - Beschreibung: PSK Multiproposal
 - Proposals: A table with columns for Verschlüsselung (AES), Authentifizierung (MD5), and Aktiviert (checkbox). Three rows are shown, all with AES and MD5 selected and the checkbox checked.
 - DH-Gruppe: Radio buttons for 1 (768 Bit), 2 (1024 Bit) (selected), and 5 (1536 Bit).
 - Lebensdauer: 14400 Sekunden, 0 kBytes
 - Authentifizierungsmethode: Preshared Keys
 - Modus: Radio buttons for Main Modus (ID Protect), Aggressiv (selected), and Strikt.
 - Lokaler ID-Typ: Fully Qualified Domain Name (FQDN)
 - Lokaler ID-Wert: r1200
- Erweiterte Einstellungen**
 - Erreichbarkeitsprüfung: Automatische Erkennung
 - Blockzeit: 30 Sekunden
 - NAT-Traversal: Aktiviert

Buttons for 'OK' and 'Abbrechen' are at the bottom.

Abb. 131: VPN -> IPsec -> Phase-1-Profil -> Neu

Das Menü VPN -> IPsec -> Phase-1-Profil -> Neu besteht aus folgenden Feldern:

Felder im Menü Phase-1-Profil Phase-1-Parameter (IKE)

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, welche die Art der Regel eindeutig identifiziert.
Proposals	<p>In diesem Feld können Sie auf Ihrem Gerät jede Kombination aus Verschlüsselungs- und Nachrichten-Hash-Algorithmen für IKE Phase 1 auswählen. Die Kombination von sechs Verschlüsselungsalgorithmen und vier Nachrichten-Hash-Algorithmen ergibt 24 mögliche Werte in diesem Feld. Mindestens ein Proposal muss vorhanden sein. Daher kann die erste Zeile der Tabelle nicht deaktiviert werden.</p> <p>Verschlüsselungsalgorithmen (Verschlüsselung):</p> <ul style="list-style-type: none"> • <i>3DES</i> (Standardwert): 3DES ist eine Erweiterung des DES Algorithmus mit einer effektiven Schlüssellänge von 112 Bit, was als sicher eingestuft wird. Es ist der langsamste Algorith-

Feld	Beschreibung
	<p>mus, 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. • <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): MD 5 (Message Digest #5) ist ein älterer Hash Algorithmus. Wird mit 96 Bit Digest Length für IPSec verwendet. • <i>SHA1</i> : SHA 1 (Secure Hash Algorithmus #1) ist ein Hash Algorithmus, der von der NSA (United States National Security Association) entwickelt wurde. Er wird als sicher eingestuft, ist

Feld	Beschreibung
	<p>aber langsamer als MD5. Wird mit 96 Bit Digest Length für IP-Sec verwendet.</p> <ul style="list-style-type: none"> • <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>Die Diffie-Hellman-Gruppe definiert den Parametersatz, der für die Schlüsselberechnung während der Phase 1 zugrunde gelegt wird. "MODP", wie es von bintec-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 bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p>

Feld	Beschreibung
	<p>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> .</p> <p>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> .</p> <p>Der Defaultwert lt. RFC wird verwendet, wenn <i>0</i> Sekunden und <i>0</i> KBytes eingetragen werden.</p>
Authentifizierungsmethode	<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 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 Authentifizierungsmethode = <i>DSA-Signatur</i>, <i>RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Dieses Feld ermöglicht Ihnen, eines Ihrer eigenen Zertifikate für die Authentifizierung zu wählen. Es zeigt die Indexnummer dieses Zertifikats und den Namen an, unter dem es gespeichert ist. Dieses Feld wird nur bei Authentifizierungseinstellungen auf Zertifikatbasis angezeigt und weist darauf hin, dass ein Zertifikat zwingend erforderlich ist.</p>
Modus	<p>Wählen Sie den Phase-1-Modus aus.</p> <p>Mögliche Werte:</p>

Feld	Beschreibung
	<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>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>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 Subjektname aus Zertifikat verwenden angezeigt.</p> <p>Wenn Sie die Option Subjektname aus Zertifikat verwenden aktivieren, wird der erste im Zertifikat angegebene Subjekt-Alternativname oder, falls keiner angegeben ist, der Subjektname des Zertifikats verwendet.</p> <p>Beachten Sie: Falls Sie Zertifikate für die Authentifizierung nutzen und Ihr Zertifikat Subjekt-Alternativnamen enthält (siehe Zertifikate auf Seite 381), müssen Sie hier achtgeben, da Ihr Gerät per Standard den ersten Subjekt-Alternativnamen wählt. Stellen Sie sicher, dass Sie und Ihr Peer beide den gleichen Namen nutzen, d. h. dass Ihre lokale ID und die Peer-ID, die Ihr</p>

Feld	Beschreibung
	Partner für Sie konfiguriert, identisch sind.

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 **Aktiv-Überprüfung** 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>Wählen Sie die Methode aus, mit der die Funktionalität der IP-Sec-Verbindung überprüft werden soll.</p> <p>Neben dem Standardverfahren Dead Peer Detection (DPD) ist auch das (proprietäre) Heartbeat-Verfahren implementiert. Dieses sendet bzw. empfängt je nach Konfiguration alle 5 Sekunden Signale, bei deren Ausbleiben die SA nach 20 Sekunden als ungültig verworfen wird</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <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) ge-

Feld	Beschreibung
	<p>mäß 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.</p> <ul style="list-style-type: none"> • <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.
Blockzeit	<p>Legen Sie fest, wie lange ein Peer für Tunnelaufbauten blockiert wird, nachdem ein Phase-1-Tunnelaufbau fehlgeschlagen ist. Dies betrifft nur lokal initiierte Aufbauversuche.</p> <p>Zur Verfügung stehen Werte von -1 bis 86400 (Sekunden), der Wert -1 bedeutet die Übernahme des Wertes im Standardprofil, der Wert 0, dass der Peer in keinem Fall blockiert wird.</p> <p>Standardwert ist 30.</p>
NAT-Traversal	<p>NAT-Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Geräte zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.</p> <p>Ohne NAT-T kann es zwischen IPSec und NAT zu Inkompatibilitäten kommen (siehe RFC 3715, Abschnitt 2). Diese behindern vor allem den Aufbau eines IPSec-Tunnels von einem Host innerhalb eines LANs und hinter einem NAT-Gerät zu einem anderen Host bzw. Gerät. NAT-T ermöglicht derartige Tunnel ohne Konflikte mit NAT-Geräten, aktiviertes NAT wird vom IPSec-Daemon automatisch erkannt und NAT-T wird verwendet.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
CA-Zertifikate	<p>Nur für Authentifizierungsmethode = <i>DSA-Signatur</i>, <i>RSA-Signatur</i> oder <i>RSA-Verschlüsselung</i></p> <p>Wenn Sie die Option Folgenden CA-Zertifikaten vertrauen</p>

Feld	Beschreibung
	aktivieren, können Sie bis zu drei CA-Zertifikate auswählen, die für dieses Profil akzeptiert werden sollen.
	Die Option ist nur konfigurierbar, wenn Zertifikate geladen sind.

11.1.3 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 web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'IPSec', 'L2TP', 'PPTP', 'GRE', 'Zertifikate', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'VPN' menu is expanded, and 'IPSec' is selected. The main content area displays a configuration page for 'Phase-2-Profile'. At the top of this page are tabs for 'IPSec-Peers', 'Phase-1-Profile', 'Phase-2-Profile', 'IP Pools', and 'Optionen'. Below the tabs is a search and filter section with 'Ansicht: 20 pro Seite', 'Filtern in: Keiner', and 'gleich'. A table is shown with the following columns: 'Standard', 'Beschreibung', 'Proposals', 'PFS-Gruppe', and 'Lebensdauer'. The 'Standard' column contains a checkbox. Below the table are three buttons: 'Neu', 'OK', and 'Abbrechen'.

Abb. 132: VPN -> IPSec -> Phase-2-Profile

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

11.1.3.1 Neu

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

The screenshot shows the configuration page for a Phase-2-Profile (IPSEC) on a bintec R1200 device. The interface includes a navigation menu on the left with options like Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN, IPsec, L2TP, PPTP, GRE, Zertifikate, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The main configuration area is titled 'Phase-2-Parameter (IPSEC)' and contains the following fields:

- Beschreibung:** Multi-Proposal
- Proposals:** A table with columns for Verschlüsselung, Authentifizierung, and Aktiviert. The values are AES, MD5, and checked for all three rows.
- PFS-Gruppe verwenden:** Aktiviert, with radio buttons for 1 (768 Bit), 2 (1024 Bit) (selected), and 5 (1536 Bit).
- Lebensdauer:** 7200 Sekunden, 0 kBytes

Below this is the 'Erweiterte Einstellungen' section:

- IP-Komprimierung:** Aktiviert
- Erreichbarkeitsprüfung:** Automatische Erkennung
- PMTU propagieren:** Aktiviert

Buttons for 'OK' and 'Abbrechen' are at the bottom.

Abb. 133: VPN -> IPsec -> Phase-2-Profil -> Neu

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

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

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung ein, die das Profil eindeutig identifiziert. Die maximal mögliche Länge des Eintrags beträgt 255 Zeichen.
Proposals	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. Verschlüsselungsalgorithmen (Verschlüsselung): <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-128</i>: Rijndael wurde aufgrund seines schnellen Schlüs-

Feld	Beschreibung
	<p>selaufbaus, 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.</p> <ul style="list-style-type: none"> • <i>AES-192</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speichieranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 192 bits angewendet. • <i>AES-256</i>: Rijndael wurde aufgrund seines schnellen Schlüsselaufbaus, der geringen Speichieranforderungen, der hohen Sicherheit gegen Angriffe und der allgemeinen Geschwindigkeit zum AES ernannt. Hier wird er mit einer Schlüssellänge von 256 bits angewendet. • <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>MD 5</i> (Standardwert): MD 5 (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>SHA 1</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>

Feld	Beschreibung
PFS-Gruppe verwenden	<p>Da PFS (Perfect Forward Secrecy) eine weitere Diffie-Hellman-Schlüsselberechnung erfordert, um neues Verschlüsselungsmaterial zu erzeugen, müssen Sie die Merkmale der Exponentiation wählen. Wenn Sie PFS aktivieren (Aktiviert), sind die Optionen die gleichen, wie bei der Konfiguration in Phase 1: Group. PFS wird genutzt, um die Schlüssel einer erneuerten Phase-2-SA zu schützen, auch wenn die Schlüssel der Phase-1-SA bekannt geworden sind.</p> <p>Das Feld hat folgende Optionen:</p> <ul style="list-style-type: none"> • <i>1 (768 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 768 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>2 (1024 Bit)</i> (Standardwert): Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1024 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen. • <i>5 (1536 Bit)</i>: Während der Diffie-Hellman-Schlüsselberechnung wird die modulare Exponentiation mit 1536 Bit genutzt, um das Verschlüsselungsmaterial zu erzeugen.
Lebensdauer	<p>Legen Sie fest, wie die Lebensdauer festgelegt wird, die ablaufen darf, bevor die Phase-2-SAs erneuert werden müssen.</p> <p>Die neuen SAs werden bereits kurz vor dem Ablauf der aktuellen SAs ausgehandelt. Der Standardwert beträgt gemäss RFC 2407 acht Stunden, das bedeutet, dass die Schlüssel erneuert werden, wenn acht Stunden abgelaufen sind.</p> <p>Folgende Optionen stehen für die Definition der Lebensdauer zur Verfügung:</p> <p>Eingabe in <i>Sekunden</i>: Geben Sie die Lebensdauer für Phase-2-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von 0 bis 2147483647 sein. Standardwert ist 28800.</p> <p>Eingabe in <i>KBytes</i>: 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>

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

Felder im Menü **Erweiterte Einstellungen**

Feld	Beschreibung
IP-Komprimierung	<p>Wählen Sie aus, ob eine Kompression vor der Datenverschlüsselung eingeschaltet wird. Das kann bei gut komprimierbaren Daten zu einer höheren Performance und geringerem zu übertragenden Datenvolumen führen. Bei schnellen Leitungen oder nicht komprimierbaren Daten wird von der Option abgeraten, da die Performance durch den erhöhten Aufwand bei der Kompression erheblich beeinträchtigt werden kann.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Erreichbarkeitsprüfung	<p>Wählen Sie, ob und in welcher Weise IPSec Heartbeats verwendet werden.</p> <p>Um feststellen zu können, ob eine Security Association (SA) noch gültig ist oder nicht, ist ein bintec 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>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>Automatische Erkennung</i>: Automatische Erkennung, ob die Gegenstelle ein bintec-Gerät ist. Wenn ja, wird Heartbeat beide (bei Gegenstelle mit bintec) oder keiner (bei Gegenstelle ohne bintec) gesetzt.
PMTU propagieren	<p>Wählen Sie aus, ob während der Phase 2 die PMTU (Path Maximum Transfer Unit) propagiert werden soll.</p>

Feld	Beschreibung
	Mit <i>Aktiviert</i> wird die Funktion aktiv.
	Standardmäßig ist die Funktion aktiv.

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

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere IP Pools einzurichten.

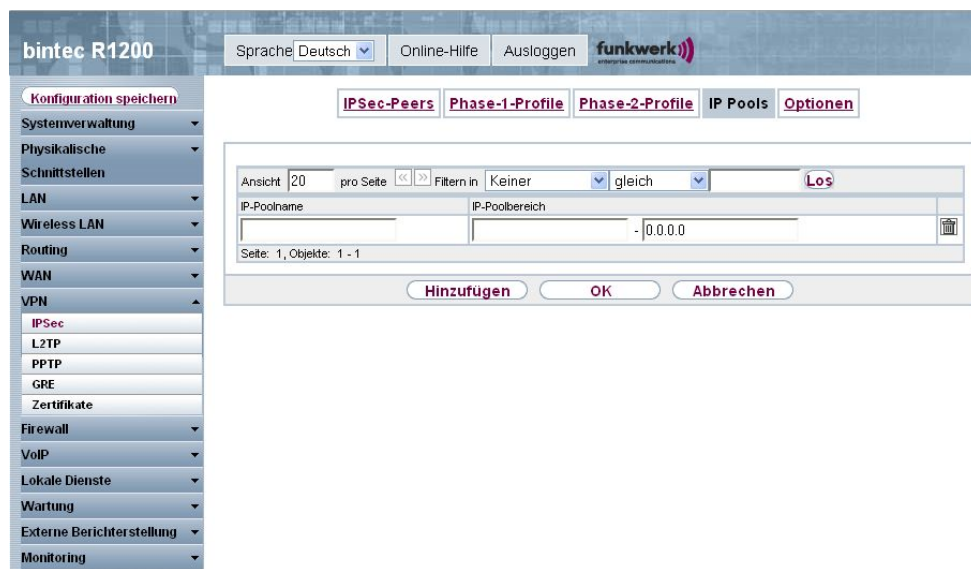


Abb. 134: VPN -> IPSec -> IP Pools -> Hinzufügen

Das Menü **VPN -> IPSec -> IP Pools -> Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Optionen IP Pools

Feld	Beschreibung
IP-Poolname	Geben Sie die Bezeichnung des IP-Pools ein.
IP-Poolbereich	Geben Sie im ersten Feld die erste IP-Adresse des Bereiches ein.

Feld	Beschreibung
	Geben Sie im zweiten Feld die letzte IP-Adresse des Bereiches ein.


11.1.5 Optionen

The screenshot shows the bintec R1200 VPN configuration interface. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a tree view with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'VPN' category is expanded to show 'IPSec', 'L2TP', 'PPTP', 'GRE', and 'Zertifikate'. The 'IPSec' sub-menu is selected, and the 'Optionen' tab is active. The main configuration area is divided into two sections: 'Globale Optionen' and 'Erweiterte Einstellungen'. 'Globale Optionen' includes 'IPSec aktivieren' (checked), 'Vollständige IPSec-Konfiguration löschen' (trash icon), and 'IPSec-Debug-Level' (set to 'Debug'). 'Erweiterte Einstellungen' includes various options like 'Initial Contact Message senden' (checked), 'SAs mit dem Status der ISP-Schnittstelle synchronisieren' (unchecked), 'Zero Cookies verwenden' (unchecked), 'Dynamische RADIUS-Authentifizierung' (unchecked), and 'PKI-Verarbeitungsoptionen' with sub-options for certificate payloads and CRLs.

Abb. 135: VPN -> IPSec -> Optionen

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

Felder im Menü Optionen 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

Feld	Beschreibung
	<p>IPSec-Konfiguration vorgenommen worden sind. Nachdem die Konfiguration gelöscht worden ist, können Sie mit einer komplett neuen IPSec-Konfiguration beginnen.</p> <p>Das Löschen der Konfiguration ist nur möglich mit IPSec aktivieren = <i>nicht aktiviert</i>.</p>
IPSec-Debug-Level	<p>Wählen Sie die Priorität der intern aufzuzeichnenden Systemprotokoll-Nachrichten des IPSec Subsystems.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Notfall</i> (höchste Priorität) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i> • <i>Benachrichtigung</i> • <i>Information</i> • <i>Debug</i> (Standardwert, niedrigste Priorität) <p>Nur Systemprotokoll-Nachrichten mit gleicher oder höherer Priorität als angegeben werden intern aufgezeichnet, d. h. dass beim Syslog-Level debug sämtliche erzeugten Meldungen aufgezeichnet werden.</p>

Im Menü **Erweiterte Einstellungen** können Sie bestimmte Funktionen und Merkmale an die besonderen Erfordernisse Ihrer Umgebung anpassen, d. h. größtenteils werden Interoperabilitäts-Flags gesetzt. Die Standardwerte sind global gültig und ermöglichen es, dass Ihr System einwandfrei mit anderen **bintec**-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
Initial Contact Message senden	Wählen Sie aus, ob bei IKE (Phase 1) IKE-Initial-Contact-Meldungen gesandt werden sollen, wenn keine SAs mit einem Peer bestehen.

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
SAs mit dem Status der ISP-Schnittstelle synchronisieren	<p>Wählen Sie aus, ob alle SAs gelöscht werden sollen, deren Datenverkehr über eine Schnittstelle geroutet wurde, an der sich der Status von <i>aktiv</i> zu <i>inaktiv</i>, <i>ruhend</i> oder <i>blockiert</i> geändert hat.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Zero Cookies verwenden	<p>Wählen Sie aus, ob zeroed (auf Null gesetzte) ISAKMP Cookies gesendet werden sollen.</p> <p>Diese sind dem SPI (Security Parameter Index) in IKE-Proposals äquivalent; da sie redundant sind, werden sie normalerweise auf den Wert der laufenden Aushandlung gesetzt. Alternativ kann Ihr Gerät Nullen für alle Werte des Cookies nutzen. Wählen Sie in diesem Fall <i>Aktiviert</i>.</p>
Größe der Zero Cookies	<p>Nur für Zero Cookies verwenden = aktiviert.</p> <p>Geben Sie die Länge der in IKE-Proposals benutzten zeroed SPI in Bytes ein.</p> <p>Der Standardwert ist 32.</p>
Dynamische RADIUS-Authentifizierung	<p>Wählen Sie aus, ob die RADIUS-Authentifizierung über IPsec aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Erweiterte Einstellungen PKI-Verarbeitungsoptionen

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

Feld	Beschreibung
	Standardmäßig ist die Funktion nicht aktiv.
Zertifikatsanforderungs-Payloads senden	<p>Wählen Sie aus, ob während der IKE (Phase 1) Zertifikatsanforderungen gesendet werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Zertifikatsketten senden	<p>Wählen Sie aus, ob während IKE (Phase 1) komplette Zertifikatsketten gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Deaktivieren Sie diese Funktion, falls Sie nicht die Zertifikate aller Stufen (von Ihrem bis zu dem der CA) an den Peer senden möchten.</p>
CRLs senden	<p>Wählen Sie aus, ob während IKE (Phase 1) CRLs gesandt werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Key Hash Payloads senden	<p>Wählen Sie aus, ob während IKE (Phase 1) Schlüssel-Hash-Nutzdaten gesandt werden sollen.</p> <p>Als Standard wird der Hash des Public Key (öffentlichen Schlüssels) der entfernten Seite zusammen mit den anderen Authentifizierungsdaten gesandt. Gilt nur für RSA-Verschlüsselung; aktivieren Sie diese Funktion mit <i>Aktiviert</i>, um dieses Verhalten zu unterdrücken.</p>

11.2 L2TP

Das Layer-2-Tunnelprotokoll (L2TP) ermöglicht das Tunneling von PPP-Verbindungen über eine UDP-Verbindung.

Ihr **bintec**-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.

11.2.1 Tunnelprofile

Im Menü **VPN -> L2TP -> Tunnelprofile** wird eine Liste aller konfigurierter Tunnelprofile angezeigt.

11.2.1.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 device. The left sidebar contains a navigation menu with options like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'IPSec', 'L2TP', 'PPTP', 'GRE', 'Zertifikate', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'VPN' menu is expanded, and 'L2TP' is selected. The main content area shows the 'Tunnelprofile' configuration page with tabs for 'Tunnelprofile', 'Benutzer', and 'Optionen'. The 'Tunnelprofile' tab is active, displaying a form for creating a new profile. The form is divided into 'Basisparameter' and 'Erweiterte Einstellungen' sections.

Basisparameter	
Beschreibung	L2TP1
Lokaler Hostname	
Entfernter Hostname	
Passwort	••••••••
Parameter des LAC-Modus	
Entfernte IP-Adresse	
UDP-Quellport	<input type="checkbox"/> Fest eingestellt
UDP-Zielport	1701
Erweiterte Einstellungen	
Lokale IP-Adresse	
Hello-Intervall	30 Sekunden
Minimale Zeit zwischen Versuchen	1 Sekunden
Maximale Zeit zwischen Versuchen	16 Sekunden
Maximale Anzahl Wiederholungen	5
Sequenznummern der Datenpakete	<input type="checkbox"/> Aktiviert

At the bottom of the form, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 136: VPN -> L2TP -> Tunnelprofile -> Neu

Das Menü **VPN -> L2TP -> Tunnelprofile -> Neu** besteht aus folgenden Feldern:

Felder im Menü Tunnelprofile 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"> • LAC: 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 SCCRP (Start Control Connection Reply). • LNS: 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"> • LAC: Definiert den Wert für Lokaler Hostname des LNS (enthalten in den vom LNS empfangene SCCRQs und vom LAC empfangene SCCRP). Der im LAC konfigurierte Lokale Hostname muss zu dem Entfernten Hostnamen passen, der für das vorgesehene Profil im LNS konfiguriert wurde und umgekehrt. • LNS: Definiert den Lokalen 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 einem passenden 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 Lokalen 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 be-</p>

Feld	Beschreibung
	rücksichtigt.

Felder im Menü Tunnelprofile 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 deaktiviert, was bedeutet, dass den Verbindungen, die dieses Profil nutzen, Ports dynamisch zugeordnet werden.</p> <p>Wenn Sie einen fixen Port eingeben möchten, aktivieren Sie die Option Fest. 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 ... 65535.</p> <p>Standardwert ist 1701 (RFC 2661).</p>

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Lokale IP-Adresse	Geben Sie die IP-Adresse ein, die als Quelladresse für alle L2TP-Verbindungen genutzt werden soll, die auf diesem Profil aufbauen.

Feld	Beschreibung
	<p>Falls dieses Feld frei gelassen wird, nutzt Ihr Gerät die IP-Adresse der Schnittstelle, über das der L2TP-Tunnel 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 1 bis 255, der Standardwert ist 1.</p>
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>

11.2.2 Benutzer

Im Menü **VPN** -> **L2TP** -> **Benutzer** wird eine Liste aller konfigurierter L2TP-Partner angezeigt.

11.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere L2TP-Partner einzurichten.

The screenshot shows the configuration interface for a new L2TP user on a bintec R1200 device. The interface is in German and includes a navigation menu on the left and a main configuration area on the right.

Navigation Menu (Left):

- Konfiguration speichern
- Systemverwaltung
- Physikalische Schnittstellen
- LAN
- Wireless LAN
- Routing
- WAN
- VPN
 - IPSec
 - L2TP**
 - PPTP
 - GRE
 - Zertifikate
- Firewall
- VoIP
- Lokale Dienste
- Wartung
- Externe Berichterstellung
- Monitoring

Main Configuration Area (Right):

Language: Deutsch | Online-Hilfe | Ausloggen | **funkwerk** enterprise communications

Buttons: **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	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

Entfernte IP-Adresse	Netzmaske	Metrik
<input type="text"/>	<input type="text"/>	1

Hinzufügen

Erweiterte Einstellungen

Blockieren nach Verbindungsfehler für	300 Sekunden
Authentifizierung	PAP/CHAP/MS-CHAP
Verschlüsselung	<input type="radio"/> Keine <input checked="" type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel
LCP-Ereichbarkeitsprüfung	<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

Buttons: **OK** | **Abbrechen**

Abb. 137: VPN -> L2TP -> Benutzer -> Neu

Das Menü **VPN** -> **L2TP** -> **Benutzer** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü Benutzer 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. Die Länge des Eintrags ist auf maximal 25 Zeichen beschränkt.</p>
Verbindungstyp	<p>Wählen Sie aus, ob der L2TP-Partner die Rolle des L2TP-Netzwerksservers (LNS) oder die Funktionen eines L2TP Access Concentrator Clients (LAC Client) übernehmen soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>LNS</i> (Standardwert): Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er L2TP-Tunnels akzeptiert und den verkapselten PPP-Datenstrom wieder herstellt. • <i>LAC</i> : Bei Auswahl dieser Option wird der L2TP-Partner so konfiguriert, dass er einen PPP-Datenstrom in L2TP verkapselt und einen L2TP-Tunnel zu einem entfernten LNS einrichtet.
Tunnelprofil	<p>Nur für Verbindungstyp = <i>LAC</i></p> <p>Wählen Sie ein im Menü Tunnelprofile 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, wieviele Sekunden zwischen Senden des letzten Nutz-Datenpakets und Abbau der Verbindung vergehen sollen.</p>

Feld	Beschreibung
	Zur Verfügung stehen Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Shorthold. Standardwert ist 300.

Felder im Menü Benutzer 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.
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>
IP-Zuordnungspool (IPCP)	<p>Nur für IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>Wählen Sie einen im Menü WAN -> Internet + Einwählen -> IP</p>

Feld	Beschreibung
	Pools konfigurierten IP Pool aus.
Lokale IP-Adresse	Nur für IP-Adressmodus = <i>Statisch</i> . Geben Sie die WAN IP-Adresse Ihres Geräts ein.
Routeneinträge	Nur für IP-Adressmodus = <i>Statisch</i> . Geben Sie Entfernte IP-Adresse und Netzmaske des LANs 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	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Standardwert ist <i>300</i> .
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen L2TP-Partner aus. Mögliche Werte: <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 <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <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.
Verschlüsselung	Wählen Sie ggf. die Art der Verschlüsselung, die für den Datenverkehr mit dem L2TP-Partner angewendet werden soll. Dies ist

Feld	Beschreibung
	<p>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> <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.
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 nicht aktiv.</p>
TCP-ACK-Pakete priorisieren	<p>Wählen Sie aus, ob der TCP-Download bei intensivem TCP-Upload optimiert werden soll. Diese Funktion kann speziell für asymmetrische Bandbreiten (ADSL) angewendet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

Felder im Menü Erweiterte Einstellungen IP-Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF Protokoll Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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, Sekundärer DNS-Server, Primärer WINS und Sekundärer WINS 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>

11.2.3 Optionen

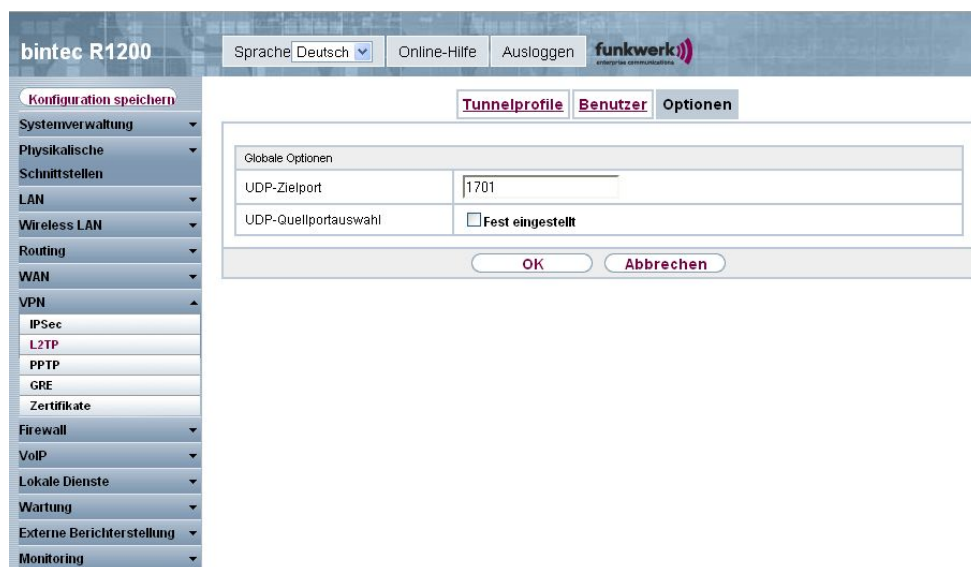


Abb. 138: VPN -> L2TP -> Optionen

Das Menü **VPN** -> **L2TP** -> **Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen 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>

11.3 PPTP

Zur Absicherung des Datenverkehrs über eine vorhandene IP-Verbindung kann mittels Point-to-Point-Tunneling-Protokoll (=PPTP) ein verschlüsselter PPTP-Tunnel aufgebaut werden.

Zunächst wird an beiden Standorten eine Verbindung zu einem ISP (=Internet Service Provider) aufgebaut. Wenn diese Verbindungen stehen, wird über das Internet ein Tunnel zum PPTP Partner, hier dann mit PPTP, aufgebaut.

Für diesen Vorgang baut das PPTP-Subsystem eine Kontrollverbindung zwischen den Tunnelendpunkten auf. Diese übermittelt Steuerungsdaten, welche die Verbindung zwischen den zwei PPTP-Tunnelendpunkten aufbauen, aufrechterhalten und beenden. Sobald diese Kontrollverbindung aufgebaut ist, überträgt das PPTP die in GRE-Pakete (GRE = Generic Routing Encapsulation) eingepackten Nutzdaten.

11.3.1 PPTP Tunnel

Im Menü **PPTP Tunnel** wird eine Liste aller PPTP-Tunnels angezeigt.

11.3.1.1 Neu

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

The screenshot shows the configuration page for a PPTP Tunnel. The left sidebar contains a navigation menu with the following items: Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN (expanded), IPsec, L2TP, PPTP (selected), GRE, Zertifikate, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The main content area is titled 'PPTP-Tunnel Optionen' and contains two sections: 'PPTP Partner Parameter' and 'Erweiterte Einstellungen'.

PPTP Partner Parameter

Beschreibung	<input type="text"/>
PPTP-Mode	<input checked="" type="radio"/> PNS <input type="radio"/> Windows-Client-Modus
Benutzername	<input type="text"/>
Passwort	••••••••
Immer aktiv	<input type="checkbox"/> Aktiviert
Timeout bei Inaktivität	300 Sekunden
Remote-PPTP-IP-Adresse	<input type="text"/>

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

Entfernte IP-Adresse	Netzmaske	Metrik
<input type="text"/>	<input type="text"/>	1

Erweiterte Einstellungen

Blockieren nach Verbindungsfehler für	300 Sekunden
Authentifizierung	MS-CHAPv2
Verschlüsselung	<input type="radio"/> Keine <input checked="" type="radio"/> Aktiviert <input type="radio"/> Windows-kompatibel
LCP-Ereichbarkeitsprüfung	<input checked="" 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
PPTP-Callback	<input type="checkbox"/> Aktiviert

Buttons: OK, Abbrechen

Abb. 139: VPN -> PPTP -> PPTP Tunnel -> Neu

Das Menü VPN -> PPTP -> PPTP Tunnel -> Neu besteht aus folgenden Feldern:

Felder im Menü PPTP Tunnel PPTP Partner Parameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Namen ein, um den Tunnel eindeutig zu be-

Feld	Beschreibung
	nennen. In diesem Feld darf das erste Zeichen keine Zahl sein. Sonderzeichen und Umlaute dürfen ebenfalls nicht verwendet werden.
PPTP-Modus	Geben Sie die Rollenverteilung der PPTP-Schnittstelle an. Mögliche Werte: <ul style="list-style-type: none"> • <i>PNS</i> (Standardwert): Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Servers zu. • <i>Windows Client Mode</i>: Hiermit weisen Sie der PPTP-Schnittstelle die Rolle des PPTP-Clients zu.
Benutzername	Geben Sie den Benutzernamen ein.
Passwort	Geben Sie das Passwort ein.
Immer aktiv	Wählen Sie aus, ob die Schnittstelle immer aktiv sein soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Timeout bei Inaktivität	Nur wenn Immer aktiv deaktiviert ist. Geben Sie das Inaktivitätsintervall in Sekunden ein. Damit legen Sie fest, wieviele Sekunden zwischen Senden des letzten Nutzdatenpakets und Abbau der Verbindung vergehen sollen. Mögliche Werte von 0 bis 3600 (Sekunden). 0 deaktiviert den Timeout. Standardwert ist 300 . Bsp. 10 für FTP-Übertragungen, 20 für LAN-zu-LAN-Übertragungen, 90 für Internetverbindungen.
Entfernte PPTP-IP-Adresse	Geben Sie die IP-Adresse des PPTP-Partners ein.

Felder im Menü PPTP Tunnels IP-Modus und Routen

Feld	Beschreibung
IP-Adressmodus	Wählen Sie aus, ob Ihrem Gerät eine statische IP-Adresse zugewiesen werden soll oder ob es diese dynamisch erhalten soll.

Feld	Beschreibung
	<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>: Ihr Gerät vergibt der Gegenstelle dynamisch eine IP-Adresse.
Standardroute	<p>Nur bei IP-Adressmodus = <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 bei IP-Adressmodus = <i>Statisch</i></p> <p>Wenn eine ISDN-Verbindung konfiguriert wird, wählen Sie aus, ob Network Address Translation (NAT) aktiviert werden soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Lokale IP-Adresse	<p>Nur für IP-Adressmodus = <i>Statisch</i></p> <p>Weisen Sie der ISDN-Schnittstelle die 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 Routing-Einträge für diesen Verbindungspartner.</p> <ul style="list-style-type: none"> • <i>Entfernte IP-Adresse</i>: IP-Adresse des Ziel-Hosts oder -LANs. • <i>Netzmaske</i>: Netzmaske zu Entfernte IP-Adresse. • <i>Metrik</i>: Je niedriger der Wert, desto höhere Priorität besitzt die Route (Wertebereich 0...15). Standardwert ist 1.
IP-Zuordnungspool (IPCP)	<p>Nur bei IP-Adressmodus = <i>IP-Adresse bereitstellen</i></p> <p>Wählen Sie einen im Menü WAN -> Internet + Einwählen -> IP Pools konfigurierten IP-Pool aus. Falls hier noch kein IP-Pool</p>

Feld	Beschreibung
	konfiguriert wurde, erscheint in diesem Feld die Meldung <i>Noch nicht definiert</i> .

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Blockieren nach Verbindungsfehler für	Geben Sie ein, für wie viele Sekunden nach fehlgeschlagenem Verbindungsaufbau kein erneuter Versuch durch Ihr Gerät unternommen werden soll. Standardwert ist <i>300</i> .
Authentifizierung	Wählen Sie das Authentifizierungsprotokoll für diesen PPTP-Partner aus. Mögliche Werte: <ul style="list-style-type: none"> • <i>PAP</i>: Nur <i>PAP</i> (PPP Password Authentication Protocol) ausführen, Passwort wird unverschlüsselt übertragen. • <i>CHAP</i>: Nur <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol nach RFC 1994) ausführen, Passwort wird verschlüsselt übertragen. • <i>PAP/CHAP</i>: Vorrangig CHAP, sonst PAP ausführen. • <i>MS-CHAPv1</i>: Nur MS-CHAP Version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol) ausführen. • <i>PAP/CHAP/MS-CHAP</i> : Vorrangig CHAP ausführen, bei Ablehnung anschließend das vom PPTP-Partner geforderte Authentifizierungsprotokoll ausführen. (MSCHAP Version 1 oder 2 möglich.) • <i>MS-CHAPv2</i>(Standardwert): Nur MS-CHAP Version 2 ausführen.
Verschlüsselung	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. Mögliche Werte: <ul style="list-style-type: none"> • <i>Keine</i> : Es wird keine MPP-Verschlüsselung angewendet.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Aktiviert</i>(Standardwert): Die MPP-Verschlüsselung V2 mit 128 bit wird nach RFC 3078 angewendet. • <i>Windows-kompatibel</i>: Die MPP-Verschlüsselung V2 mit 128 bit wird kompatibel zu Microsoft und Cisco angewendet.
LCP-Erreichbarkeitsprüfung	<p>Wählen Sie aus, ob die Erreichbarkeit der Gegenstelle durch Senden von LCP Echo Requests bzw. Replies überprüft werden soll. Dies ist empfehlenswert für Fest-, PPTP- und L2TP-Verbindungen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Erweiterte Einstellungen IP Optionen

Feld	Beschreibung
OSPF-Modus	<p>Wählen Sie aus, ob und wie über die Schnittstellerouten propagiert und/oder OSPF Protokoll Pakete gesendet werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Passiv</i> (Standardwert): OSPF ist nicht für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden keine Routen propagiert oder OSPF-Protokoll-Pakete gesendet. Über diese Schnittstelle erreichbare Netze werden jedoch bei der Berechnung der Routing Informationen berücksichtigt und über aktive Schnittstellen propagiert. • <i>Aktiv</i>: OSPF ist für diese Schnittstelle aktiviert, d. h. über diese Schnittstelle werden Routen propagiert und/oder OSPF-Protokoll-Pakete gesendet. • <i>Inaktiv</i>: OSPF ist für diese Schnittstelle deaktiviert.
Proxy-ARP-Modus	<p>Wählen Sie aus, ob Ihr Gerät ARP-Requests aus dem eigenen LAN stellvertretend für den spezifischen PPTP-Partner beantworten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Inaktiv</i> (Standardwert): Deaktiviert Proxy-ARP für diesen PPTP-Partner. • <i>Aktiv oder Ruhend</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-

Feld	Beschreibung
	<p>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.</p> <ul style="list-style-type: none"> • <i>Nur aktiv</i>: Ihr Gerät beantwortet einen ARP-Request nur, wenn der Status der Verbindung zum PPTP-Partner <i>aktiv</i> (aktiv) ist, wenn also bereits eine Verbindung zum PPTP-Partner besteht.
DNS-Aushandlung	<p>Wählen Sie aus, ob Ihr Gerät IP-Adressen für Primärer DNS-Server, Sekundärer DNS-Server vom PPTP-Partner erhalten soll oder diese zum PPTP-Partner schicken soll.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>

Felder im Menü Erweiterte Einstellungen PPTP-Callback

Feld	Beschreibung
Callback	<p>Ermöglicht den Aufbau eines PPTP-Tunnels über das Internet mit einem PPTP-Partner, selbst wenn dieser momentan nicht online ist. In der Regel wird mittels ISDN-Ruf der PPTP-Partner aufgefordert, online zu gehen und eine PPTP-Verbindung aufzubauen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Beachten Sie, dass Sie die entsprechende Option auf den Gateways beider Partner aktivieren müssen. Für diese Funktion wird in der Regel ein ISDN-Anschluss benötigt. Ohne ISDN ist Callback nur in Spezialanwendungen zu aktivieren.</p>
Eingehende ISDN-Nummer	<p>Nur wenn Callback aktiviert ist.</p> <p>Geben Sie die ISDN-Nummer an, von der aus das entfernte Gerät das lokale Gerät ruft (Calling Party Number).</p>
Ausgehende ISDN-Nummer	<p>Nur wenn Callback aktiviert ist.</p> <p>Geben Sie die ISDN-Nummer an, unter der das lokale Gerät das entfernte Gerät ruft (Called Party Number).</p>

Felder im Menü Erweiterte Einstellungen Auswahl des Wählports (nur wenn Callback = aktiviert)

Feld	Beschreibung
Ausgewählte Ports	<p>Geben Sie die ISDN-Ports an, über die der Callback ausgeführt werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle Ports</i>: Der Callback wird über einen der verfügbaren ISDN-Ports ausgeführt. • <i>Port angeben</i>: In Spezifische Ports können Sie die gewünschten ISDN-Ports auswählen.
Spezifische Ports	Nur für Ausgewählte Ports = <i>Port angeben</i> können Sie mit Hinzufügen weitere Ports auswählen.

11.3.2 Optionen

In diesem Menü können Sie allgemeine Einstellungen des globalen PPTP Profils vornehmen.

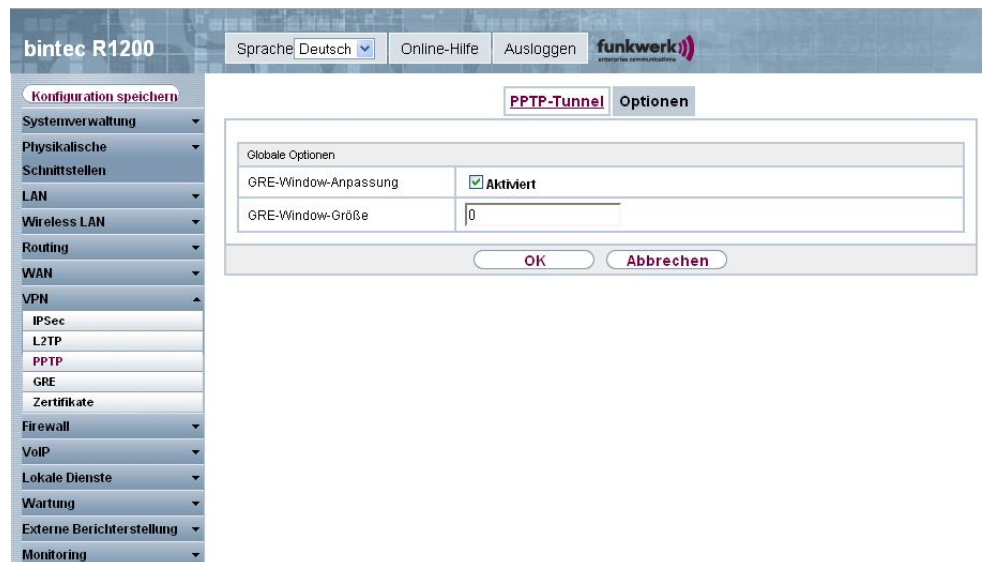


Abb. 140: VPN -> PPTP -> Optionen

Das Menü VPN -> PPTP -> Optionen besteht aus folgenden Feldern:

Felder im Menü Optionen Globale Optionen

Feld	Beschreibung
GRE-Win- dow-Anpassung	<p>Wählen Sie, ob Sie die GRE Window Adaption aktivieren wollen.</p> <p>Diese Anpassung ist erst notwendig, wenn Sie auf der Windows XP Seite das Service Pack 1 von Microsoft installiert haben. Da Microsoft mit SP 1 den Bestätigungsalgorithmus innerhalb des GRE-Protokolls geändert hat, muss auf der funkwerk-Seite die automatische Window-Anpassung für GRE abgeschaltet werden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
GRE-Window-Größe	<p>Geben Sie die maximale Anzahl an GRE Paketen ein, die ohne Bestätigung geschickt werden kann.</p> <p>Windows XP verwendet ein höheres initiales Empfangs-Window im GRE, weshalb hier die maximale Sende-Window-Größe auf der funkwerk-Seite über den Wert GRE Window-Größe angepasst werden sollte. Mögliche Werte sind 0 bis 256.</p>

11.4 GRE

Das Generic Routing Encapsulation (GRE) ist ein Netzwerkprotokoll, das dazu dient, andere Protokolle einzukapseln und so in Form von IP-Tunneln zu den spezifizierten Empfänger zu transportieren.

Die Spezifikation des GRE-Protokolls liegt in zwei Versionen vor:

- GRE V.1 zur Verwendung in PPTP-Verbindungen (RFC 2637, Konfiguration im Menü **PPTP**)
- GRE V.0 (RFC 2784) zur allgemeinen 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.

11.4.1 GRE-Tunnel

Im Menü **VPN** -> **GRE** -> **GRE-Tunnel** wird eine Liste aller konfigurierten GRE-Tunnel angezeigt.

11.4.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere GRE Tunnels einzurichten.

Abb. 141: VPN -> GRE -> GRE -Tunnel

Das Menü **VPN -> GRE -> GRE-Tunnel** besteht aus folgenden Feldern:

Felder im Menü GRE-Tunnel Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine Bezeichnung für den GRE-Tunnel ein.
Lokale GRE-IP-Adresse	Geben Sie die Quell-IP-Adresse der GRE-Pakete zum GRE-Partner ein. Wird keine IP-Adresse (dies entspricht der IP-Adresse 0.0.0.0) angegeben, wird die Quell-IP-Adresse der GRE-Pakete automatisch aus einer der Adressen der Schnittstellen ausgewählt, über die der GRE-Partner erreicht wird.
Entfernte GRE-IP-Adresse	Geben Sie die Ziel-IP-Adresse des Hosts bzw. Netzwerks, zu dem die Pakete durch den GRE-Tunnel geschickt werden sollen.
Standardroute	Wenn Sie die Default Route aktivieren, werden automatisch alle Daten auf eine Verbindung geleitet. Standardmäßig ist die Funktion nicht aktiv.


Feld	Beschreibung
Lokale IP-Adresse	Geben Sie die IP-Adresse ein, die als Quelladresse für diese GRE-Verbindung genutzt wird.
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 Remote-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.
MTU	<p>Geben Sie die maximale Paketgröße (Maximum Transfer Unit, MTU) in Bytes an, die für die GRE-Verbindung zwischen den Partnern verwendet werden darf.</p> <p>Mögliche Werte sind 1 bis 8192.</p> <p>Der Standardwert ist 1500.</p>
Schlüssel verwenden	<p>Aktivieren Sie die Eingabe einer Kennung für die GRE-Verbindung, welche die Unterscheidung mehrerer parallel laufender GRE-Verbindungen zwischen zwei GRE-Partnern ermöglicht (siehe RFC 1701).</p> <p>Mit <i>Aktiviert</i> wird die Kennung aktiviert.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Schlüsselwert	<p>Nur wenn Use Key aktiviert ist.</p> <p>Geben Sie die GRE-Verbindungskennung ein.</p> <p>Mögliche Werte sind 0 bis 2147483647.</p> <p>Der Standardwert ist 0.</p>

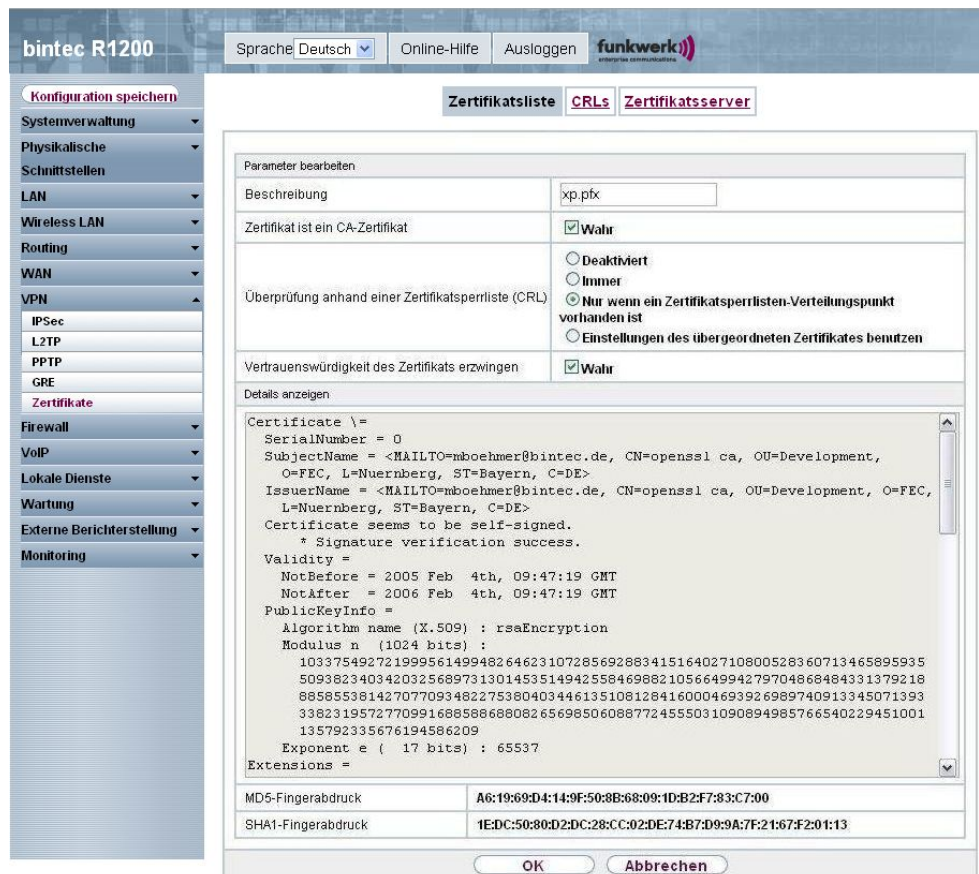
11.5 Zertifikate


11.5.1 Zertifikatsliste

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

11.5.1.1 Bearbeiten

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



bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen 

Konfiguration speichern

Systemverwaltung
 Physikalische Schnittstellen
 LAN
 Wireless LAN
 Routing
 WAN
 VPN
 IPsec
 L2TP
 PPTP
 GRE
Zertifikate
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

Zertifikatsliste CRLs Zertifikatsserver

Parameter bearbeiten

Beschreibung:

Zertifikat ist ein CA-Zertifikat: **Wahr**

Überprüfung anhand einer Zertifikatsperrliste (CRL):
 Deaktiviert
 Immer
 Nur wenn ein Zertifikatsperrlisten-Verteilungspunkt vorhanden ist
 Einstellungen des übergeordneten Zertifikates benutzen

Vertrauenswürdigkeit des Zertifikats erzwingen: **Wahr**

Details anzeigen

```

Certificate \ =
  SerialNumber = 0
  SubjectName = <MAILTO=mboehmer@bintec.de, CN=openssl ca, OU=Development, O=FEC, L=Nuernberg, ST=Bayern, C=DE>
  IssuerName = <MAILTO=mboehmer@bintec.de, CN=openssl ca, OU=Development, O=FEC, L=Nuernberg, ST=Bayern, C=DE>
  Certificate seems to be self-signed.
  * Signature verification success.
  Validity =
    NotBefore = 2005 Feb 4th, 09:47:19 GMT
    NotAfter = 2006 Feb 4th, 09:47:19 GMT
  PublicKeyInfo =
    Algorithm name (X.509) : rsaEncryption
    Modulus n (1024 bits) :
      1033754927219995614994826462310728569288341516402710800528360713465895935
      5093823403420325689731301453514942558469882105664994279704668484331379218
      8858553814270770934822753804034461351081284160004693926989740913345071393
      3382319572770991688588688082656985060887724555031090894985766540229451001
      135792335676194586209
    Exponent e ( 17 bits) : 65537
  Extensions =
  
```

MD5-Fingerabdruck: A6:19:69:D4:14:9F:50:8B:68:09:1D:B2:F7:83:C7:00
 SHA1-Fingerabdruck: 1E:DC:50:80:D2:DC:28:CC:02:DE:74:B7:D9:9A:7F:2:16:7F:2:0:1:13

OK Abbrechen

Abb. 142: VPN -> 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 **VPN -> Zertifikate -> Zertifikatsliste ->**  besteht aus folgenden Feldern:

Felder im Menü

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 (falls unter "Phase-1-Profile" nicht abweichend angegeben).</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 des 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.

11.5.1.2 Anforderung

Registration-Authority-Zertifikate im SCEP

Bei der Verwendung von SCEP 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-Zertifikate** = *-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 **Anforderung**, um weitere Zertifikaten zu beantragen oder zu importieren.

bintec R1200 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Systemverwaltung
 Physikalische Schnittstellen
 LAN
 Wireless LAN
 Routing
 WAN
 VPN
 IPsec
 L2TP
 PPTP
 GRE
Zertifikate
 Firewall
 VoIP
 Lokale Dienste
 Wartung
 Externe Berichterstellung
 Monitoring

Zertifikatsliste CRLs Zertifikatsserver

Zertifikatsanforderung

Zertifikatsanforderungsbeschreibung

Modus Manuell SCEP

Privaten Schlüssel generieren RSA 1024 Bits

Subjektname

Benutzerdefiniert Aktiviert

Allgemeiner Name

E-Mail

Organisationseinheit

Organisation

Standort

Staat/Provinz

Land

Erweiterte Einstellungen

Subjekt-Alternativnamen

#1 Keiner

#2 Keiner

#3 Keiner

Optionen

Autospeichermodus Aktiviert

OK Abbrechen

Abb. 143: VPN ->Zertifikate -> Zertifikatsliste -> Anforderung

Das Menü VPN -> Zertifikate -> Zertifikatsliste -> Anforderung besteht aus folgenden Feldern:

Felder im Menü Zertifikatsliste Zertifikatsanforderung

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

Feld	Beschreibung
	<p>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. http://scep.funkwerk.de:8080/scep/scep.dll</p> <p>Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator.</p>
CA-Zertifikat	<p>Nur für Modus = <i>SCEP</i></p> <p>Wählen Sie das CA-Zertifikat aus.</p> <ul style="list-style-type: none"> • <i>-Download-</i>: Geben Sie in CA-Name den Namen des CA-Zertifikats der Zertifizierungsstelle (CA) ein, von der Sie Ihr Zertifikat anfordern möchten, z. B. <i>cawindows</i>. Die entsprechenden Daten erhalten Sie von Ihrem CA-Administrator. <p>Falls keine CA-Zertifikate zur Verfügung stehen, wird Ihr Gerät zuerst das CA-Zertifikat der betroffenen CA herunterladen. Es fährt dann mit dem Registrierungsprozess fort, sofern kei-</p>

Feld	Beschreibung
	<p>ne 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 Zertifikatserver 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-Zertifikate 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 Zertifikatsliste Subjektnamen

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

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

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

Felder im Menü Erweiterte Einstellungen Subjekt-Alternativnamen

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

Felder im Menü Erweiterte Einstellungen Optionen

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

11.5.1.3 Importieren

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

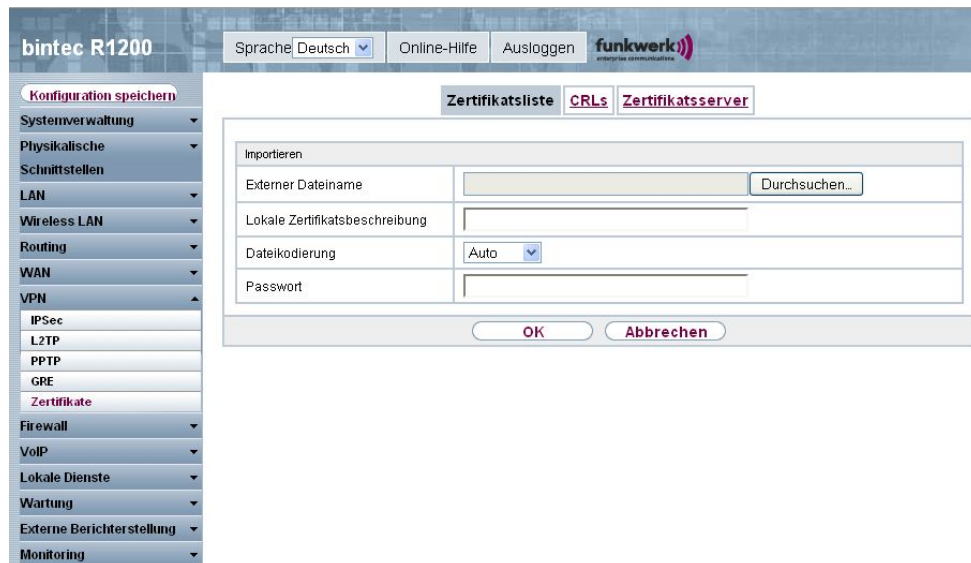


Abb. 144: VPN -> Zertifikate -> Zertifikatsliste -> Importieren

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

Felder im Menü Zertifikatsliste 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 Codierung, so dass Ihr Gerät das Zertifikat decodieren kann. Mögliche Werte: <ul style="list-style-type: none"> <i>Auto</i> (Standardwert): Aktiviert die automatische Kodiererkennung. Falls der Zertifikat-Download im Auto-Modus fehlschlägt, versuchen Sie es mit einer bestimmten Kodierung.

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

11.5.2 CRLs

Im Menü **VPN -> Zertifikate -> CRLs** wird eine Liste aller CRLs angezeigt.

11.5.2.1 Importieren

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

The screenshot shows the 'bintec R1200' web interface. At the top, there are options for 'Sprache' (Deutsch), 'Online-Hilfe', and 'Ausloggen', along with the 'funkwerk' logo. A navigation menu on the left lists various system management options, with 'VPN' expanded to show 'Zertifikate' and 'CRLs' selected. The main content area displays the 'Zertifikatsliste' tab, and a 'CRL-Import' dialog box is open. The dialog box contains the following fields:

- Externer Dateiname:** A text input field with a 'Durchsuchen...' button.
- Lokale Zertifikatsbeschreibung:** A text input field.
- Dateikodierung:** A dropdown menu currently set to 'Auto'.
- Passwort:** A text input field.

At the bottom of the dialog box, there are two buttons: 'OK' and 'Abbrechen'.

Abb. 145: VPN -> Zertifikate -> CRLs -> Importieren

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

Felder im Menü CRLs CRL-Import

Feld	Beschreibung
Externer Dateiname	Geben Sie den Dateipfad und -namen der CRL ein, welche im-

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

11.5.3 Zertifikatsserver

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

11.5.3.1 Neu

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

The screenshot shows the configuration interface for a bintec R1200 device. The left sidebar lists various configuration categories, with 'VPN' expanded to show 'Zertifikate' (Certificates) selected. The main content area displays the 'Zertifikatsserver' configuration page. At the top, there are tabs for 'Zertifikatsliste', 'CRLs', and 'Zertifikatsserver'. Below this is a 'Basisparameter' section with two input fields: 'Beschreibung' and 'LDAP-URL-Pfad'. The 'LDAP-URL-Pfad' field contains the text 'ldap://'. At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 146: VPN -> Zertifikate -> Zertifikatsserver -> Neu

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

Felder im Menü Zertifikatsserver Basisparameter

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

Kapitel 12 Firewall

Mit einer Stateful Inspection Firewall (SIF) verfügen **bintec** 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

bintecs Stateful Inspection Firewall fügt sich wegen ihrer einfachen Konfiguration gut in die bestehende Sicherheitsarchitektur der **bintec**-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).

12.1 Richtlinien

12.1.1 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 später 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. Wählen Sie die Option Administrative Zugriffsregeln anzeigen, um auch gegebenenfalls vorhandene Filterregeln für den administrativen Zugriff auf Ihre Gerät anzuzeigen (siehe **Systemverwaltung -> Administrativer Zugriff -> Zugriff**). Diese Regeln können hier auch bearbeitet werden.

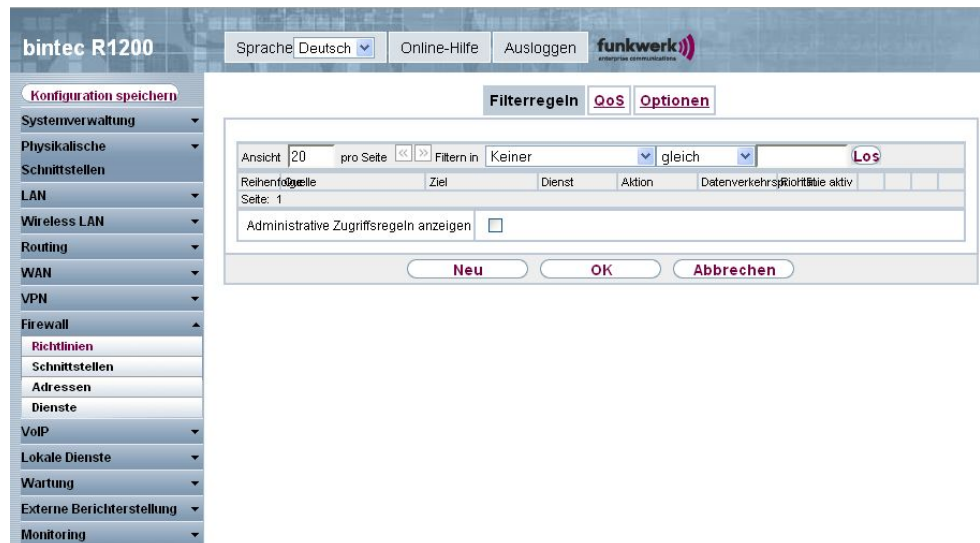




Abb. 147: Firewall -> Richtlinien -> Filterregeln

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.

12.1.1.1 Neu

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



Abb. 148: Firewall -> Richtlinien -> Filterregeln -> Neu

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

Felder im Menü Richtlinien 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>

Feld	Beschreibung
Ziel	<p>Wählen Sie einen der vorkonfigurierten Aliase für das Ziel des Pakets aus.</p> <p>In der die Liste stehen alle WAN-/LAN-Schnittstellen, Schnittstellengruppen (siehe Firewall -> Schnittstellen ->Gruppen), Adressen (siehe Firewall -> Adressen -> Adressliste) und Adressgruppen (siehe Firewall -> Adressen -> Gruppen) zur Auswahl.</p> <p>Der Wert <i>Beliebig</i> bedeutet, dass weder Ziel-Schnittstelle noch Ziel-Adresse überprüft werden.</p>
Dienst	<p>Wählen Sie einen der vorkonfigurierten Dienste aus, dem das zu filternde Paket zugeordnet sein muss.</p> <p>Werkseitig ist eine umfangreiche Reihe von Diensten vorkonfiguriert, unter anderem:</p> <ul style="list-style-type: none"> • <i>FTP</i> • <i>TELNET</i> • <i>SMTP</i> • <i>DNS</i> • <i>HTTP</i> • <i>NNTP</i> • <i>Internet</i> • <i>Netmeeting</i> <p>Weitere Dienste werden in Firewall -> Dienste -> Dienstliste angelegt.</p> <p>Außerdem stehen die in Firewall -> Dienste -> Gruppen konfigurierten Dienstgruppen 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 Feh-

Feld	Beschreibung
	Istmeldung 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 Datenverkehrspriorität 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 nicht ausdrücklich zugelassen wurde, von der Firewall geblockt wird!</p>
Datenverkehrspriorität	<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>

12.1.2 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 und Bandbreite für diese reserviert werden.

Im Menü **Firewall** -> **Richtlinien** -> **QoS** wird eine Liste aller QoS-Regeln angezeigt.

12.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere QoS-Regeln einzurichten.



Abb. 149: Firewall -> Richtlinien -> QoS -> Neu

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

Felder im Menü QoS QoS-Schnittstelle konfigurieren

Feld	Beschreibung
Schnittstelle	Wählen Sie die Schnittstelle aus, auf der das Bandbreitenmanagement erfolgen soll.
Traffic Shaping	Wählen Sie aus, ob Sie für die gewählte Schnittstelle das Bandbreitenmanagement aktivieren wollen. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Bandbreite angeben	Nur für Traffic Shaping = <i>Aktiviert</i> . Geben Sie die maximal zur Verfügung stehende Bandbreite in KBit/s für die gewählte Schnittstelle ein.
Filterregeln	Dieses Feld enthält eine Liste aller konfigurierten Firewall-

Feld	Beschreibung
	<p>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 KBit/s für den unter Dienste genannten Dienst ein. Standardmäßig ist 0 eingetragen. • Gebunden: 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.

12.1.3 Optionen

The screenshot shows the configuration page for Firewall -> Richtlinien -> Optionen. The page title is "bintec R1200" and the language is set to "Deutsch". The navigation menu on the left includes "Systemverwaltung", "Physikalische Schnittstellen", "LAN", "Wireless LAN", "Routing", "WAN", "VPN", "Firewall", "Richtlinien", "Schnittstellen", "Adressen", "Dienste", "VoIP", "Lokale Dienste", "Wartung", "Externe Berichterstellung", and "Monitoring". The main content area shows "Globale Firewall-Optionen" with a table of settings:

Globale Firewall-Optionen		
Firewall Status	<input checked="" type="checkbox"/>	Aktiviert
Protokollierte Aktionen	Alle	
Sitzungstimer		
UDP-Inaktivität	180	Sekunden
TCP-Inaktivität	3600	Sekunden
PPTP-Inaktivität	86400	Sekunden
Andere Inaktivität	30	Sekunden

Buttons for "OK" and "Abbrechen" are located at the bottom of the configuration area.

Abb. 150: Firewall -> Richtlinien -> Optionen

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

Felder im Menü Optionen 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". • <i>Annehmen</i>: Nur Accept-Ereignisse werden angezeigt. • <i>Keine</i>: Systemprotokoll-Nachrichten werden nicht erzeugt.

Felder im Menü Optionen 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>

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

12.2 Schnittstellen

12.2.1 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.

12.2.1.1 Neu

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



Abb. 151: Firewall -> Schnittstellen -> Gruppen -> Neu

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

Felder im Menü Gruppen 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 Mitglieder .

12.3 Adressen

12.3.1 Adressliste

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

12.3.1.1 Neu

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



Abb. 152: Firewall -> Adressen -> Adressliste -> Neu

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

Felder im Menü Adressliste 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> .
Adressbereich	Nur für Adresstyp = <i>Adressbereich</i> Geben Sie die Anfangs- und End-IP-Adresse des Bereiches ein.

12.3.2 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.

12.3.2.1 Neu

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

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Firewall', with 'Adressen' selected. The main content area is titled 'Gruppen' and contains a form with the following fields:

- Basisparameter** (Section header)
- Beschreibung**: A text input field.
- Auswahl**: A dropdown menu showing 'Adressen: Auswahl' and 'ANY', with a checkbox to its right.

At the bottom of the form are two buttons: 'OK' and 'Abbrechen'.

Abb. 153: Firewall -> Adressen -> Gruppen -> Neu

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

Felder im Menü Gruppen 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 .

12.4 Dienste

12.4.1 Diensteliste

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

12.4.1.1 Neu

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

The screenshot shows the web interface for a bintec R1200 device. At the top, there's a header with 'bintec R1200', a language dropdown set to 'Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. A left sidebar menu includes categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'Firewall' section is expanded, showing 'Richtlinien', 'Schnittstellen', 'Adressen', and 'Dienste' (which is highlighted). The main content area is titled 'Dienste' and has a sub-tab 'Gruppen'. Below this is a form for adding a new service. The form has a 'Basisparameter' section with two fields: 'Beschreibung' (a text input) and 'Protokoll' (a dropdown menu currently showing 'Beliebig'). At the bottom of the form are two buttons: 'OK' and 'Abbrechen'.

Abb. 154: Firewall -> Dienste -> Diensteliste -> Neu

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

Felder im Menü Diensteliste Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie einen Alias für den Dienst ein, den Sie konfigurieren wollen.
Protokoll	Wählen Sie das Protokoll aus, auf dem der Dienst basieren soll. Es stehen die wichtigsten Protokolle zur Auswahl.
Zielportbereich	Nur für Protokoll = <i>TCP</i> , <i>UDP/TCP</i> oder <i>UDP</i>

Feld	Beschreibung
	<p>Geben Sie im ersten Feld den Ziel-Port an, über den der Dienst laufen soll.</p> <p>Soll ein Port-Nummern-Bereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Port-Bereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>.</p>
Quellportbereich	<p>Nur für Protokoll = <i>TCP</i> , <i>UDP/TCP</i> oder <i>UDP</i></p> <p>Geben Sie im ersten Feld den ggf. zu überprüfenden Quell-Port an.</p> <p>Soll ein Portnummernbereich angegeben werden, geben Sie im zweiten Feld ggf. den letzten Port eines Portbereichs ein. Standardmäßig enthält das Feld keinen Eintrag. Wird ein Wert angezeigt, bedeutet das, dass die zuvor angegebene Portnummer verifiziert wird. Soll ein Portbereich überprüft werden, ist hier die Obergrenze einzutragen.</p> <p>Mögliche Werte sind <i>1</i> bis <i>65535</i>.</p>
Typ	<p>Nur für Protokoll = <i>ICMP</i></p> <p>Das Feld Typ gibt die Klasse der ICMP-Nachrichten an, das Feld Code spezifiziert die Art der Nachricht genauer.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Echo Replay</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>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Timestamp Reply</i> • <i>Information Request</i> • <i>Information Reply</i> • <i>Adress Mask Request</i> • <i>Adress Mask Reply</i>
Code	<p>Nur für Typ = <i>Destination Unreachable</i> stehen Ihnen Auswahlmöglichkeiten für den ICMP Code zur Verfügung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Beliebig</i> (Standardwert) • <i>Net Unreachable</i> • <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>

12.4.2 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.

12.4.2.1 Neu

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

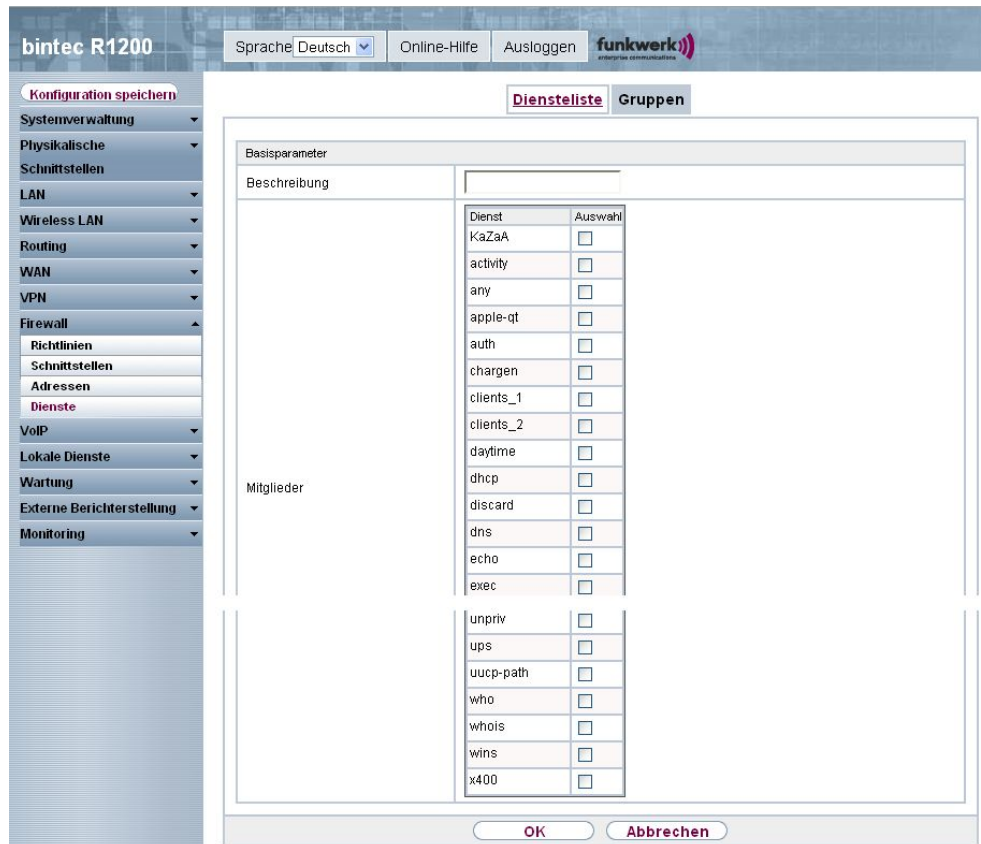


Abb. 155: Firewall -> Dienste -> Gruppen -> Neu

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

Felder im Menü Gruppen Basisparameter

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

Kapitel 13 VoIP

Voice over IP (VoIP) nutzt das IP-Protokoll für Sprach- und Bildübertragung.

Der wesentliche Unterschied zur herkömmlichen Telefonie besteht darin, dass die Sprachinformationen nicht über eine geschaltete Verbindung in einem Telefonnetz übertragen werden, sondern durch das Internet Protokoll in Datenpakete aufgeteilt, die auf nicht festgelegten Wegen in einem Netzwerk zum Ziel gelangen. Diese Technologie macht sich so für die Sprachübertragung die Infrastruktur eines bestehenden Netzwerks zu Nutze und teilt sich dieses mit anderen Kommunikationsdiensten.

13.1 Application Level Gateway

Um IP-Telefonen die Verbindung über SIP mit einem VoIP Provider zu ermöglichen, verfügt Ihr Gerät über ein Application Level Gateway (ALG), d.h. einen entsprechenden Proxy, der die notwendigen NAT- und Firewall-Freigaben vornimmt.




Hinweis

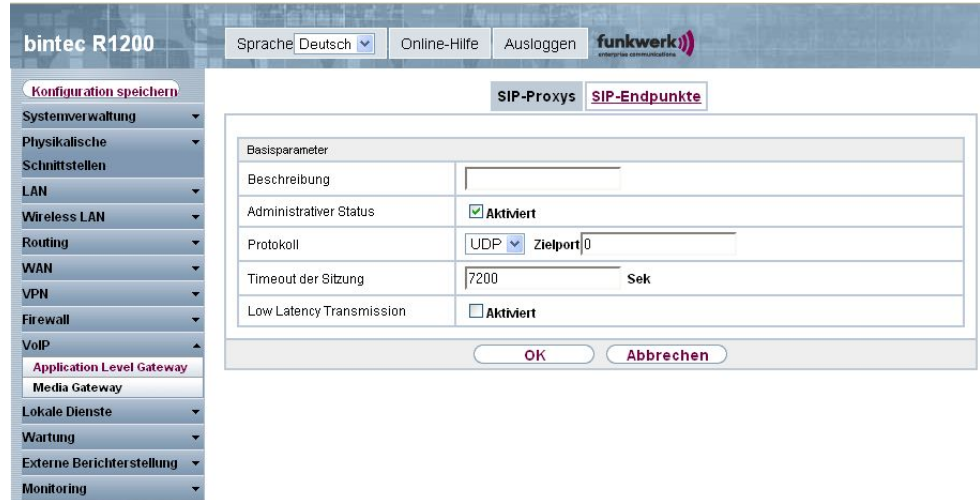
Das Application Level Gateway muss immer dann genutzt werden, wenn auf der Schnittstelle, welche die Verbindung zum Internet herstellt, NAT aktiviert ist.

13.1.1 SIP-Proxys

Sie sehen hier eine Liste der bereits konfigurierten Application Level Gateway Einträge. Diese Einträge aktivieren das ALG. Jeder Eintrag definiert einen bestimmten TCP oder UDP Zielpport, der vom ALG überwacht werden soll. Standardmäßig sind im Auslieferungszustand zwei Einträge für die SIP Ports TCP 5060 und UDP 5060 entsprechend der IANA Definition angelegt.

13.1.1.1 Bearbeiten/Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Application Level Gateway Einträge zu erstellen.



The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', and 'VoIP'. Under 'VoIP', 'Application Level Gateway' is selected. The main content area has two tabs: 'SIP-Proxy' (active) and 'SIP-Endpunkte'. The 'SIP-Proxy' configuration form includes the following fields:

- Basisparameter** (Section Header)
- Beschreibung**: Text input field.
- Administrativer Status**: **Aktiviert**
- Protokoll**: Dropdown menu set to 'UDP', followed by 'Zielport' and a text input field with '0'.
- Timeout der Sitzung**: Text input field with '7200' and 'Sek'.
- Low Latency Transmission**: **Aktiviert**

Buttons for 'OK' and 'Abbrechen' are located at the bottom of the form.

Abb. 156: VoIP -> Application Level Gateway -> SIP-Proxys -> Bearbeiten/Neu

Das Menü **VoIP -> Application Level Gateway -> SIP-Proxys -> Bearbeiten/Neu** besteht aus folgenden Feldern:

Felder im Menü SIP-Proxys Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Application Level Gateways ein.
Administrativer Status	Wählen Sie aus, ob der SIP Proxy aktiv sein soll. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Protokoll	Wählen Sie das Protokoll aus, welches verwendet werden soll. Mögliche Werte: <i>UDP</i> (Standardwert) oder <i>TCP</i> . Geben Sie als Zielport den Port ein, der vom Proxy überwacht werden soll. Pro Destination Port, zu dem sich VoIP Clients aus dem LAN verbinden können, müssen Sie einen Proxy anlegen.

Feld	Beschreibung
	Die Ports können Provider-spezifisch sein.
Timeout der Sitzung	<p>Geben Sie die Zeit in Sekunden ein, welche eine Session bestehen bleiben soll, wenn keine Datenpakete gesendet oder empfangen werden.</p> <p>Dieser Wert muss größer sein als die SIP Expire Time des angeschlossenen SIP Clients (SIP Telefone, Terminaladapter usw.)</p> <p>Standardwert ist <i>1800</i> .</p>
Low Latency Transmission	<p>Wählen Sie aus, ob ein Mechanismus zur Minimierung der Laufzeit, die VoIP-Datenpakete für den "Weg" zwischen zwei Gesprächspartnern benötigen, verwendet werden soll. Das garantiert eine gute Sprachqualität bei hoher Leitungsauslastung.</p> <p>Beachten Sie, dass Low Latency Transmission nicht eingeschaltet zu sein braucht, wenn das Media Gateway die VoIP-Verbindungen überwacht.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>

13.1.2 SIP-Endpunkte


Hier werden die Sessions angezeigt, welche aktuell vom ALG verwaltet werden.



Hinweis

Alle Clients, die länger als 24 Stunden nicht verwendet wurden, werden automatisch aus der Tabelle gelöscht.

13.1.2.1 Bearbeiten/Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um statische Einträge für SIP Server / Proxies innerhalb des LAN hinzuzufügen, welche über die NAPT-Barriere erreichbar sein sollen.

Nur wenn sich Terminals von außen an einen internen Server anmelden sollen, müssen

Sie hier für den SIP Server Werte eingeben.

Abb. 157: VoIP -> Application Level Gateway -> SIP-Endpunkte -> Bearbeiten/Neu
Das Menü VoIP ->Application Level Gateway -> SIP-Endpunkte -> Bearbeiten/Neu besteht aus folgenden Feldern:

Felder im Menü SIP-Endpunkte Basisparameter

Feld	Beschreibung
Endpunkttyp	Wählen Sie das SIP Terminal, das verwendet werden soll. Mögliche Werte: <i>Client</i> (Standardwert): interne Terminals (z. B. Telefone) werden verwendet. <i>Server</i> : es wird ein Server verwendet, damit sich Terminals von extern anmelden können.
Protokoll	Wählen Sie das Protokoll aus, welches für die Datenübertragung verwendet werden soll. Mögliche Werte: <i>UDP</i> (Standardwert) oder <i>TCP</i> . Wenn ein Protokoll automatisch erkannt wurde, sollte es nicht geändert werden.
Interne IP-Adresse	Geben Sie die interne IP-Adresse des Terminals an.
Entfernter Port	Nur für Endpunkttyp = <i>Client</i> . Geben Sie den Remote Port an.
Interner Port	Nur für Endpunkttyp = <i>Server</i> .

Feld	Beschreibung
	Geben Sie den internen Port an.
Externer Port	Externer Port, der dem internen Port zugeordnet werden sollte. Bei Clients wird der externe Port automatisch erkannt und sollte nicht geändert werden.

13.2 Media Gateway

13.2.1 Teilnehmer

Hier können Sie die Rufnummern der Endgeräte konfigurieren, die an das Media Gateway angebunden sind, d.h. die Rufnummern der SIP Endgeräte sowie die Rufnummern der angeschalteten ISDN oder analogen Endgeräte abhängig von den verfügbaren PSTN-Schnittstellen.

Im Menü **VoIP** -> **Media Gateway** -> **Teilnehmer** wird eine Liste aller vorhandenen Teilnehmer angezeigt.

13.2.1.1 Bearbeiten/Neu


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

Abb. 158: VoIP -> Media Gateway -> Teilnehmer -> Bearbeiten/Neu

Das Menü VoIP ->Media Gateway -> Teilnehmer -> Bearbeiten/Neu besteht aus folgenden Feldern:

Felder im Menü Teilnehmer Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Endgeräts ein.
Teilnehmer / Benutzername	Geben Sie die Rufnummer ein. Maximal können 40 Zeichen eingegeben werden.
Schnittstellentyp	Wählen Sie den Schnittstellentyp aus, welcher verwendet werden soll. Die Auswahl ist von den verfügbaren Schnittstellen abhängig.
Wähle ISDN-Schnittstelle	Nur für Schnittstellentyp = ISDN. Wählen Sie eine ISDN-Schnittstelle aus. Welche ISDN-Schnittstellen Sie auswählen können, hängt vom verwendeten Gerät ab.

Feld	Beschreibung
Wähle analoge Schnittstelle	<p>Nur für Schnittstellentyp = <i>Analogue</i>.</p> <p>Wählen Sie eine analoge Schnittstelle aus. Welche analoge Schnittstellen Sie auswählen können, hängt vom verwendeten Gerät ab.</p>
Registrierung	<p>Nur für Schnittstellentyp = <i>SIP</i>.</p> <p>Wählen Sie, ob der Registrierungsmechanismus per SIP REGISTER benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion nicht aktiv.</p>
Gültigkeit	<p>Nur wenn Registrierung aktiviert ist.</p> <p>Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird.</p> <p>Bei Clients wird der externe Port automatisch erkannt und sollte nicht geändert werden.</p> <p>Zur Verfügung stehen Werte von 0 bis 38400 .</p> <p>Der Standardwert ist 60 .</p>
SIP-Endpunkt-IP-Adresse	<p>Nur wenn Registrierung deaktiviert ist.</p> <p>Für Konfigurationen, bei denen keine Registrierung vorgesehen ist (z. B. Anbindung an einen Microsoft Exchange Communication Server), kann die Verbindung als statischer Host eingerichtet werden. Hierzu ist es nötig, die statische IP-Adresse des Endgeräts anzugeben.</p>
Authentifizierungs-ID	<p>Nur für Schnittstellentyp = <i>SIP</i></p> <p>Tragen Sie einen Namen ein, der zur Authentifizierung verwendet wird. Maximal können 20 Zeichen eingegeben werden.</p>

Feld	Beschreibung
	<p>Den hier vergebenen Namen müssen Sie auch auf dem SIP-Telefon eingeben.</p> <p>Wenn Sie keinen Namen eingeben, wird der Name im Feld Teilnehmer / Benutzername verwendet.</p>
Passwort	<p>Nur für Schnittstellentyp = SIP</p> <p>Geben Sie hier ein Passwort ein. Maximal können 20 Zeichen eingegeben werden.</p> <p>Das hier vergebene Passwort müssen Sie auch auf dem SIP-Telefon eingeben.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches für die Datenübertragung verwendet werden soll.</p> <p>Mögliche Werte: <i>UDP</i> (Standardwert), <i>TCP</i> oder <i>SIPS</i>.</p> <p>Wenn ein Protokoll automatisch erkannt wurde, sollte es nicht geändert werden.</p>

Felder im Menü Erweiterte Einstellungen Codec-Einstellungen

Feld	Beschreibung
Codec-Vorschlagssequenz	<p>Wählen Sie die Reihenfolge der Codecs, wie sie vom Media Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Der Codec, welcher im abgebildeten Menü an erster Stelle steht, wird verwendet, wenn möglich. • <i>Qualität</i> : Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • <i>Niedrigste</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • <i>Höchste</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchsten Bandbreite benötigt, wird verwendet, wenn möglich.

Feld	Beschreibung
Sortierreihenfolge	<p>Zeigt abhängig von der Einstellung im Feld Codec-Vorschlagssequenz die Codecs in der Reihenfolge, in welcher versucht wird, sie zu verwenden. Es wird immer der erste Codec in der Reihe verwendet, wenn möglich.</p> <p>Standardmäßig sind alle angezeigten Codecs aktiv. Sie können Codecs deaktivieren.</p>


Felder im Menü **Erweiterte Einstellungen Sprachqualitätseinstellungen**

Feld	Beschreibung
Echounterdrückung	<p>Wählen Sie aus, ob Echounterdrückung verwendet werden soll.</p> <p>Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Erzeugung von Hintergrundrauschen (Comfort Noise Generation, CNG)	<p>Wählen Sie aus, ob Erzeugung von Hintergrundrauschen (Comfort Noise Generation, CNG) verwendet werden soll.</p> <p>Bei digitaler Sprachübertragung sorgt Erzeugung von Hintergrundrauschen durch leichtes Hintergrundrauschen dafür, dass während Gesprächspausen bei den Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Packetgröße	<p>Geben Sie in Millisekunden ein, wie lange es dauern soll, um ein RTP Datenpaket zu übertragen.</p> <p>Zur Verfügung stehen Werte von <i>10</i> bis <i>210</i> .</p> <p>Der Standardwert ist <i>30</i> .</p>

13.2.2 SIP-Konten

Im Menü **VoIP** -> **Media Gateway** -> **SIP-Konten** wird eine Liste aller vorhandenen SIP-Konten angezeigt.

13.2.2.1 Bearbeiten/Neu

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

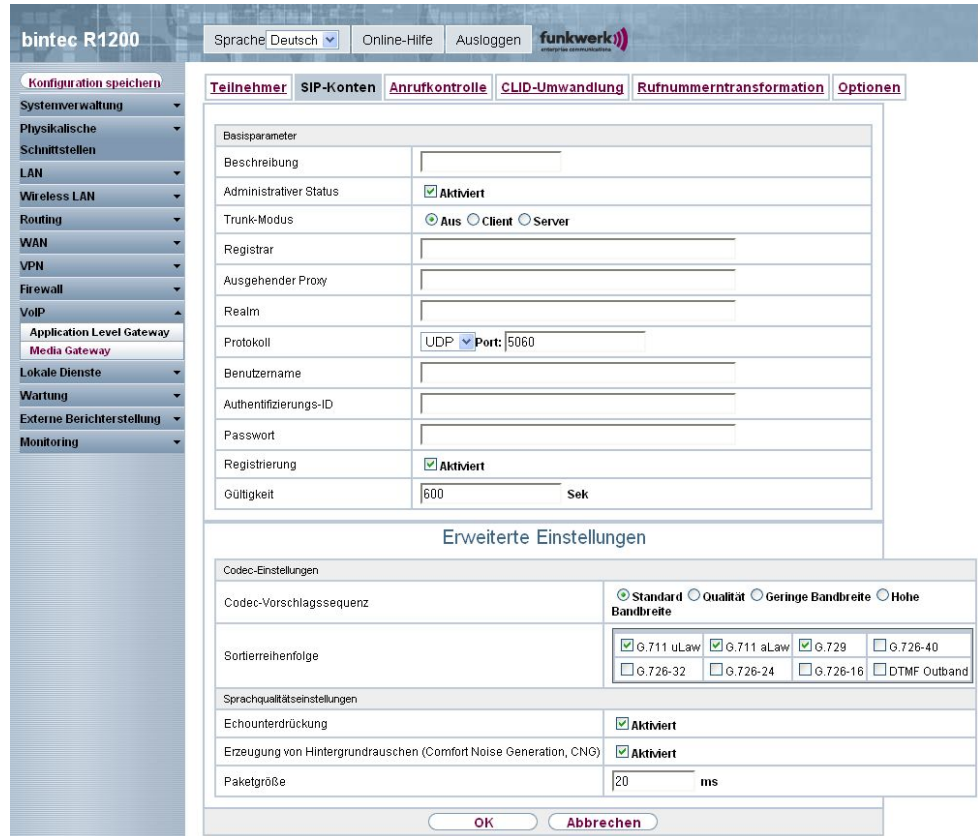


Abb. 159: VoIP -> Media Gateway -> SIP-Konten -> Bearbeiten/Neu

Das Menü **VoIP ->Media Gateway ->SIP-Konten-> Bearbeiten/Neu** besteht aus folgenden Feldern:

Felder im Menü SIP-Konten Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Accounts ein.
Administrativer Status	Wählen Sie aus, ob der Administrationsstatus des Accounts aktiv sein soll.

Feld	Beschreibung
	<p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Trunk-Modus	<p>Wählen Sie den Trunk Mode aus, der verwendet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</i> (Standardwert): Der Trunk Mode wird nicht verwendet. • <i>Client</i>: Das Media Gateway wird als SIP Client betrieben. • <i>Server</i>: Das Media Gateway wird als SIP Server betrieben.
Registrar	<p>Nur für Trunk-Modus = <i>Aus</i> oder Trunk-Modus = <i>Client</i>.</p> <p>Tragen Sie die IP-Adresse oder den Domännennamen (FQDN) des SIP Registrars bzw. des SIP Proxy Servers ein. Maximale Zeichenzahl ist 40.</p>
Ausgehender Proxy	<p>Nur für Trunk-Modus = <i>Server</i>.</p> <p>Geben Sie den Namen oder die IP-Adresse des SIP Outbound Proxy Servers ein.</p> <p>Maximal können 32 Zeichen eingegeben werden.</p> <p>Hier müssen Sie nur dann einen Namen eintragen, wenn bei allen SIP Sessions die Kommunikation nicht direkt sondern über einen weiteren Proxy erfolgen soll.</p> <p>Tragen Sie nur dann einen Namen oder eine IP-Adresse ein, wenn dies explizit vom Provider vorgegeben wird.</p>
Realm	<p>Tragen Sie einen weiteren Domännennamen oder eine weitere IP-Adresse des SIP Proxy Servers ein.</p> <p>Wenn Sie keinen Domännennamen eingeben, wird der Name im Feld Registrar verwendet.</p> <p>Tragen Sie nur dann einen Namen ein, wenn dieser explizit vom Provider vorgegeben wird.</p>
Protokoll	<p>Wählen Sie das Protokoll aus, welches zum Datentransport verwendet werden soll.</p> <p>Mögliche Werte: <i>udp</i> (Standardwert) oder <i>tcp</i>.</p>

Feld	Beschreibung
	<p>Geben Sie den Port ein, über den die Daten transportiert werden sollen.</p> <p>Die Ports können Provider-spezifisch sein.</p> <p>Standardwert ist <i>5060</i> .</p>
Benutzername	<p>Tragen Sie den Benutzernamen für die Authentifizierung ein, wenn Ihnen Ihr VoIP Provider einen solchen zugewiesen hat.</p>
Authentifizierungs-ID	<p>Tragen Sie einen Namen ein, der zur Authentifizierung verwendet wird.</p> <p>Wenn Sie keinen Namen eingeben, wird der Name im Feld Benutzername verwendet.</p> <p>Tragen Sie nur dann einen Namen ein, wenn dieser explizit vom Provider vorgegeben wird.</p>
Passwort	<p>Der VoIP Provider weist Ihnen ein. Passwort für die Authentifizierung zu. Diesen Wert müssen Sie hier eingeben.</p> <p>Maximal können 40 Zeichen eingegeben werden.</p>
Registrierung	<p>Wählen Sie, ob der Registrierungsmechanismus per SIP REGISTER benutzt werden soll. Dazu meldet jeder SIP Client (Benutzer) seine aktuelle Position an einen REGISTRAR Server mittels einer REGISTER Meldung. Diese Information über den Benutzer und seine aktuelle Adresse wird vom REGISTRAR auf einem Server gespeichert, der von anderen Proxies benutzt wird, um den Benutzer zu finden.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Gültigkeit	<p>Nur wenn Registrierung aktiviert ist.</p> <p>Geben Sie die Zeit in Sekunden ein, nach der die aktuelle Registrierung ungültig wird und daher eine neue Registrierungsanfrage geschickt wird.</p> <p>Zur Verfügung stehen Werte von <i>0</i> bis <i>99999</i> .</p> <p>Der Standardwert ist <i>600</i> .</p>

Feld	Beschreibung
	Ein Server kann in einer Antwort auf eine REGISTER Anfrage eine andere Expire Time festlegen, welche die hier festgelegte überschreibt.

Felder im Menü SIP-Konten Trunk-Einstellungen

Feld	Beschreibung
SIP-Header-Feld(er) für Anruferadresse	<p>Nur für Trunk-Modus = <i>Client</i> oder Trunk-Modus = <i>Server</i>.</p> <p>Wählen Sie, wo und wie für ausgehende Rufe die DDI Absenderadresse übertragen wird. (Bei eingehenden Rufen wird automatisch die Rufnummer gesucht.)</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Deaktiviert</i> (Standardwert): Die DDI Absenderadresse wird nicht übertragen. • <i>Anzeige und Benutzername</i> : Die Absenderadresse wird im SIP Header im Feld "Display" und im Feld "User" übertragen. • <i>Nur Anzeige</i>: Die Absenderadresse wird im SIP Header im Feld "Display" übertragen. • <i>Nur Benutzer</i>: Die Absenderadresse wird im SIP Header im Feld "User" übertragen. • <i>P-Preferred</i>: Der SIP Header wird durch das sogenannte "p-preferred-identity" Feld erweitert, um dort die Absenderadresse zu übertragen. • <i>P-Asserted</i>: Der SIP Header wird durch das sogenannte "p-asserted-identity" Feld erweitert, um dort die Absenderadresse zu übertragen.
Rufnummer	<p>Nur für Trunk-Modus = <i>Server</i>.</p> <p>Sie können eine Nummer setzen, die bei ausgehenden Rufen als Prefix vorangestellt wird und bei eingehenden Rufen von der Absenderadresse abgeschnitten wird. Das entspricht der Rumpfnummer einer TK-Anlage.</p>

Felder im Menü Erweiterte Einstellungen Codec-Einstellungen

Feld	Beschreibung
Codec-Vor-	Wählen Sie die Reihenfolge der Codecs, wie sie vom Media

Feld	Beschreibung
schlagssequenz	<p>Gateway zur Benutzung vorgeschlagen werden. Kann der erste Codec nicht angewendet werden, wird versucht den zweiten zu benutzen usw.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Standard</i> (Standardwert): Der Codec, welcher im abgebildeten Menü an erster Stelle steht, wird verwendet, wenn möglich. • <i>Qualität</i> : Die Codecs werden nach Qualität sortiert. Der Codec mit der besten Qualität wird verwendet, wenn möglich. • <i>Geringe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die niedrigste Bandbreite benötigt, wird verwendet, wenn möglich. • <i>Hohe Bandbreite</i>: Die Codecs werden nach benötigter Bandbreite sortiert. Der Codec, welcher die höchsten Bandbreite benötigt, wird verwendet, wenn möglich.
Sortierreihenfolge	<p>Wählen sie die Codecs aus, die für die Verbindung vorgeschlagen werden sollen. Abhängig von der Einstellung im Feld Codec-Vorschlagssequenz werden die hier ausgewählten Codecs in einer bestimmten Reihenfolge vorgeschlagen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>G.711 uLaw</i>: ISDN Codec nach US Kennlinie • <i>G.711 aLaw</i>: ISDN Codec nach EU Kennlinie • <i>G.729</i>: Komprimiert von 31 auf 8 KBit/s; gute Sprachqualität • <i>G.726-40</i>: Komprimiert von 63 auf 40 KBit/s • <i>G.726-32</i>: Komprimiert von 55 auf 32 KBit/s • <i>G.726-24</i>: Komprimiert von 47 auf 24 KBit/s • <i>G.726-16</i>: Komprimiert von 39 auf 16 KBit/s • <i>DTMF outb.</i>: DTMF Outband. Zuerst wird versucht RFC 2833 zu verwenden. Wenn die Gegenstelle diesen Standard nicht "beherrscht", wird SIP Info verwendet. <p>Standardmäßig sind <i>G.711 uLaw</i>, <i>G.711 aLaw</i> und <i>G.729</i> aktiviert.</p>

Felder im Menü Erweiterte Einstellungen Sprachqualitätseinstellungen


Feld	Beschreibung
Echounterdrückung	<p>Wählen Sie aus, ob Echounterdrückung verwendet werden soll.</p> <p>Bei der Echounterdrückung handelt es sich um ein Verfahren, das bei Sprachkommunikation auf Voll-Duplex-Leitungen Echo-Rückkopplungen unterdrückt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Erzeugung von Hintergrundrauschen (Comfort Noise Generation, CNG)	<p>Wählen Sie aus, ob Erzeugung von Hintergrundrauschen (Comfort Noise Generation, CNG) verwendet werden soll.</p> <p>Bei digitaler Sprachübertragung sorgt Erzeugung von Hintergrundrauschen durch leichtes Hintergrundrauschen dafür, dass während Gesprächspausen bei den Gesprächspartner der Eindruck vermieden wird, die Verbindung sei unterbrochen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Packetgröße	<p>Geben Sie in Millisekunden ein, wie lange es dauern soll, um ein RTP Datenpaket zu übertragen.</p> <p>Zur Verfügung stehen Werte von <i>10</i> bis <i>210</i> .</p> <p>Der Standardwert ist <i>20</i> .</p>

13.2.3 Anrufkontrolle

Hier können Sie die Bedingungen für das Weiterleiten von Anrufen (Routing) festlegen.

Im Menü **VoIP** -> **Media Gateway** -> **Anrufkontrolle** wird eine Liste aller vorhandenen Einträge angezeigt.

13.2.3.1 Bearbeiten/Neu

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

The screenshot shows the configuration page for 'Anrufkontrolle' (Call Control) in the bintec R1200 web interface. The page is titled 'bintec R1200' and includes a language dropdown set to 'Deutsch', an 'Online-Hilfe' link, and an 'Ausloggen' button. The 'funkwerk' logo is visible in the top right corner.

The main navigation menu on the left includes: 'Konfiguration speichern', 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Application Level Gateway', 'Media Gateway', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'.

The 'Anrufkontrolle' configuration page has several tabs: 'Teilnehmer', 'SIP-Konten', 'Anrufkontrolle', 'CLID-Umwandlung', 'Rufnummerntransformation', and 'Optionen'. The 'Anrufkontrolle' tab is active.

The configuration form is divided into two sections: 'Basisparameter' and 'Routing-Regel'.

Basisparameter:

- Beschreibung: Text input field.
- Administrativer Status: **Aktivieren**
- Typ: Dropdown menu set to 'Extern'.
- Anrufende Leitung: Dropdown menu set to 'Beliebig'.
- Anrufende Adresse: Text input field.
- Angerufene Adresse: Text input field.

Routing-Regel:

- Priorität: Text input field set to '1'.
- Administrativer Status: **Aktivieren**
- Ausgehende Leitung: Dropdown menu.
- Transformation der gerufenen Adresse: Text input field.

At the bottom of the form, there are buttons for 'Übernehmen', 'OK', and 'Abbrechen'. A table below the form shows the current configuration for the routing rule:

Priorität	Leitung	Transformation der gerufenen Adresse	Status	Aktion
1	-			

Abb. 160: VoIP -> Media Gateway -> Anrufkontrolle-> Bearbeiten/Neu

Das Menü VoIP ->Media Gateway ->Anrufkontrolle-> Bearbeiten/Neu besteht aus folgenden Feldern:

Felder im Menü Anrufkontrolle Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des Anrufkontroll-Eintrags ein.
Administrativer Status	Wählen Sie aus, ob der Anrufkontroll-Eintrag aktiv sein soll. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.
Typ	Wählen Sie, wie der Ruf weitergeleitet werden soll. Mögliche Werte: <ul style="list-style-type: none"> • <i>Extern</i> (Standardwert): Für Rufe, die als externe Gespräche abgehend weitergeleitet werden sollen. Dazu können Standard SIP Accounts oder SIP Trunking Accounts im DDI Client Modus verwendet werden. • <i>Trunk</i> : Für Rufe, die an eine Telefonanlage hinter dem Me-

Feld	Beschreibung
	<p>die Gateway weitergeleitet werden sollen, die über eine PSTN-Leitung angeschlossen ist. Dazu können verwendet werden: PRI Schnittstellen im NT Modus, BRI Schnittstellen im NT Modus, FXS Schnittstellen, SIP Trunking Accounts im DDI Server Modus.</p> <ul style="list-style-type: none"> • <i>Verweigern</i>: Für Rufe, die nicht weitergeleitet (gesperrt) werden sollen.
Anrufende Leitung	<p>Sie können den Routing-Eintrag auf die Leitung begrenzen, auf welcher der Ruf ankommt..</p> <p>Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP Accounts ab.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PRI</i> : Begrenzt den Routing-Eintrag auf die gewählte PRI-Schnittstelle. • <i>BRI</i> : Begrenzt den Routing-Eintrag auf die gewählte BRI-Schnittstelle. • <i>FXO</i>: Begrenzt den Routing-Eintrag auf die gewählte FXO-Schnittstelle. • <i><SIP Account></i>: Begrenzt den Routing-Eintrag auf den gewählten SIP Account. • <i>Beliebig</i>: Keine Begrenzung des Routing-Eintrags.
Anrufende Adresse	<p>Sie können den Routing-Eintrag auf einen bestimmten Anrufer begrenzen. Dazu müssen Sie die Rufnummer exakt angeben (keine Wildcards).</p>
Angerufene Adresse	<p>Sie können eine Adresse numerisch (z. B. eine Rufnummer) oder alphanumerisch (z. B. für einen Trunk) eintragen, die mit der gewählten Adresse verglichen wird.</p> <p>Dabei können Sie folgende Wildcards verwenden:</p> <ul style="list-style-type: none"> • * bedeutet, dass am Ende einer Zeichenfolge beliebige weitere Zeichen folgen können. • ? dient als Platzhalter für ein beliebiges Zeichen. <p>Wenn die konfigurierte Adresse mit der signalisierten Adresse übereinstimmt, wird der Routing-Eintrag angewandt.</p>

Im Bereich **Routing-Regeln** fügen Sie Routing Einträge hinzu und konfigurieren diese. Sie können auch Routing Einträge löschen.

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

Felder im Menü Anrufkontrolle Routing-Regeln (Nur wenn Typ nicht Verweigern gewählt ist)

Feld	Beschreibung
Priorität	<p>Geben Sie eine ganze Zahl beginnend mit 1 in aufsteigender Reihenfolge ein, um die Reihenfolge der Filterregeln festzulegen.</p> <p>Die Regeln werden in der Liste in der angegebenen Reihenfolge "abgearbeitet".</p> <p>Ist eine Leitung bzw. ein SIP Account nicht verfügbar, wird automatisch die nächste Regel verwendet.</p>
Administrativer Status	<p>Wählen Sie aus, ob die Filterregel aktiv sein soll.</p> <p>Mit <i>Aktiviert</i> wird die Regel aktiv.</p> <p>Standardmäßig ist die Regel aktiv.</p>
Ausgehende Leitung	<p>Wählen Sie die verwendete PSTN Leitung (PRI, BRI, FXO) für den ausgehenden Ruf.</p>
Trunk-Leitung	<p>Nur für Typ = Trunk.</p> <p>Wählen Sie den verwendeten PSTN SIP Account für den ausgehenden Ruf.</p>
Transformation der gerufenen Adresse	<p>Geben Sie ein, wie die Rufnummer manipuliert werden soll, bevor sie für den Wahlvorgang verwendet wird.</p> <p>Notation: <a:b>, d.h. a wird durch b ersetzt. Mehrere Regeln können zu einer Regelkette zusammengefaßt werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert.</p> <p>Numerische und alphanumerische Werte sind zulässig.</p> <p>? dient als Platzhalter für ein beliebiges Zeichen.</p>


Feld	Beschreibung
	<p>Beispiel 13.1. Beispiel für eine Regel</p> <ul style="list-style-type: none"> • Regel: <:+49911> • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

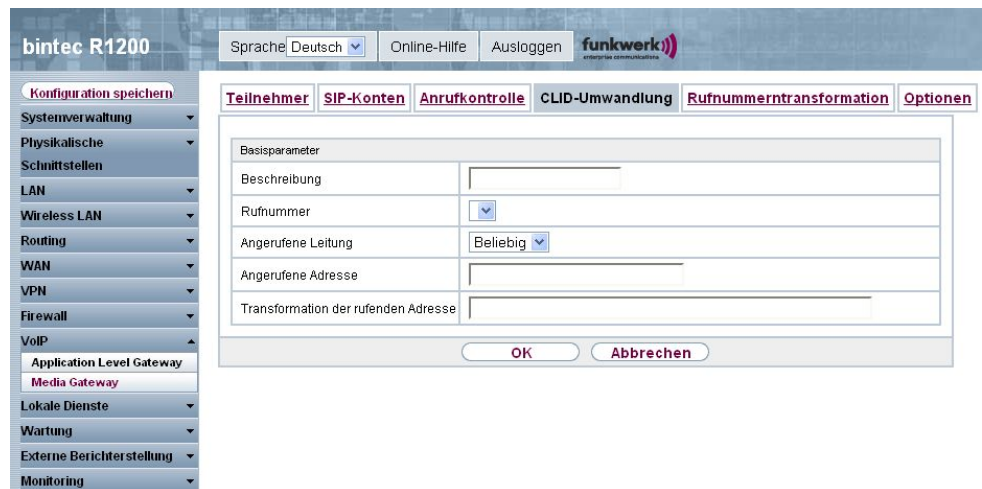
13.2.4 CLID-Umwandlung

Hier legen Sie die Bearbeitung der Rufnummer des Anrufers (Calling Party Number) bei eingehenden Anrufen fest. Sie können z. B. zu einer empfangenen Telefonnummer einen Prefix hinzufügen, um entsprechende ausgehende Gespräche über einen bestimmten Account zu routen.

Im Menü **VoIP** -> **Media Gateway** -> **CLID-Umwandlung** wird eine Liste aller vorhandenen Einträge angezeigt, bei denen die empfangene Rufnummer bearbeitet wird.

13.2.4.1 Bearbeiten/Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um Einträge für CLID-Umwandlung hinzuzufügen.



The screenshot shows the web interface for the bintec R1200. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'VoIP' section is expanded, showing 'Application Level Gateway' and 'Media Gateway'. The 'Media Gateway' section is further expanded to show 'CLID-Umwandlung'. The main configuration area for 'CLID-Umwandlung' has tabs for 'Teilnehmer', 'SIP-Konten', 'Anrufkontrolle', 'CLID-Umwandlung', 'Rufnummertransformation', and 'Optionen'. The 'CLID-Umwandlung' tab is active, displaying a 'Basisparameter' form with the following fields:

- Beschreibung:
- Rufnummer:
- Angerufene Leitung:
- Angerufene Adresse:
- Transformation der rufenden Adresse:

At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 161: **VoIP** -> **Media Gateway** -> **CLID-Umwandlung** -> **Bearbeiten/Neu**

Das Menü **VoIP** -> **Media Gateway** -> **CLID-Umwandlung** -> **Bearbeiten/Neu** besteht aus folgenden Feldern:

Felder im Menü CLID-Umwandlung Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen des CLID-Umwandlung Eintrags ein.
Rufnummer	<p>Wählen Sie die PSTN Leitung oder den SIP Account, von welcher bzw. von welchem der Anruf kommt.</p> <p>Die Auswahl hängt von den verfügbaren Schnittstellen und den angelegten SIP Accounts ab.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PRI</i> : Begrenzt den Eintrag auf die gewählte PRI-Schnittstelle. • <i>BRI</i> : Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • <i>FXO</i>: Begrenzt den Eintrag auf die gewählte FXO-Schnittstelle. • <i><SIP Account></i>: Begrenzt den Eintrag auf den gewählten SIP Account. • <i>Alle</i>: Keine Begrenzung des Eintrags.
Angerufene Leitung	<p>Sie können optional die Zielleitung des Anrufs angeben.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PRI</i> : Begrenzt den Eintrag auf die gewählte PRI-Schnittstelle. • <i>BRI</i> : Begrenzt den Eintrag auf die gewählte BRI-Schnittstelle. • <i>FXO</i>: Begrenzt den Eintrag auf die gewählte FXO-Schnittstelle. • <i><SIP Account></i>: Begrenzt den Eintrag auf den gewählten SIP Account. • <i>Beliebig</i>: Keine Begrenzung des Eintrags. <p>Geben Sie entweder Angerufene Leitung oder Angerufene Adresse ein.</p> <p>Wird ein Wert gewählt, der nicht <i>Beliebig</i> ist, so sollte Angerufene Adresse nicht benutzt werden. Ist Angerufene Leitung = <i>Beliebig</i> gesetzt und wird Angerufene Adresse nicht benutzt, so werden alle Anrufe der Angerufene Leitung behandelt.</p>

Feld	Beschreibung
Angerufene Adresse	<p>Sie können optional die Zieladresse des Anrufs angeben.</p> <p>Geben Sie entweder Angerufene Leitung oder Angerufene Adresse ein. Wird Angerufene Adresse benutzt, so sollte Angerufene Leitung = <i>Beliebig</i> gesetzt sein.</p>
Transformation der rufenden Adresse	<p>Geben Sie die Transformationsregel an, die auf die Rufnummer angewendet werden soll.</p> <p>Notation: <a:b>, d.h. a wird durch b ersetzt. Mehrere Regeln können zu einer Regelkette zusammengefaßt werden, indem die einzelnen Regeln durch Strichpunkte voneinander getrennt werden, z. B. <a:b>;<c:d>;<e:f>. Die Regelkette wird nach Bestätigung der Eingabe automatisch nach der "best match" Methode sortiert.</p> <p>? dient als Platzhalter für eine beliebige Ziffer.</p> <hr/> <p>Beispiel 13.2. Beispiel für eine Regel</p> <ul style="list-style-type: none"> • Regel: <:+49911> • gewählte Rufnummer: 96731234 • manipulierte Nummer: +4991196731234

13.2.5 Rufnummertransformation

Hier können Sie eine Liste zum Umsetzen von Rufnummern erstellen, d.h. in dieser Liste werden externe und interne Nummern einander zugeordnet.




Hinweis

Welche Rufnummer (Called Party Number oder Calling Party Number) umgesetzt wird, hängt von der Richtung (eingehend oder ausgehend) des jeweiligen Rufs ab. Bei eingehenden Rufen wird die Called Party Number, bei ausgehenden Rufen die Calling Party Number umgesetzt.

Sie können z. B. die interne Rufnummer 340 nach außen als 09119673900 darstellen oder einen Ruf von außen, der an die Nummer 09119673200 gehen soll, intern an die Nummer 340 weiterleiten.

Im Menü **VoIP** -> **Media Gateway** -> **Rufnummertransformation** wird eine Liste aller vorhandenen Einträge angezeigt, bei denen die empfangene Rufnummer bearbeitet wird.

13.2.5.1 Bearbeiten/Neu

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

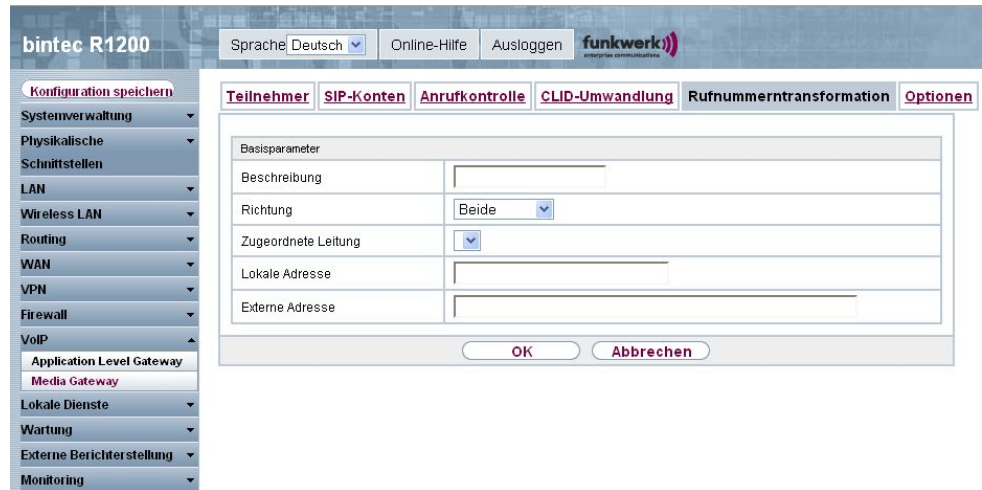


Abb. 162: **VoIP** -> **Media Gateway** -> **Rufnummertransformation** -> **Bearbeiten/Neu**

Das Menü **VoIP** -> **Media Gateway** -> **Rufnummertransformation** -> **Bearbeiten/Neu** besteht aus folgenden Feldern:

Felder im Menü Rufnummertransformation Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie den Namen der Rufnummertransformation ein.
Richtung	Wählen Sie die Rufrichtung für den Eintrag. Mögliche Werte: <ul style="list-style-type: none"> • <i>Beide</i> (Standardwert): Für eingehende und ausgehende Rufe (bidirektional). • <i>Eingehend</i> : Für eingehende Rufe. • <i>Ausgehend</i>: Für ausgehende Rufe.
Zugeordnete Leitung	Wählen Sie die Leitung oder den SIP Account, über die bzw.

Feld	Beschreibung
	<p>über den Rufe geleitet werden sollen..</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>PRI</i> : Begrenzt den Ruf auf die gewählte PRI-Schnittstelle. • <i>BRI</i> : Begrenzt den Ruf auf die gewählte BRI-Schnittstelle. • <i>FXO</i>: Begrenzt den Ruf auf die gewählte FXO-Schnittstelle. • <i>FXS</i>: Begrenzt den Ruf auf die gewählte FXS-Schnittstelle. • <i><SIP Account></i>: Begrenzt den Ruf auf den gewählten SIP Account.
Lokale Adresse	<p>Geben Sie die interne Rufnummer (z. B. Nummer einer Nebenstelle oder TK-Anlage) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld Externe Adresse) auf die Lokale Adresse umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld Lokale Adresse) auf die Externe Adresse umgesetzt.</p> <p>Numerische und alphanumerische Zeichen sind zulässig.</p> <p>? dient als Platzhalter für eine beliebige Ziffer.</p> <p>Beachten Sie, dass Lokale Adresse und Externe Adresse dieselbe Anzahl von Wildcards enthalten müssen.</p>
Externe Adresse	<p>Das Feld Externe Adresse ist nicht sichtbar, wenn das Feld Zugeordnete Leitung = <i><SIP Account></i> gesetzt ist.</p> <p>Geben Sie die externe Rufnummer (z. B. ISDN MSN oder die Rufnummer des SIP Accounts) an. Bei eingehenden Rufen wird die signalisierte Called Party Number (entspricht im Menü dem Feld Externe Adresse) auf die Lokale Adresse umgesetzt. Bei ausgehenden Rufen wird die signalisierte Calling Party Number (entspricht im Menü dem Feld Lokale Adresse) auf die Externe Adresse umgesetzt.</p>

13.2.6 Optionen

Im Menü **VoIP** -> **Media Gateway** -> **Optionen** können Sie globale Einstellungen für das Media Gateway vornehmen.



Abb. 163: VoIP ->Media Gateway-> Optionen

Das Menü **VoIP ->Media Gateway-> Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen Basisparameter

Feld	Beschreibung
Session Border Controller Modus	<p>Wählen Sie aus, wie sich das Media Gateway in Verbindung mit einem Session Border Controller Modus verhalten soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>AUS</i> : Die Anrufkontrolle wird ausschließlich vom Media Gateway entsprechend der konfigurierten Anrufkontrolle und der lokalen Nebenstellen durchgeführt. Für Rufe, die über einen bestimmten Provider (Account) geroutet werden sollen, müssen Sie einen entsprechenden Anrufkontrolle Eintrag konfigurieren. Interne Rufe (von interner Nebenstelle zu interner Nebenstelle), die nur lokal geroutet werden müssen, benötigen keinen zusätzlichen Anrufkontrolle Eintrag. • <i>Auto</i> : Die Anrufkontrolle wird für alle Nebenstellen, die mit einem existierenden Account exakt übereinstimmen, vom Session Border Controller Modus durchgeführt, d.h. alle SIP Meldungen, die für den entsprechenden Account konfiguriert sind, werden an den Session Border Controller Modus weitergeleitet. Für alle anderen Nebenstellen wird die Anrufkontrolle vom Media Gateway entsprechend der dort konfigurierten Anrufkontrolle Einträge durchgeführt. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der

Feld	Beschreibung
	<p>Provider nicht verfügbar ist (Backup).</p> <ul style="list-style-type: none"> • <i><SIP Trunk></i>: Ein SIP Trunk Konto ist unter VoIP -> Media Gateway -> SIP-Konten konfiguriert und für den Session Border Controller Modus ausgewählt. Die Anruferkontrolle wird in diesem Fall für alle Nebenstellen vom Session Border Controller Modus ausgeführt, alle SIP Meldungen, die für das ausgewählte Konto konfiguriert sind, werden an den Session Border Controller Modus weitergeleitet. Beachten Sie, dass das Routing vom Media Gateway durchgeführt wird, wenn der Provider nicht verfügbar ist (Backup).
Media Stream Termination	<p>Wählen Sie, wie RTP-Sessions vom System kontrolliert werden sollen.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p> <p>Wenn die Funktion aktiv ist, werden die RTP-Sessions auf dem Media Gateway terminiert, d.h. alle RTP Streams werden vom Media Gateway kontrolliert und über das Media Gateway geroutet. Die beteiligten Endgeräte (z. B. SIP-Telefone) sind nicht direkt miteinander verbunden. Beachten Sie, dass das Media Gateway bei VoIP-zu-VoIP-Verbindungen unterschiedliche Codecs der beteiligten VoIP-Endgeräte nicht übersetzt. Daher müssen die Codecs von Media Gateway und VoIP-Endgeräten übereinstimmen.</p> <p>Wenn die Funktion nicht aktiv ist, werden die RTP-Sessions nicht auf dem Media Gateway terminiert, d.h. alle RTP Streams werden ohne Terminierung vom Media Gateway geroutet. Die RTP-Datenpakete können in komplexen Netzen somit auch über andere Gateways geroutet werden.</p>
Standard-Abwurfnebenstelle	<p>Sie können eine Nebenstelle angeben, zu der Telefonate geleitet werden, die nicht geroutet werden können, da für sie kein gültiger Routing-Eintrag existiert.</p>
Wahlpause	<p>Geben Sie die maximale Verzögerungszeit ein bis das System die eingegebene Telefonnummer als vollständig wertet und der SIP-Wählvorgang (Senden der SIP INVITE Message) startet. Diese Zeitspanne wird mit jedem Tastendruck zurückgesetzt.</p> <p>Der Standardwert ist 5.</p>

Feld	Beschreibung
	Wenn Sie die Rufnummer mit # abschließen, wird sofort gewählt.

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Kurzwahl	Klicken Sie auf Hinzufügen um neue Kurzwahlen zu konfigurieren.

Kapitel 14 Lokale Dienste

14.1 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 (Forwarded Domains) ein.
- DNS Cache, um die positiven und negativen Ergebnisse von DNS-Anfragen zu speichern.
- Statische Einträge (Static Hosts), um Zuordnungen von IP-Adressen zu Namen manuell festzulegen oder zu verhindern.
- DNS-Monitoring, um einen Überblick über DNS-Anfragen auf Ihrem Gerät zu ermöglichen.

Globale Name-Server

Unter **Lokale Dienste** -> **DNS** -> **Globale Einstellungen** -> **Basisparameter** werden die IP-Adressen von globalen Name-Servern eingetragen, die befragt werden, wenn Ihr Gerät Anfragen nicht selbst oder durch Forwarding-Einträge beantworten kann.

Für lokale Anwendungen kann als globaler Name-Server die IP-Adresse Ihres Geräts selbst oder die allgemeine Loopback-Adresse (127.0.0.1) eingetragen werden.

Die Adressen der globalen Name-Server kann Ihr Gerät auch dynamisch 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 globale Name-Server eingetragen sind, der primäre DNS-Server, danach der sekundäre DNS-Server befragt. Sind für lokale Anwendungen die IP-Adresse Ihres Geräts oder die Loopback-Adresse eingetragen, werden diese hier ignoriert. 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, wenn das Überschreiben der Adressen der globalen Name-Server zulässig ist (**DNS-Serverkonfiguration** = *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 werden diese als globale Name-Server eingetragen und stehen 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.

14.1.1 Globale Einstellungen

bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk**
enterprise communications

Konfiguration speichern

Globale Einstellungen Statische Hosts Domänenweiterleitung Cache Statistik

Basisparameter

Domänenname:

DNS-Serverkonfiguration: Dynamisch Statisch

WINS-Server

Primär:

Sekundär:

Erweiterte Einstellungen:

Positiver Cache: Aktiviert

Negativer Cache: Aktiviert

Cache-Größe:

Maximale TTL für positive Cacheeinträge:

Maximale TTL für negative Cacheeinträge:

Alternative Schnittstelle, um DNS-Server zu erhalten:

Für DNS-WINS-Serverzuordnung zu verwendende IP-Adresse

Als DHCP-Server: Keine Eigene IP-Adresse Globale DNS-Einstellung

Als IPCP-Server: Keine Eigene IP-Adresse Globale DNS-Einstellung

OK Abbrechen

Abb. 164: Lokale Dienste -> DNS -> Globale Einstellungen

Das Menü **Lokale Dienste -> DNS -> Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Globale Einstellungen Basisparameter

Feld	Beschreibung
Domänenname	Geben Sie den Standard Domain-Namen Ihres Geräts ein.
DNS-Serverkonfiguration	<p>Wählen Sie aus, ob die Adressen der globalen Name-Server auf Ihrem Gerät mit übermittelten Name-Server-Adressen überschrieben werden dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> <i>Dynamisch</i> (Standardwert): Die Name-Server-Adressen können automatisch überschrieben werden.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Statisch</i>: Die Name-Server-Adressen werden nicht überschrieben.
DNS-Server	Nur für DNS-Serverkonfiguration = <i>Statisch</i>
Primär	Geben Sie die IP-Adresse des ersten und falls erforderlich des zweiten globalen DNS-Servers ein.
Sekundär	
WINS-Server	Geben Sie die IP-Adresse des ersten und falls erforderlich des alternativen globalen Windows Internet Name Servers (=WINS) oder NetBIOS Name Servers (=NBNS) ein.
Primär	
Sekundär	

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

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Positiver Cache	<p>Wählen Sie aus, ob der positive dynamische Cache aktiviert werden soll, d. h. ob erfolgreich aufgelöste Namen und IP-Adressen im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Negativer Cache	<p>Wählen Sie aus, ob der negative dynamische Cache aktiviert werden soll, d. h. ob angefragte Namen, zu denen ein DNS-Server eine negative Antwort geschickt hat, als negative Einträge im Cache gespeichert werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Cache-Größe	<p>Geben Sie die maximale Gesamtanzahl der statischen und dynamischen Einträge ein.</p> <p>Wird dieser Wert erreicht, wird bei einem neu hinzukommenden Eintrag derjenige dynamische Eintrag gelöscht, der am längsten nicht angefragt wurde. Wird Cache-Größe vom Benutzer heruntersgesetzt, werden gegebenenfalls dynamische Einträge gelöscht. Statische Einträge werden nicht gelöscht. Cache-Größe</p>

Feld	Beschreibung
	<p>kann nicht kleiner als die aktuell vorhandene Anzahl von statischen Einträgen gesetzt werden.</p> <p>Mögliche Werte: <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>
Schnittstelle zurücksetzen, um DNS-Server zu erhalten	<p>Wählen Sie die Schnittstelle aus, zu der eine Verbindung zur Name-Server-Verhandlung aufgebaut wird, wenn andere Versuche zur Namensauflösung nicht erfolgreich waren.</p> <p>Standardwert ist <i>Automatisch</i> d. h. es wird einmalig eine Verbindung zum ersten geeigneten Verbindungspartner aufgebaut, der im System konfiguriert ist.</p>
Für DNS-/WINS-Serverzuordnung zu verwendende IP-Adresse	<p>Als DHCP-Server</p> <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>Globale DNS-Einstellung</i> : Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt. <p>Als IPCP-Server</p> <p>Wählen Sie aus, welche Name-Server-Adressen von Ihrem Ge-</p>

Feld	Beschreibung
	<p>rät 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>Globale DNS-Einstellung</i> (Standardwert): Es werden die Adressen der auf Ihrem Gerät eingetragenen globalen Name-Server übermittelt.

14.1.2 Statische Hosts

Im Menü **Lokale Dienste** -> **DNS** -> **Statische Hosts** wird eine Liste aller konfigurierten statischen Hosts angezeigt.

14.1.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere statische Hosts einzurichten.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache' (Deutsch), 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. A left sidebar contains a menu with 'Konfiguration speichern' at the top, followed by 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', and 'Monitoring'. Under 'Lokale Dienste', the sub-menu is expanded to show 'DNS', 'DynDNS-Client', 'DHCP-Server', 'Web-Filter', 'CAPI-Server', 'Scheduling', 'Überwachung', 'ISDI-Diebstahlsicherung', 'Funkwerk Discovery', 'UPnP', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The main content area has tabs for 'Globale Einstellungen', 'Statische Hosts', 'Domänenweiterleitung', 'Cache', and 'Statistik'. The 'Statische Hosts' tab is active, showing a 'Basisparameter' table with the following fields: 'Beschreibung' (empty), 'Antwort' (Positiv), 'IP-Adresse' (0.0.0.0), and 'TTL' (86400 Sekunden). At the bottom of the table are 'OK' and 'Abbrechen' buttons.

Abb. 165: Lokale Dienste -> DNS -> Statische Hosts -> Neu

Das Menü **Lokale Dienste -> DNS -> Statische Hosts -> Neu** besteht aus folgenden Feldern:

Felder im Menü Statische Hosts Basisparameter

Feld	Beschreibung
Beschreibung	<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. *.funkwerk-ec.com.</p> <p>Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK "<Name>." ergänzt.</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 Name wird negativ be-

Feld	Beschreibung
	<p>antwortet.</p> <ul style="list-style-type: none"> • <i>Positiv</i> (Standardwert): Eine DNS-Anfrage nach Name wird mit der dazugehörigen IP-Adresse beantwortet. • <i>Keiner</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 Name zugeordnet wird.</p>
TTL	<p>Geben Sie die Gültigkeitsdauer der Zuordnung von Name 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>

14.1.3 Domänenweiterleitung

Im Menü **Lokale Dienste** -> **DNS** -> **Domänenweiterleitung** wird eine Liste aller konfigurierter Weiterleitungen für definierte Domänen angezeigt.

14.1.3.1 Neu

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

bintec R1200 Sprache: Deutsch ▼ Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Globale Einstellungen **Statische Hosts** **Domänenweiterleitung** **Cache** **Statistik**

Weiterleitungsparameter

Weiterleiten Host Domäne

Host

Weiterleiten an Schnittstelle DNS-Server

Schnittstelle Automatisch ▼

OK **Abbrechen**

Systemverwaltung ▼

Physikalische ▼

Schnittstellen

LAN ▼

Wireless LAN ▼

Routing ▼

WAN ▼

VPN ▼

Firewall ▼

VoIP ▼

Lokale Dienste ▲

DNS

DynDNS-Client

DHCP-Server

Web-Filter

CAPi-Server

Scheduling

Überwachung

ISDI-Diebstahlsicherung

Funkwerk Discovery

UPnP

Wartung ▼

Externe Berichterstellung ▼

Monitoring ▼

Abb. 166: Lokale Dienste -> DNS -> Domänenweiterleitung -> Neu

Das Menü **Lokale Dienste** -> **DNS** -> **Domänenweiterleitung** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü Domänenweiterleitung Weiterleitungsparameter

Feld	Beschreibung
Weiterleiten	<p>Wählen Sie aus, ob ein Host oder eine Domäne weitergeleitet werden soll.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Host</i> (Standardwert) • <i>Domäne</i>
Host	<p>Nur für Weiterleiten = <i>Host</i></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. *.funkwerk.com. Bei Eingabe eines Namens ohne Punkt wird nach Bestätigung mit OK " <Default Domain>." ergänzt.</p>

Feld	Beschreibung
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. *.funkwerk.com. 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-Servers ein.</p>

14.1.4 Cache

Im Menü **Lokale Dienste** -> **DNS** -> **Cache** wird eine Liste aller vorhandenen Cache-Einträge angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with 'Konfiguration speichern' at the top, followed by 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', and 'Lokale Dienste'. Under 'Lokale Dienste', several options are listed: 'DNS', 'DynDNS-Client', 'DHCP-Server', 'Web-Filter', 'CAPT-Server', 'Scheduling', 'Überwachung', 'ISDI-Diebstahlsicherung', 'Funkwerk Discovery', 'UPnP', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The main content area is titled 'Cache' and contains a table with the following structure:

Beschreibung	IP-Adresse	Antwort	TTL	Referenzzähler	Alle auswählen / Alle deaktivieren	Als statisch festlegen
Setze: 1						

At the top of the main content area, there is a control bar with 'Automatisches Aktualisierungsintervall 60 Sekunden' and a 'Übernehmen' button. Below the table, there are 'OK' and 'Abbrechen' buttons.

Abb. 167: 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 damit aus dieser Liste und wird in der Liste im Menü **Statische Hosts** aufgelistet. Die TTL wird dabei übernommen.

14.1.5 Statistik

The screenshot shows the web interface of a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', and 'Monitoring'. Under 'Lokale Dienste', 'DNS' is selected. The main content area has tabs for 'Globale Einstellungen', 'Statische Hosts', 'Domänenweiterleitung', 'Cache', and 'Statistik'. The 'Statistik' tab is active, displaying a table of DNS statistics. At the top of the statistics section, there is a field for 'Automatisches Aktualisierungsintervall' set to '60' seconds and a 'Übernehmen' button.

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. 168: Lokale Dienste -> DNS -> Statistik

Im Menü **Lokale Dienste** -> **DNS** -> **Statistik** werden folgende statistische Werte angezeigt:

Felder im Menü Statistik 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.

Feld	Beschreibung
Cache-Trefferrate (%)	Zeigt die Anzahl der Cache-Treffer pro DNS-Anforderung 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.

14.2 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, 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.

14.2.1 DynDNS-Aktualisierung

Im Menü **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Aktualisierung** wird eine Liste aller konfigurierten DynDNS-Registrierungen angezeigt, die aktualisiert werden sollen.

14.2.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere zu aktualisierende DynDNS-Registrierungen einzurichten.

bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk**
enterprise communications

Konfiguration speichern

- Systemverwaltung
- Physikalische Schnittstellen
- LAN
- Wireless LAN
- Routing
- WAN
- VPN
- Firewall
- VoIP
- Lokale Dienste**
 - DNS
 - DynDNS-Client**
 - DHCP-Server
 - Web-Filter
 - CAPT-Server
 - Scheduling
 - Überwachung
 - ISDH-Diebstahlsicherung
 - Funkwerk Discovery
 - UPnP
- Wartung
- Externe Berichterstellung
- Monitoring

DynDNS-Aktualisierung **DynDNS-Provider**

Basisparameter

Hostname	<input type="text"/>
Schnittstelle	Eine auswählen <input type="button" value="v"/>
Benutzername	<input type="text"/>
Passwort	••••••••
Provider	dyndns <input type="button" value="v"/>
Aktualisierung aktivieren	<input type="checkbox"/> Aktiviert

Erweiterte Einstellungen

Mail-Exchanger (MX)	<input type="text"/>
Wildcard	<input type="checkbox"/> Aktiviert

Abb. 169: Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu

Das Menü **Lokale Dienste -> DynDNS-Client -> DynDNS-Aktualisierung -> Neu** besteht aus folgenden Feldern:

Felder im Menü DynDNS-Aktualisierung 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	Wählen Sie den DynDNS-Provider aus, bei dem oben genannte Daten registriert sind.

Feld	Beschreibung
	<p>Im unkonfigurierten Zustand stehen Ihnen bereits DynDNS-Provider zur Auswahl, deren Protokolle unterstützt werden.</p> <p>Weitere DynDNS-Provider können im Menü Lokale Dienste -> DynDNS-Client -> DynDNS-Provider konfiguriert werden.</p> <p>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>

14.2.2 DynDNS-Provider

Im Menü **Lokale Dienste** -> **DynDNS-Client** -> **DynDNS-Provider** wird eine Liste aller konfigurierter DynDNS-Provider angezeigt.

14.2.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere DynDNS-Provider einzurichten.

The screenshot shows the configuration interface for a DynDNS provider on a bintec R1200 device. The left sidebar contains a menu with 'Lokale Dienste' expanded to 'DynDNS-Client'. The main content area is titled 'DynDNS-Aktualisierung' and 'DynDNS-Provider'. It contains a 'Basisparameter' table with the following fields:

Basisparameter	
Providername	<input type="text"/>
Server	<input type="text"/>
Aktualisierungspfad	<input type="text"/>
Port	80
Protokoll	DynDNS
Aktualisierungsintervall	300 Sekunden

Buttons for 'OK' and 'Abbrechen' are located at the bottom of the form.

Abb. 170: Lokale Dienste -> DynDNS-Client -> DynDNS-Provider -> Neu

Das Menü **Lokale Dienste -> DynDNS-Client -> DynDNS-Provider -> Neu** besteht aus folgenden Feldern:

Felder im Menü DynDNS-Provider 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.

Feld	Beschreibung
Port	<p>Geben Sie den Port ein, auf dem Ihr Gerät den Server Ihres Providers ansprechen soll.</p> <p>Erfragen Sie den entsprechenden Port bei Ihrem Provider.</p> <p>Standardwert ist <i>80</i> .</p>
Protokoll	<p>Wählen Sie eines der implementierten Protokolle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>DynDNS</i> (Standardwert) • <i>Statischer DynDNS</i> • <i>ODS</i> • <i>HN</i> • <i>DYNS</i> • <i>GnuDIP-HTML</i> • <i>GnuDIP-TCP</i> • <i>Benutzerdefinierter DynDNS</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>

14.3 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. Ein Rechner sendet einen ARP-Request aus und erhält daraufhin seine IP-Adresse von Ihrem Gerät zugewiesen. 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.

14.3.1 DHCP-Pool

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-Pool** wird eine Liste aller konfigurierter IP-Adresspools angezeigt.

In der Liste haben Sie zu jedem Eintrag unter **Pool** die Möglichkeit, die angelegten DHCP-Pools zu aktivieren bzw. deaktivieren.

14.3.1.1 Neu


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



Abb. 171: Lokale Dienste -> DHCP-Server -> DHCP-Pool -> Neu

Das Menü **Lokale Dienste** -> **DHCP-Server** -> **DHCP-Pool** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü DHCP-Pool Basisparameter

Feld	Beschreibung
Schnittstelle	<p>Wählen Sie die Schnittstelle aus, über welche die in IP-Bereich definierten Adressen an anfragende DHCP-Clients vergeben werden.</p> <p>Wenn eine DHCP-Anfrage über diese Schnittstelle eingeht, wird eine der Adressen aus dem Adress-Pool zugeteilt.</p>
IP-Adressbereich	<p>Geben Sie die erste (erstes Feld) und die letzte (zweites Feld) IP-Adresse des IP-Adress-Pools ein.</p>
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>Lokal/Relay</i>: Der DHCP-Pool wird für DHCP-Anfragen im selben Subnetz und aus anderen Subnetzen verwendet. • <i>Relay</i>: Der DHCP-Pool wird nur für weitergeleitete DHCP-Anfragen aus anderen Subnetz 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>: Wird die für Schnittstelle definierte IP-Adresse übertragen. • <i>Kein Gateway</i> (Standardwert): Es wird keine IP-Adresse übermittelt. • <i>Angeben</i>: Geben Sie die entsprechende IP-Adresse ein.

Feld	Beschreibung
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	<p>Geben Sie an, welche zusätzlichen Daten dem DHCP Client weitergegeben werden sollen.</p> <p>Mögliche Werte für Option:</p> <ul style="list-style-type: none"> • <i>Time Server</i> (Standardwert): Geben Sie die IP-Adresse des Zeit-Servers ein, die dem Client übermittelt werden soll. • <i>DNS-Server</i>: Geben Sie die IP-Adresse des DNS-Servers ein, die dem Client übermittelt werden soll. • <i>DNS-Domänename</i>: Geben Sie die DNS Domain ein, die dem Client übermittelt werden soll. • <i>WINS/NBNS-Server</i>: Geben Sie die IP-Adresse des WINS/NBNS-Servers ein, die dem Client übermittelt werden soll. • <i>WINS/NBT Node Type</i>: Geben Sie den Typ des WINS/NBT Nodes ein, 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. <p>Es sind mehrere Einträge möglich. Fügen Sie weitere Einträge mit der Schaltfläche Hinzufügen ein.</p>

14.3.2 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 nun 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 Verbindung** 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 Pool** IP-Adressbereiche konfiguriert wurden.

14.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere IP/MAC-Bindungen einzurichten.

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 IP/MAC-Bindung 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.

Feld	Beschreibung
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.

14.3.3 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.

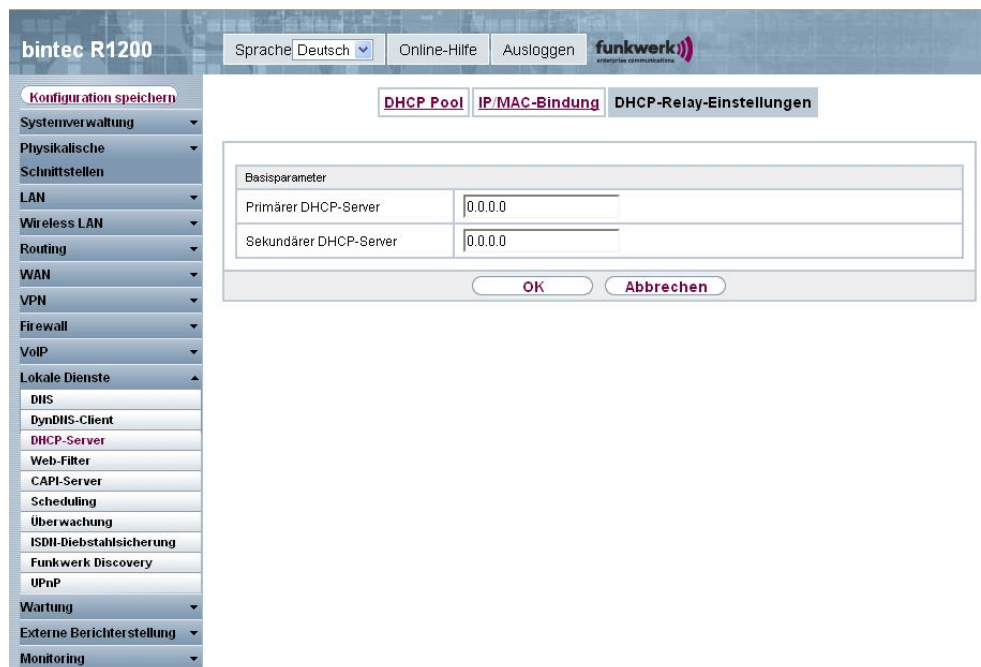


Abb. 173: Lokale Dienste -> DHCP-Server -> DHCP-Relay-Einstellungen

Das Menü **Lokale Dienste -> DHCP-Server -> DHCP-Relay-Einstellungen** besteht aus folgenden Feldern:

Felder im Menü DHCP-Relay-Einstellungen 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.

14.4 Web-Filter

Im Menü **Lokale Dienste** -> **Web-Filter** lässt sich ein URL-basierter Web-Filter-Dienst konfigurieren, der zur Laufzeit auf das Proventia Web Filter der Firma Internet Security Systems (www.iss.net) zugreift und überprüft, wie eine angeforderte Internet-Seite durch das Proventia Web Filter kategorisiert worden ist. Die Aktion, die sich aus der Kategorisierung ergibt, wird auf Ihrem Gerät konfiguriert.

14.4.1 Globale Einstellungen

In diesem Menü finden Sie die Konfiguration grundlegender Parameter für die Nutzung des Proventia Web Filters.

The screenshot shows the configuration page for the bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Lokale Dienste', with 'Web-Filter' selected. The main content area is titled 'Globale Einstellungen' and contains two sections: 'Web-Filter Optionen' and 'Lizenzinformation'.

Web-Filter Optionen:

- Web-Filter aktivieren:
- Gefilterte Eingangs-Schnittstelle(n):
- Maximale Anzahl der Einträge im Verlauf:
- URL Pfadtiefe:
- Aktion wenn Server nicht erreichbar: Alle zulassen Alle blockieren Alle protokollieren
- Aktion, wenn Lizenz nicht registriert: Alle zulassen Alle blockieren Alle protokollieren

Lizenzinformation:

- Lizenzschlüssel: [\[Aktiviere 30-Tage-Demo-Lizenz\]](#)
- Lizenzstatus:
- Lizenz gültig bis:

At the bottom of the license section is a button labeled 'Übernehmen'.

Abb. 174: Lokale Dienste -> Web-Filter -> Globale Einstellungen

Das Menü **Lokale Dienste -> Web-Filter -> Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Globale Einstellungen Web-Filter Optionen

Feld	Beschreibung
Web-Filter aktivieren	Aktivieren oder deaktivieren Sie das Filter. Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Gefilterte Eingangs-	Wählen Sie aus, für welche der vorhandenen Ethernet-

Feld	Beschreibung
Schnittstelle(n)	<p>Schnittstellen Web Filtering aktiviert werden soll.</p> <p>Drücken Sie die Hinzufügen-Schaltfläche, wenn Sie weitere Schnittstellen hinzufügen wollen. Die Anforderungen von http-Internetseiten, die Ihr Gerät über diese Schnittstellen erreichen, werden dann vom Web Filtering überwacht.</p>
Maximale Anzahl der Einträge im Verlauf	<p>Definieren Sie die Anzahl an Einträgen, die im Web Filtering Verlauf (Menü Geschichte) gespeichert werden sollen.</p> <p>Mögliche Werte sind 1 bis 512.</p> <p>Standardwert ist 64.</p>
URL Pfadtiefe	<p>Wählen Sie aus, bis zu welcher Pfadtiefe eine URL durch den Cobion Orange Filter geprüft werden soll.</p>
Aktion wenn Server nicht erreichbar	<p>Wählen Sie aus, wie mit URL-Anforderungen verfahren werden soll, wenn der Web-Filtering-Server nicht erreichbar ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle zulassen</i> (Standardwert): Der Aufruf wird zugelassen. • <i>Alle blockieren</i>: Der Aufruf der angeforderten Seite wird geblockt. • <i>Alle protokollieren</i>: Der Aufruf wird zugelassen, aber protokolliert.
Aktion wenn Lizenz nicht registriert	<p>Wählen Sie aus, wie mit URL-Anforderungen verfahren werden soll, wenn der Lizenzschlüsselstatus <i>Nicht gültig</i> ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Alle zulassen</i> (Standardwert): Der Aufruf wird zugelassen. • <i>Alle blockieren</i>: Der Aufruf der angeforderten Seite wird geblockt. • <i>Alle protokollieren</i>: Der Aufruf wird zugelassen, aber protokolliert.

Das Menü **Lizenzinformation** besteht aus folgenden Feldern:

Felder im Menü Globale Einstellungen Lizenzinformation

Feld	Beschreibung
Lizenzschlüssel	<p>Tragen Sie die Nummer der erworbenen Proventia Web Filter-Lizenz ein. Die voreingestellte, von ISS vergebene Kennung bezeichnet den Gerätetyp.</p> <p>Im Auslieferungszustand haben Sie die Möglichkeit eine 30-Tage-Demoversion des Proventia Web Filter zu aktivieren. Klicken Sie hierzu die Verknüpfung [Aktiviere 30-Tage-Demo-Lizenz]</p>
Lizenz-Status	Zeigt das Ergebnis der letzten Gültigkeitsprüfung der Lizenz an. Die Gültigkeit der Lizenz wird alle 23 Stunden überprüft.
Lizenz gültig bis	Zeigt das Ablaufdatum der Lizenz (relativ zur eingestellten Zeit auf Ihrem Gerät) an und kann nicht editiert werden.

14.4.2 Filterliste

Im Menü **Lokale Dienste** -> **Web-Filter** -> **Filterliste** konfigurieren Sie, welche Kategorien von Internetseiten auf welche Weise behandelt werden sollen.

Hierfür konfigurieren Sie entsprechende Filter. Eine Liste der bereits konfigurierten Filter wird angezeigt.

Bei der Konfiguration der Filter gibt es grundsätzlich unterschiedliche Ansätze:

- Zum einen kann man eine Filterliste anlegen, die nur Einträge für solche Adressen enthält, die blockiert werden sollen. In diesem Fall ist es notwendig, am Ende der Filterliste einen Eintrag vorzunehmen, der alle Zugriffe, auf die kein Filter zutrifft, gestattet. (Einstellung dafür: **Kategorie** = *Default behaviour*, **Aktion** = *Zulassen oder Zulassen und Protokollieren*)
- Wenn Sie nur Einträge für solche Adressen anlegen, die zugelassen bzw. protokolliert werden sollen, ist eine Änderung des Standardverhaltens (=alle übrigen Aufrufe werden geblockt) nicht notwendig.

14.4.2.1 Neu

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

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'bintec R1200', a language dropdown set to 'Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', and 'Monitoring'. Under 'Lokale Dienste', 'Web-Filter' is highlighted. The main content area displays the 'Filtereinstellungen' configuration form. It has tabs for 'Globale Einstellungen', 'Filterliste', 'Black / White List', and 'Verlauf'. The form fields are: 'Kategorie' (dropdown menu showing 'Pornography / Nudity'), 'Tag' (dropdown menu showing 'Täglich'), 'Zeitplan (Start-/Stopzeit)' (input fields for 'Von 00:00' and 'bis 00:00'), and 'Aktion' (radio buttons for 'Zulassen', 'Zulassen und Protokollieren', and 'Blockieren und Protokollieren', with the last one selected). At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 175: Lokale Dienste -> Web-Filter -> Filterliste

Das Menü **Lokale Dienste -> Web-Filter -> Filterliste** besteht aus folgenden Feldern:

Felder im Menü Filterliste Filtereinstellungen

Feld	Beschreibung
Kategorie	<p>Wählen Sie aus, auf welche Kategorie von Adressen/URLs das Filter angewendet werden soll.</p> <p>Zur Auswahl stehen zum einen die Standardkategorien des Proventia Web Filters (Standardwert: <i>Pornography/Nudity</i>). Darüber hinaus können Aktionen für folgende Sonderfälle definiert werden, z. B.:</p> <ul style="list-style-type: none"> • <i>Default behaviour</i>: Diese Kategorie trifft auf alle Internet-Adressen zu. • <i>Other Category</i>: Manche Adressen sind dem Proventia Web Filter bereits bekannt, aber noch nicht kategorisiert. Für derartige Adressen wird die mit dieser Kategorie verbundene

Feld	Beschreibung
	<p>Aktion angewendet.</p> <ul style="list-style-type: none"> • <i>Unknown URL</i>: Wenn eine Adresse dem Proventia Web Filter nicht bekannt ist, wird die mit dieser Kategorie verbundene Aktion angewendet.
Tag	<p>Wählen Sie aus, an welchen Tagen das Filter aktiv sein soll.</p> <p>Zur Verfügung stehen:</p> <ul style="list-style-type: none"> • <i>Täglich</i> (Standardwert): Das Filter gilt für jeden Tag der Woche. • <i><Wochentag></i>: Das Filter gilt für einen bestimmten Tag der Woche. Es kann pro Filter nur ein Tag ausgewählt werden, für mehrere einzelne Tage müssen mehrere Filter angelegt werden. • <i>Montag-Freitag</i>: Das Filter gilt montags bis freitags. Standardwert ist <i>Täglich</i>.
Zeitplan (Start-/Stopzeit)	<p>Geben Sie bei Von ein, nach welcher Uhrzeit das Filter aktiviert werden soll. Die Eingabe erfolgt nach dem Schema hh:mm. Standardwert ist 00:00. Geben Sie bei bis ein, zu welcher Uhrzeit das Filter deaktiviert werden soll. Die Eingabe erfolgt nach dem Schema hh:mm. Standardwert ist 00:00.</p>
Aktion	<p>Wählen Sie die Aktion, die ausgeführt werden soll, wenn das Filter auf einen Aufruf zutrifft.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Blockieren und Protokollieren</i> (Standardwert): Der Aufruf der angeforderten Seite wird unterbunden und protokolliert. • <i>Zulassen und Protokollieren</i>: Der Aufruf wird zugelassen, aber protokolliert. Einsicht in die protokollierten Ereignisse ist im Menü Lokale Dienste -> Web-Filter -> Filterliste möglich. • <i>Zulassen</i>: Der Aufruf wird zugelassen und nicht protokolliert.

14.4.3 Black / White List

Das Menü **Lokale Dienste** -> **Web-Filter** -> **Black / White List** enthält eine Liste derjenigen URLs bzw. IP-Adressen, die auch dann aufgerufen werden können, wenn sie aufgrund der Filterkonfiguration und der Klassifizierung im Proventia Web Filter blockiert würden (in der Standardkonfiguration sind keine Einträge enthalten).

14.4.3.1 Hinzufügen

Wählen Sie die Schaltfläche **Hinzufügen**, um weitere URLs oder IP-Adressen der Liste hinzuzufügen.

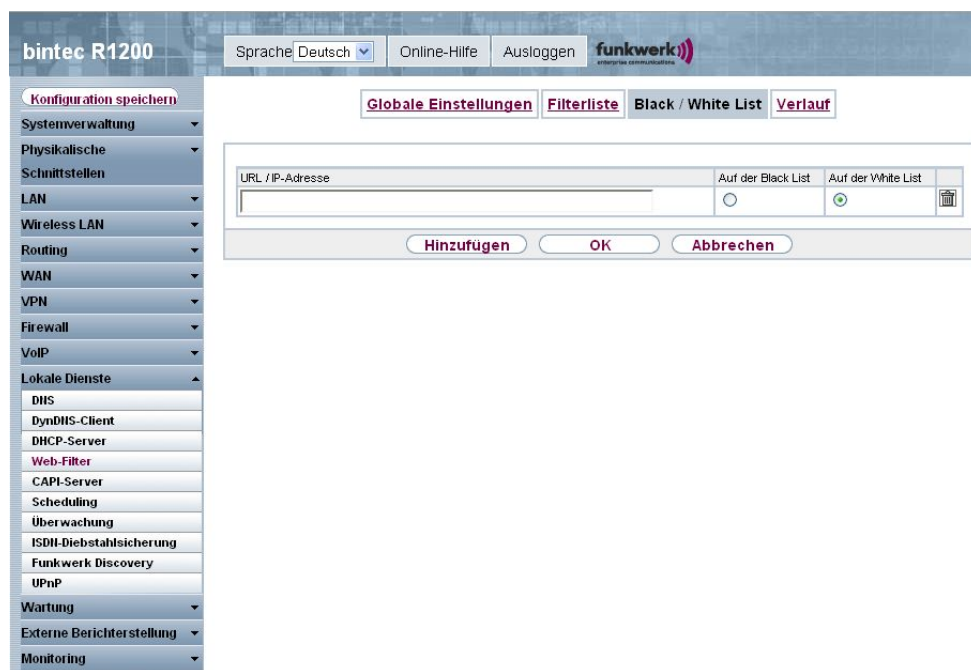


Abb. 176: Lokale Dienste -> Web-Filter -> Black / White List -> Hinzufügen

Das Menü **Lokale Dienste** -> **Web-Filter** -> **Black / White List** -> **Hinzufügen** besteht aus folgenden Feldern:

Felder im Menü Black / White List

Feld	Beschreibung
URL/IP-Adresse	Geben Sie eine URL oder IP-Adresse ein. Die Länge des Eintrags ist auf 60 Zeichen begrenzt.

Feld	Beschreibung
Auf der Black List Auf der White List	<p>Sie können wählen, ob eine URL oder IP-Adresse immer (<i>auf der White List</i>) oder nie (<i>auf der Black List</i>) aufgerufen werden kann.</p> <p>Standardmäßig ist <i>Auf der White List</i> aktiviert.</p> <p>Adressen, die in der White List geführt sind, werden automatisch zugelassen. Die Konfiguration eines entsprechenden Filters ist nicht notwendig.</p>

14.4.4 Verlauf

Im Menü **Lokale Dienste** -> **Web-Filter** -> **Verlauf** können Sie den aufgezeichneten Verlauf des Web Filters einsehen. Es werden alle Aufrufe protokolliert, die durch einen entsprechenden Filter dafür markiert werden (**Aktion** = *Protokollieren*), ebenso alle abgewiesenen Aufrufe.

The screenshot shows the web interface for a bintec R1200 device. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', and 'Lokale Dienste'. Under 'Lokale Dienste', 'Web-Filter' is selected. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. Below the top bar, there are tabs for 'Globale Einstellungen', 'Filterliste', 'Black / White List', and 'Verlauf'. The 'Verlauf' tab is active, displaying a search interface with 'Ansicht: 20 pro Seite', 'Filtern in: Keiner', and 'gleich'. Below the search bar is a table with columns: '#', 'Datum', 'Zeit', 'Quelle', 'URL', 'Kategorie', and 'Ergebnis'. The table shows 'Seite: 1' at the bottom left.

Abb. 177: Lokale Dienste -> Web-Filter -> Verlauf

14.5 CAPI-Server

Mit der Funktion CAPI-Server können Sie an Nutzer der CAPI-Anwendungen Ihres Geräts Benutzernamen und Passwörter vergeben. So stellen Sie sicher, dass nur autorisierte Nutzer eingehende Rufe empfangen und ausgehende Verbindungen über CAPI aufbauen können.

Der Dienst CAPI ermöglicht eingehenden und ausgehenden Daten- und Sprachrufen die Verbindung mit Kommunikationsanwendungen auf Hosts im LAN, die auf die Remote-CAPI-Schnittstelle Ihres Geräts zugreifen. So können beispielsweise mit Ihrem Gerät verbundene Hosts Faxe empfangen und senden.



Hinweis

Im Auslieferungszustand ist für das Subsystem CAPI immer ein Benutzer mit dem Benutzernamen *default* ohne Passwort eingetragen. Alle Rufe an die CAPI werden somit mit allen CAPI-Applikationen im LAN angeboten.

Um die eingehenden Rufe für das Subsystem CAPI auf definierte Benutzer mit Passwort zu verteilen, sollten Sie in diesem Menü Einstellungen vornehmen. Den Benutzer *default* ohne Passwort sollten Sie dann löschen.

14.5.1 Benutzer

Im Menü **Lokale Dienste** -> **CAPI-Server** -> **Benutzer** wird eine Liste aller konfigurierter CAPI Benutzer angezeigt.

14.5.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere CAPI-Benutzer einzurichten.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. Under 'Lokale Dienste', 'CAPI-Server' is selected. The main content area is titled 'Benutzer' and 'Optionen'. It features a 'Basisparameter' section with three rows: 'Benutzername' (text input), 'Passwort' (password input with masked characters), and 'Zugriff' (checkbox labeled 'Aktiviert' which is checked). At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 178: Lokale Dienste -> CAPI-Server -> Benutzer -> Neu

Das Menü **Lokale Dienste -> CAPI-Server -> Benutzer -> Neu** besteht aus folgenden Feldern:

Felder im Menü Benutzer Basisparameter

Feld	Beschreibung
Benutzername	Geben Sie den Benutzernamen ein, für den der Zugriff auf den CAPI-Dienst erlaubt bzw. gesperrt werden soll.
Passwort	Geben Sie das Passwort ein, mit dem sich der Benutzer User-name identifizieren muss, um Zugang zum CAPI Dienst zu erhalten.
Zugriff	Wählen Sie aus, ob der Zugriff auf den CAPI-Dienst für den Benutzer erlaubt oder gesperrt werden soll. Mit Auswahl von <i>Aktivieren</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

14.5.2 Optionen

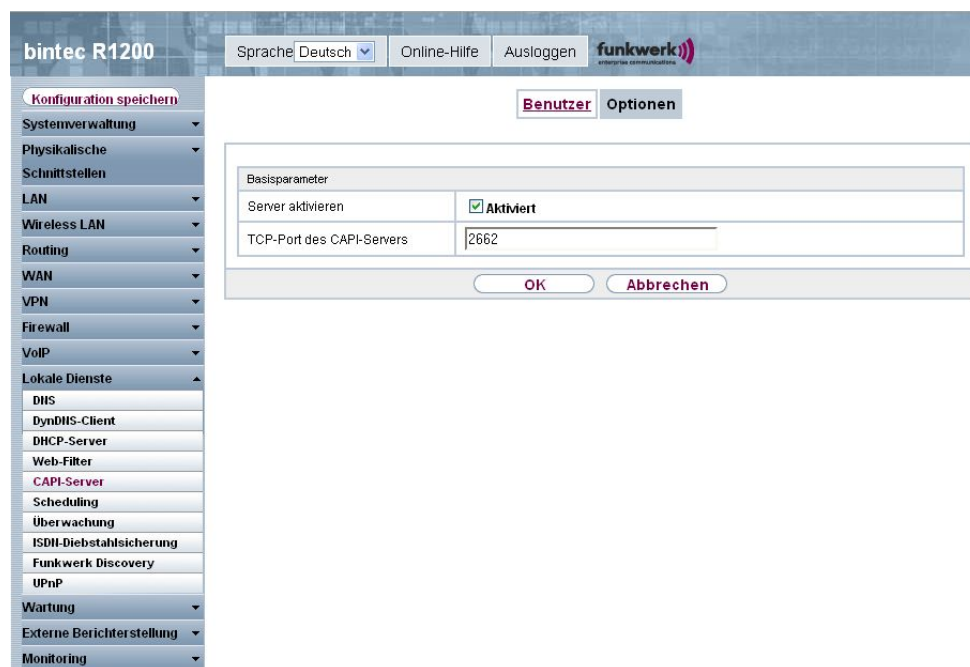


Abb. 179: Lokale Dienste -> CAPI-Server -> Optionen

Das Menü **Lokale Dienste -> CAPI-Server -> Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen Basisparameter

Feld	Beschreibung
Server aktivieren	<p>Wählen Sie aus, ob Ihr Gerät als CAPI-Server aktiviert werden soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
TCP-Port des CAPI-Servers	<p>Das Feld ist nur editierbar, wenn Server aktivieren aktiviert ist.</p> <p>Geben Sie die TCP-Port-Nummer für Remote-CAPI-Verbindungen ein.</p> <p>Standardwert ist 2662 .</p>

14.6 Scheduling

Ihr Gerät verfügt über einen Aufgabenplaner, mit dem bestimmte Standardaktionen (Aktivierung bzw. Deaktivierung von Schnittstellen) zeitabhängig durchgeführt werden können.



Hinweis

Voraussetzung für den Betrieb des Aufgabenplaners ist ein auf Ihrem Gerät eingestelltes Datum ab dem 1.1.2000.

14.6.1 Zeitplan

Im Menü **Lokale Dienste** -> **Scheduling** -> **Zeitplan** wird eine Liste aller geplanten Aufgaben angezeigt.

14.6.1.1 Neu

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

Abb. 180: Lokale Dienste -> Scheduling -> Zeitplan -> Neu

Das Menü **Lokale Dienste -> Scheduling -> Zeitplan -> Neu** besteht aus folgenden Feldern:

Felder im Menü Zeitplan Basisparameter

Feld	Beschreibung
Beschreibung	Geben Sie eine beliebige Bezeichnung für die geplante Aufgabe ein.

Felder im Menü Zeitplan Aktion

Feld	Beschreibung
Aktion auswählen	<p>Wählen Sie die gewünschte Aktion aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Gerät neu starten</i> (Standardwert): Ihr Gerät wird neu gestartet. • <i>Schnittstelle aktivieren</i>: Die im Feld Schnittstelle auswählen festgelegte Schnittstelle wird aktiv. • <i>Schnittstelle deaktivieren</i>: Die im Feld Schnittstelle auswählen festgelegte Schnittstelle wird deaktiviert.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>WLAN aktivieren</i>: Die im Feld Schnittstelle auswählen festgelegte WLAN-Schnittstelle wird aktiv. • <i>WLAN deaktivieren</i>: Die im Feld Schnittstelle auswählen festgelegte WLAN-Schnittstelle wird deaktiviert. • <i>Scan des 5-GHz-Bands initiieren</i>: Das in Radio auswählen ausgewählte Funkmodul wird im 5-GHz-Frequenzband gescannt. Während des Scans werden alle Funkverbindungen unterbrochen. • <i>Softwareaktualisierung auslösen</i>: Es wird ein Software-Update initiiert. • <i>Konfigurationssicherung auslösen</i>: Die Sicherung der Geräte-Konfiguration auf einen TFTP-Server wird initiiert.
WLAN-Modul auswählen	<p>Nur für Aktion auswählen = <i>Scan des 5-GHz-Bands initiieren</i></p> <p>Wählen Sie aus, über welches Funkmodul gescannt werden soll.</p>
Schnittstelle auswählen	<p>Nur für Aktion auswählen = <i>Schnittstelle aktivieren</i> bzw. <i>Schnittstelle deaktivieren</i></p> <p>bzw. für</p> <p>Aktion auswählen = <i>WLAN aktivieren</i> bzw. <i>WLAN deaktivieren</i></p> <p>Wählen Sie aus, welche Schnittstelle aktiviert bzw. deaktiviert werden soll.</p>
Quelle	<p>Nur für Aktion auswählen = <i>Softwareaktualisierung auslösen</i></p> <p>Wählen Sie die gewünschte Quelle aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aktuelle Software vom Funkwerk-Server</i>: Die aktuelle Software wird vom Funkwerk-Server geladen. • <i>HTTP-Server</i>: Die aktuelle Software wird von einem HTTP-Server geladen, den Sie über die <i>Aktualisierungs-URL</i> festlegen.

Feld	Beschreibung
Aktualisierungs-URL	Nur für Aktion auswählen = <i>Softwareaktualisierung auslösen</i> und Quelle = <i>HTTP-Server</i> Geben Sie die URL des HTTP-Servers ein, von dem Sie eine Konfigurationsdatei holen wollen.
TFTP-Server	Nur für Aktion auswählen = <i>Konfigurationssicherung auslösen</i> Geben Sie die IP-Adresse des TFTP-Servers ein, zu dem Sie eine Konfigurationsdatei transferieren wollen.
TFTP-Dateiname	Nur für Aktion auswählen = <i>Konfigurationssicherung auslösen</i> Geben Sie den Namen ein, unter dem die Konfigurationsdatei zum TFTP-Server transferiert werden soll.

Felder im Menü Zeitplan Zeitintervall auswählen

Feld	Beschreibung
Zeitbedingung	<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> (Standardwert): Wählen Sie in Bedingungs-einstellungen einen Wochentag aus. • <i>Perioden</i>: Wählen Sie in Bedingungs-einstellungen einen bestimmten Turnus aus. • <i>Tag des Monats</i>: Wählen Sie in Bedingungs-einstellungen einen bestimmten Tag im Monat aus. <p>Mögliche Werte für Bedingungs-einstellungen bei Bedingungs-typ = <i>Wochentag</i>:</p> <p><i>Montag</i> (Standardwert) ... <i>Sonntag</i>.</p> <p>Mögliche Werte für Bedingungs-einstellungen bei Bedingungs-typ = <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

Feld	Beschreibung
	<p>Freitag aktiv.</p> <ul style="list-style-type: none"> • <i>Montag-Samstag</i> : Der Auslöser wird täglich von Montag bis Samstag aktiv. • <i>Samstag-Sonntag</i> : Der Auslöser wird Samstag und Sonntag aktiv. <p>Mögliche Werte für Bedingungeinstellungen bei Bedingungstyp = Tag des Monats:</p> <p>1 ... 31.</p>
Startzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser aktiviert werden soll. Die Aktivierung erfolgt mit dem nächsten Scheduling-Intervall. Der Standardwert dieses Intervalls ist 55 Sekunden.
Stoppzeit	Geben Sie den Zeitpunkt ein, ab dem der Auslöser deaktiviert werden soll. Die Deaktivierung erfolgt mit dem nächsten Scheduling-Intervall. Wenn Sie keine Stoppzeit eingeben oder Stoppzeit = Startzeit setzen, wird der Auslöser aktiviert und nach 10 Sekunden deaktiviert.

14.6.2 Optionen

Im Menü **Lokale Dienste** -> **Scheduling** -> **Optionen** konfigurieren Sie das Schedule-Intervall.

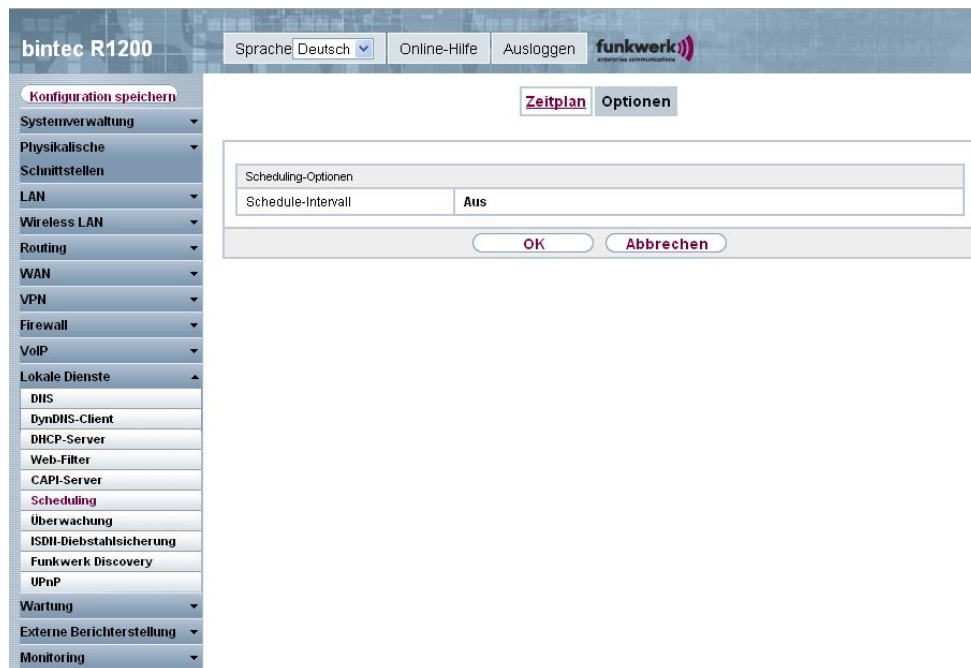


Abb. 181: Lokale Dienste -> Scheduling -> Optionen

Das Menü **Lokale Dienste -> Scheduling -> Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen Scheduling-Optionen

Feld	Beschreibung
Schedule-Intervall	<p>Geben Sie das Intervall in Sekunden ein, in dem das System überprüft, ob geplante Aufgaben anstehen.</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> <p>Wird in diesem Feld 0 angezeigt, ist der Scheduler deaktiviert.</p>

14.7 Überwachung

In diesem Menü können Sie eine automatische Erreichbarkeitsprüfung von Hosts oder Schnittstellen und automatische Ping-Tests konfigurieren.



Hinweis

Diese Funktion kann auf Ihrem Gerät nicht für Verbindungen eingerichtet werden, die über einen RADIUS-Server authentifiziert werden.

14.7.1 Hosts

Im Menü **Lokale Dienste** -> **Überwachung** -> **Hosts** wird eine Liste aller überwachten Hosts angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The top bar includes the language set to 'Deutsch', 'Online-Hilfe', 'Ausloggen', and the Funkwerk logo. The left navigation menu is expanded to 'Lokale Dienste', with 'Überwachung' selected. The main content area shows the 'Hosts' configuration page with a table of monitored hosts.

Gruppen-ID	Überwachen IP-Adresse	Status	Schnittstellenaktion	Schnittstelle		
0	0.0.0.0	+	Deaktivieren	en1-0		


Below the table is a 'Neu' button.

Abb. 182: Lokale Dienste -> Überwachung -> Hosts

Werte in der Liste Hosts

Feld	Beschreibung
Gruppen-ID	Zeigt die gewählte Gruppen-ID an.
Überwachte IP-Adresse	Zeigt die IP-Adresse, die überwacht werden soll an.
Status	Zeigt den Betriebszustand der überwachten IP-Adresse an.
Schnittstellenaktion	Zeigt die gewählte Schnittstellenaktion an.
Schnittstelle	Zeigt die Schnittstelle an, auf die die gewählte Schnittstellenaktion angewendet werden soll.

14.7.1.1 Bearbeiten / Neu

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

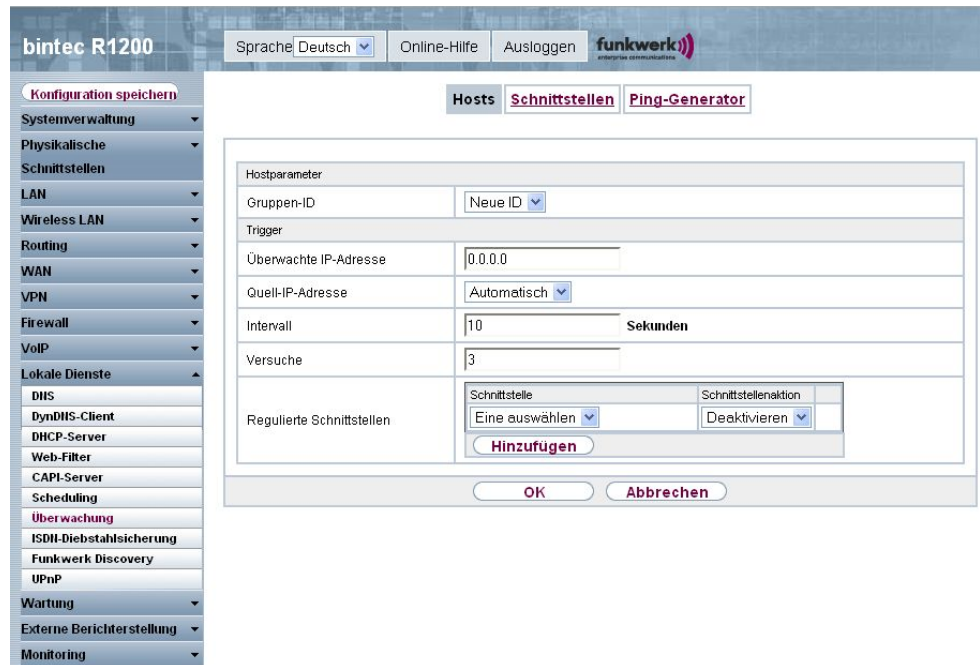


Abb. 183: Lokale Dienste -> Überwachung -> Hosts -> Neu

Das Menü **Lokale Dienste -> Überwachung -> Hosts -> Neu** besteht aus folgenden Feldern:

Feld im Menü Hosts Hostparameter

Feld	Beschreibung
Gruppen-ID	<p>Wählen Sie eine ID für die Gruppe von Hosts aus, deren Erreichbarkeit von Ihrem Gerät überwacht werden soll.</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>

Feld	Beschreibung
	Die in Schnittstellen-Aktion konfigurierte Aktion wird nur dann ausgeführt, wenn kein Gruppen-Mitglied mehr erreichbar ist.

Felder im Menü Hosts Trigger

Feld	Beschreibung
Überwachte IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, der überwacht werden soll.
Quell-IP-Adresse	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. Mögliche Werte: <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	Geben Sie das Zeitintervall (in Sekunden) ein, das zur Überprüfung der Erreichbarkeit des Hosts verwendet werden soll. Mögliche Werte sind 1 bis 65536. Standardwert ist 10 . Innerhalb einer Gruppe wird das kleinste Intervall der Gruppenmitglieder verwendet.
Versuche	Geben Sie die Anzahl der Pings ein, die unbeantwortet bleiben müssen, damit der Host als nicht erreichbar angesehen wird. Mögliche Werte sind 1 bis 65536. Standardwert ist 3 .
Regulierte Schnittstellen	Wählen Sie aus, für welche Schnittstelle(n) die unter Schnittstellenaktion festgelegte Aktion ausgeführt werden soll. Auswählbar sind alle physikalischen und virtuellen Schnittstellen. Wählen Sie zu jeder Schnittstelle aus, ob sie aktiviert (<i>Akti-</i>

Feld	Beschreibung
	<i>vieren</i>) oder deaktiviert (<i>Deaktivieren</i> , Standardwert) werden soll(en).

14.7.2 Schnittstellen

Im Menü **Lokale Dienste** -> **Überwachung** -> **Schnittstellen** wird eine Liste aller überwachten Schnittstellen angezeigt.


The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache' (Deutsch), 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Lokale Dienste' (Local Services), with 'Überwachung' (Monitoring) selected. Under 'Überwachung', the 'Schnittstellen' (Interfaces) option is highlighted. The main content area features three tabs: 'Hosts', 'Schnittstellen', and 'Ping-Generator'. Below the tabs is a table with columns for 'Überwachte Schnittstelle', 'Status', 'Trigger', 'Schnittstellenaktion', and 'Schnittstelle'. A 'Neu' button is located below the table.

Abb. 184: Lokale Dienste -> Überwachung -> Schnittstellen

Werte in der Liste Schnittstellen

Feld	Beschreibung
Überwachte Schnittstelle	Zeigt die Schnittstelle an, die überwacht werden soll.
Status	Zeigt den Betriebszustand der gewählten Schnittstelle an.
Trigger	Zeigt den gewählten Statusübergang an.
Schnittstellenaktion	Zeigt die Schnittstellenaktion an.
Schnittstelle	Zeigt die Schnittstelle an, auf die die gewählte Schnittstellenaktion angewendet werden soll.

14.7.2.1 Bearbeiten / Neu

Wählen Sie das Symbol , um vorhandene Einträge zu bearbeiten. Wählen Sie die Schaltfläche **Neu**, um die Überwachung weiterer Schnittstellen einzurichten.

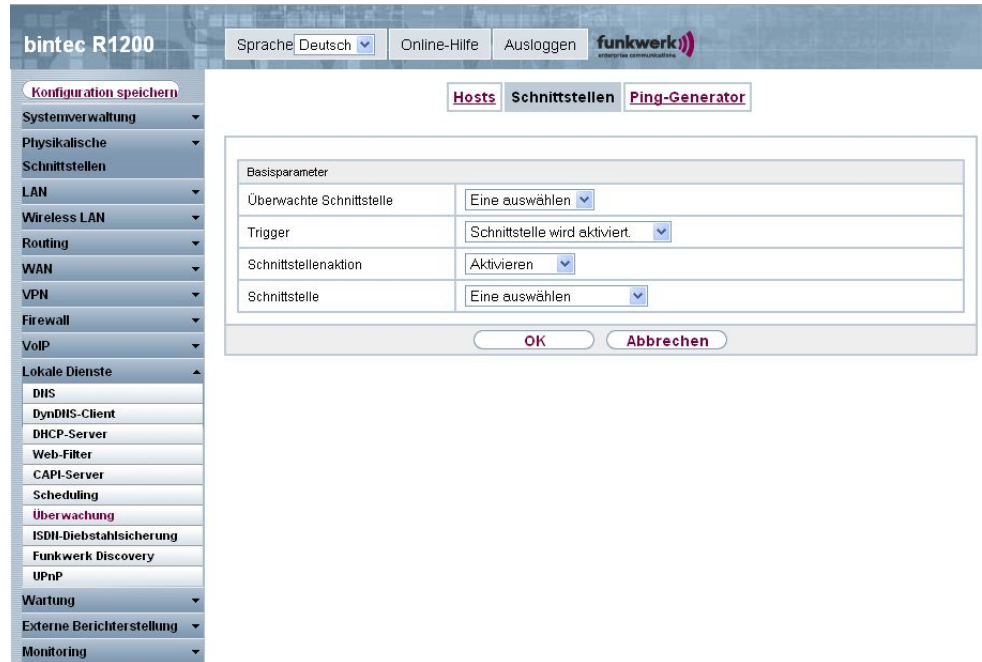


Abb. 185: Lokale Dienste -> Überwachung -> Schnittstellen -> Neu

Das Menü **Lokale Dienste -> Überwachung -> Schnittstellen -> Neu** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen 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)

Feld	Beschreibung
	<ul style="list-style-type: none">• <i>Schnittstelle wird deaktiviert</i>
Schnittstellenaktion	<p>Wählen Sie die Aktion aus, die bei dem in Trigger definierten Status bzw. Statusübergang folgen soll.</p> <p>Die Aktion wird auf die in Schnittstelle ausgewählte(n) Schnittstelle(n) angewendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">• <i>Aktiviert</i> (Standardwert): Aktivierung der Schnittstelle(n)• <i>Deaktiviert</i> : Deaktivierung der Schnittstelle(n)
Schnittstelle	<p>Wählen Sie aus, für welche Schnittstelle(n) die unter Schnittstellenaktion festgelegte Aktion ausgeführt werden soll.</p> <p>Auswählbar sind alle physikalischen und virtuellen Schnittstellen und die Optionen <i>Alle PPP-Schnittstellen</i> und <i>Alle IPSec-Schnittstellen</i>.</p>

14.7.3 Ping-Generator

Im Menü **Lokale Dienste** -> **Überwachung** -> **Ping-Generator** wird eine Liste aller konfigurierter Pings angezeigt, die automatisch generiert werden.

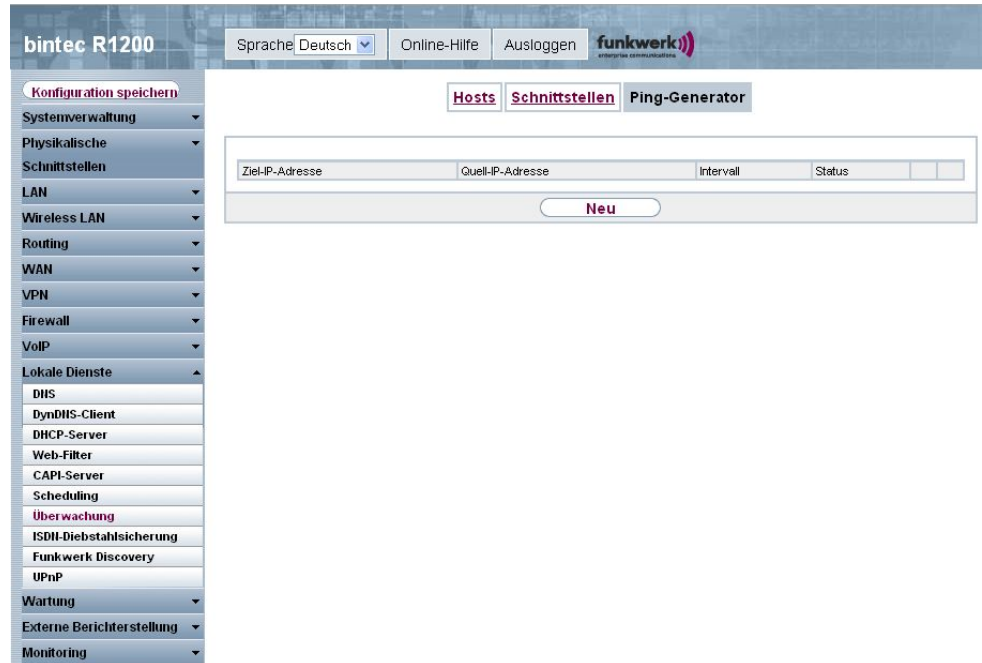



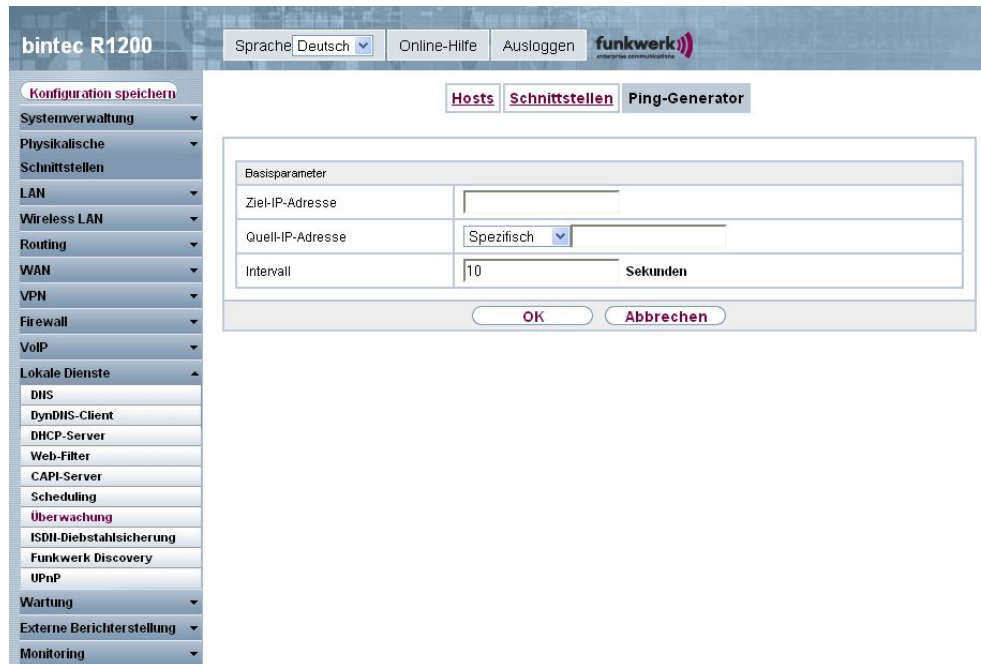
Abb. 186: Lokale Dienste -> Überwachung -> Ping-Generator

Werte in der Liste Ping-Generator

Feld	Beschreibung
Ziel-IP-Adresse	Zeigt die IP-Adresse an, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Zeigt die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein.
Intervall	Zeigt das Intervall in Sekunden ein, während dessen der Ping an die angegebene Adresse abgesetzt werden soll.
Status	Zeigt den Betriebszustand der Ziel-IP-Adresse an.

14.7.3.1 Bearbeiten / Neu

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



The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with 'Lokale Dienste' expanded to show 'Überwachung'. The main content area has three tabs: 'Hosts', 'Schnittstellen', and 'Ping-Generator'. The 'Ping-Generator' tab is active, showing a form with the following fields:

- Ziel-IP-Adresse**: An empty text input field.
- Quell-IP-Adresse**: A dropdown menu currently set to 'Spezifisch'.
- Intervall**: A text input field containing '10' followed by the label 'Sekunden'.

At the bottom of the form are two buttons: 'OK' and 'Abbrechen'.

Abb. 187: Lokale Dienste -> Überwachung -> Ping-Generator -> Neu


Das Menü **Lokale Dienste -> Überwachung -> Ping-Generator -> Neu** besteht aus folgenden Feldern:

Felder im Menü Ping-Generator Basisparameter

Feld	Beschreibung
Ziel-IP-Adresse	Geben Sie die IP-Adresse ein, an die ein Ping automatisch abgesetzt werden soll.
Quell-IP-Adresse	Geben Sie die Quell-IP-Adresse der ausgehenden ICMP-Echoanfrage-Pakete ein. Mögliche Werte: <ul style="list-style-type: none"> • <i>Automatisch</i> : Die IP-Adresse wird automatisch ermittelt. • <i>Spezifisch</i>(Standardwert): Geben Sie die IP-Adresse in

Feld	Beschreibung
	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 Ziel-IP-Adresse angegebene Adresse abgesetzt werden soll.</p> <p>Mögliche Werte sind 1 bis 65536.</p> <p>Standardwert ist 10 .</p>

14.8 ISDN-Diebstahlsicherung

Mit der Funktion ISDN-Diebstahlsicherung können Sie verhindern, dass sich ein Dieb, der ein Gateway gestohlen hat, Zutritt zum LAN des Gateway-Besitzers verschafft. (Ohne Diebstahlsicherung könnte er sich über ISDN in das LAN einwählen, wenn unter **WAN-> Internet + Einwählen ->ISDN ->**  das Feld **Immer aktiv** aktiviert ist.)

14.8.1 Optionen

Alle Schnittstellen, für welche die Diebstahlsicherung aktiv ist, werden beim Booten des Gateways administrativ auf "down" gesetzt.

Anschließend ruft sich das Gateway über ISDN selbst an und überprüft seinen Standort. Wenn die konfigurierten ISDN Rufnummern von den gewählten Rufnummern abweichen, bleiben die Schnittstellen deaktiviert.

Stimmen die Nummern überein, geht das Gerät davon aus, dass es sich am ursprünglichen Standort befindet, und die Schnittstellen werden administrativ auf "up" gesetzt.

Um Kosten zu sparen, nutzt die Funktion den ISDN D-Kanal.



Hinweis

Beachten Sie, dass die Funktion ISDN-Diebstahlsicherung für Ethernet-Schnittstellen nicht zur Verfügung steht.

bintec R1200 Sprache: **Deutsch** Online-Hilfe Ausloggen **funkwerk**
 Konfiguration speichern

Optionen

Basisparameter

ISDN-Diebstahlsicherungsdienst **Aktiviert**

Wählnummer

Eingehende Nummer

Ausgehende Nummer

Überwachte Schnittstellen

Schnittstelle

Hinzufügen

Erweiterte Einstellungen

Anzahl der Wählversuche

Timeout Sekunden

OK **Abbrechen**

Lokale Dienste

- DHIS
- DynDHIS-Client
- DHCP-Server
- Web-Filter
- CAPI-Server
- Scheduling
- Überwachung
- ISDN-Diebstahlsicherung**
- Funkwerk Discovery
- UPnP
- Wartung
- Externe Berichterstellung
- Monitoring

Abb. 188: Lokale Dienste ->ISDN-Diebstahlsicherung -> Optionen

Das Menü **Lokale Dienste ->ISDN-Diebstahlsicherung -> Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen Basisparameter

Feld	Beschreibung
ISDN-Diebstahlsicherungsdienst	Aktivieren oder deaktivieren Sie die Funktion ISDN-Diebstahlsicherung. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Wählnummer	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Geben Sie die Rufnummer ein, die das Gateway wählt, wenn es sich selbst anruft.
Eingehende Nummer	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Geben Sie die Rufnummer ein, die mit der aktuellen Calling Party Number verglichen werden soll.

Feld	Beschreibung
Ausgehende Nummer	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Geben Sie die Rufnummer ein, die als Calling Party Number gesetzt wird.
Überwachte Schnittstellen	Nur wenn ISDN-Diebstahlsicherungsdienst aktiviert ist. Fügen Sie mit Hinzufügen eine neue Schnittstelle hinzu. Wählen Sie unter den zur Verfügung stehenden Schnittstellen diejenigen aus, auf welche die Funktion ISDN-Diebstahlsicherung angewendet werden soll.

Felder im Menü Erweiterte Einstellungen

Feld	Beschreibung
Anzahl der Wählversuche	Geben Sie die Anzahl der Wählversuche ein, die das Gateway unternehmen soll, um sich nach einem Neustart über ISDN selbst anzurufen. Mögliche Werte sind 1 bis 255. Standardwert ist 3.
Timeout	Geben Sie die Zeitspanne ein, die das Gateway warten soll, bis es sich nach einem erfolglosen Versuch erneut selbst anruft. Mögliche Werte sind 2 bis 20. Standardwert ist 5.

14.9 Funkwerk Discovery

14.9.1 Gerätesuche

Das funkwerk Discovery Protokoll dient zur Erkennung und Konfiguration von **bintec** 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 Administratorpasswort).

**Hinweis**

Eventuell vorhandene **bintec** Access-Points werden mittels eines Multicasts ermittelt. Daher ist es unerheblich ob und welche IP-Adresse der Access-Point hat.

Beachten Sie, dass erkannte **bintec** Access-Points nicht im Flash gespeichert werden, d. h. die Erkennung muss nach einem Neustart Ihres Geräts wiederholt werden.


Im Menü **Lokale Dienste** -> **Funkwerk Discovery** -> **Gerätesuche** wird unter **Ergebnisse** eine Liste aller erkannten Access-Points im Netzwerk angezeigt. Im Feld **Ethernet-Schnittstelle** wählen Sie die Ethernet-Schnittstelle Ihres Geräts aus, über das die **bintec** Access-Point Erkennung durchgeführt werden soll. Mit der Option *-Alle-* werden alle Ethernet-Schnittstellen abgefragt.

Unter Ermittlungsstatus wird der aktuelle Erkennungsstatus für jede einzelne Ethernet-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**.

14.9.1.1 Finden

Wählen Sie die Schaltfläche **Finden**, um die **bintec** Access-Point-Erkennung zu starten.

bintec R1200 Sprache Online-Hilfe Ausloggen 

Konfiguration speichern Gerätesuche **Optionen**

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**




Ermittlungsstatus

Schnittstelle	Status
en1-0	Keiner

Funkwerk Discovery starten

Schnittstelle

Ergebnisse


Schnittstelle	Knotenname	IP-Adresse/Maske	MAC-Adresse	Letztes Schreibergebnis	
en1-0	w1002n	192.168.0.253 / 255.255.255.0	00:01:cd:0e:58:3e	Kein Fehler	
en1-0	wi3040	192.168.0.254 / 255.255.255.0	00:01:cd:06:1c:9e	Kein Fehler	

Finden

Lokale Dienste

- DHIS
- DynDNS-Client
- DHCP-Server
- Web-Filter
- CAPI-Server
- Scheduling
- Überwachung
- ISDI-Diebstahlsicherung
- Funkwerk Discovery**
- UPnP
- Wartung
- Externe Berichterstellung
- Monitoring

Abb. 189: Lokale Dienste -> Funkwerk 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.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with 'Lokale Dienste' expanded to 'Funkwerk Discovery'. The main content area displays the 'Gerätesuche' (Device Search) configuration page, which includes a table of 'Basisparameter' (Basic Parameters) for a discovered device.

Basisparameter	
Schnittstelle	en1-0
MAC-Adresse	00:01:cd:06:1c:9e
Knotenname	wi3040
IP-Adresse	192.168.0.254
Netzmaske	255.255.255.0
Gateway	0.0.0.0
Authentifizierungspasswort	
Letztes Schreibergebnis	Kein Fehler

At the bottom of the configuration area, there are 'OK' and 'Abbrechen' buttons.

Abb. 190: Lokale Dienste -> Funkwerk Discovery -> Gerätesuche ->

Dieses Menü **Lokale Dienste -> Funkwerk Discovery -> Gerätesuche ->** besteht aus folgenden Feldern:

Felder im Menü Funkwerk Discovery 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.

Feld	Beschreibung
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.
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>Keine Antwort</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>Ziel nicht erreichbar</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>Andere AP 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.

14.9.2 Optionen

In diesem Menü können Sie die Erlaubnis erteilen, dass auch Ihr Gerät von anderen **bintec**-Geräten mittels funkwerk Discovery Protokoll gefunden und über dieses konfiguriert werden kann.

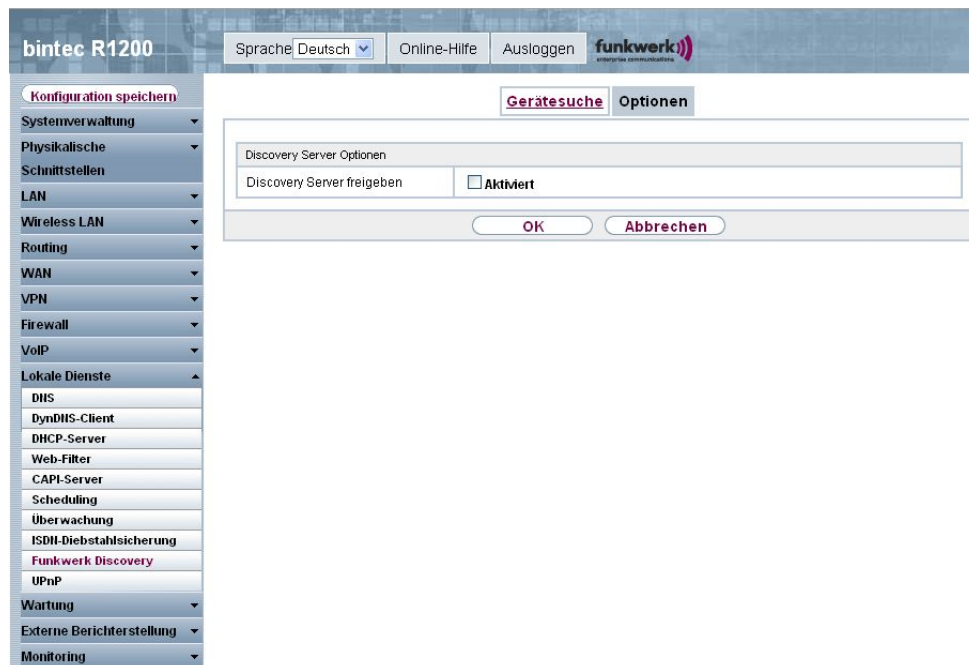


Abb. 191: Lokale Dienste -> Funkwerk Discovery -> Optionen

Das Menü **Lokale Dienste -> Funkwerk Discovery -> Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen Discovery Server Optionen

Feld	Beschreibung
Discovery Server freigeben	<p>Wählen Sie aus, ob Ihr Gerät im Netzwerk von anderen bintec-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>

14.10 UPnP

Universal Plug and Play (UPnP) ermöglicht die Nutzung aktueller Messenger-Dienste (z. B. Realtime-Video/Audiokonferenzen) als Peer-to-Peer Kommunikation, wobei einer der Peers hinter einem Gateway mit aktiver NAT-Funktion liegt.

UPnP befähigt (meist) Windows-basierte Betriebssysteme, die Kontrolle über andere Geräte im lokalen Netzwerk mit UPnP Funktionalität zu übernehmen und diese zu steuern. Dazu zählen u.a. Gateways, Access Points und Printserver. Es sind keine speziellen Gerätetreiber notwendig, da gemeinsame und bekannte Protokolle genutzt werden wie TCP/IP, HTTP und XML.

Ihr Gateway ermöglicht die Nutzung des Subsystems des Internet Gateway Devices (IGD) aus dem UPnP-Funktionsspektrum.

In einem Netzwerk hinter einem Gateway mit aktiver NAT Funktion agieren die UPnP-konfigurierten Rechner als LAN UPnP Clients. Dazu muss die UPnP Funktion auf dem PC aktiviert sein.

Der auf dem Gateway voreingestellte Port, über den die UPnP-Kommunikation zwischen LAN UPnP Clients und dem Gateway läuft, ist *5678*. Der LAN UPnP Client dient hierbei als sogenannter Service Control Point, d.h. er erkennt und kontrolliert die UPnP-Geräte im Netzwerk.

Die z. B. vom MSN Messenger dynamisch zugewiesenen Ports liegen im Bereich von *5004* bis *65535*. Die Ports werden gatewayintern bei Anforderung freigegeben, d.h. beim Start einer Audio-/Videoübertragung im Messenger. Nach Beenden der Anwendung werden die Ports sofort wieder geschlossen.

Die Peer-to-Peer-Kommunikation wird über öffentliche SIP Server initiiert, wobei lediglich die Informationen beider Clients weitergereicht werden. Anschließend kommunizieren die Clients direkt miteinander.

Weitere Informationen zu UPnP erhalten Sie auf www.upnp.org.

14.10.1 Schnittstellen

In diesem Menü konfigurieren Sie die UPnP-Einstellungen individuell für jede Schnittstelle auf Ihrem Gateway.

Sie können festlegen, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle angenommen werden (für Anfragen aus dem lokalen Netzwerk) und/oder ob die Schnittstelle über UPnP-Anfragen kontrolliert werden kann.

Abb. 192: Lokale Dienste -> UPnP-> Schnittstellen

Das Menü **Lokale Dienste ->UPnP-> Schnittstellen** besteht aus folgenden Feldern:

Felder im Menü Schnittstellen

Feld	Beschreibung
Auf Client-Anfrage antworten	Legen Sie fest, ob UPnP-Anfragen von Clients über die jeweilige Schnittstelle (aus dem lokalen Netzwerk) beantwortet werden. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion nicht aktiv.
Schnittstelle ist UPnP-kontrolliert	Legen Sie fest, ob die NAT Konfiguration dieser Schnittstelle von UPnP kontrolliert wird. Mit <i>Aktiviert</i> wird die Funktion aktiv. Standardmäßig ist die Funktion aktiv.

14.10.2 Globale Einstellungen

In diesem Menü nehmen Sie grundlegende UPnP-Einstellungen vor.

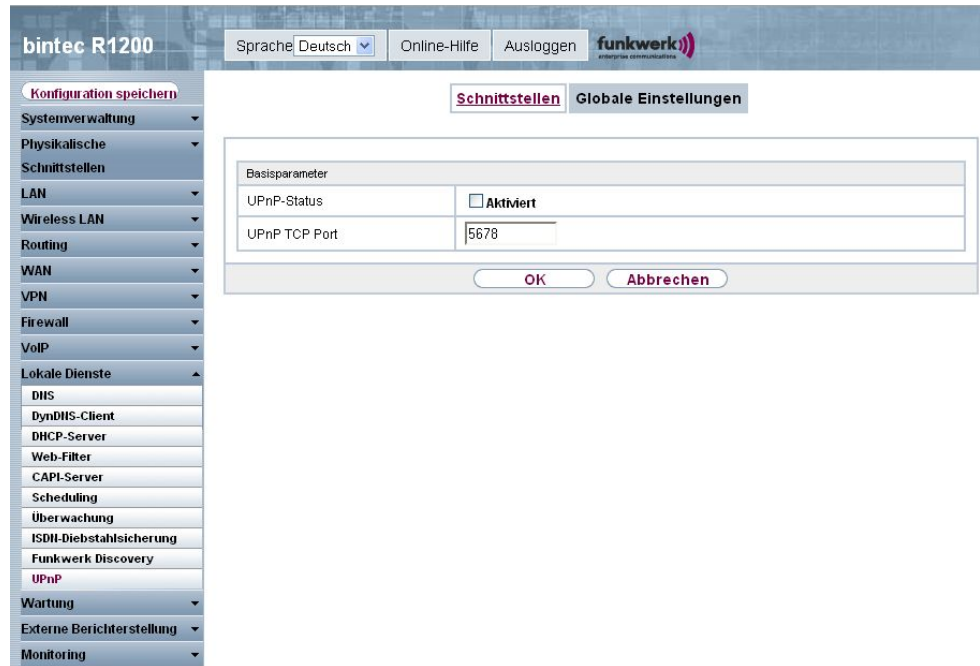


Abb. 193: Lokale Dienste -> UPnP-> Globale Einstellungen

Das Menü **Lokale Dienste ->UPnP-> Globale Einstellungen** besteht aus folgenden Feldern:

Felder im Menü Globale Einstellungen

Feld	Beschreibung
UPnP-Status	<p>Entscheiden Sie, wie das Gateway mit UPnP-Anfragen aus dem LAN verfährt.</p> <p>Mit <i>Aktiviert</i> wird die Funktion aktiv. Das Gateway nimmt die UPnP-Freigaben gemäß der in der Anfrage des LAN UPnP Clients beinhalteten Parameter vor, unabhängig von der IP Adresse des anfragenden LAN UPnP Clients.</p> <p>Standardmäßig ist die Funktion nicht aktiv. Das Gateway verwirft UPnP-Anfragen, NAT-Freigaben werden nicht vorgenommen.</p>

Feld	Beschreibung
UPnP TCP Port	<p data-bbox="635 213 1278 273">Tragen Sie die Nummer des Ports ein, auf dem das Gateway auf UPnP-Anfragen lauscht.</p> <p data-bbox="635 298 1285 333">Mögliche Werte sind 1 bis 65535, der Standardwert ist 5678.</p>

Kapitel 15 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.

15.1 Diagnose

Im Menü **Wartung** -> **Diagnose** können Sie die Erreichbarkeit von einzelnen Hosts, die Auflösung von Domain-Namen und bestimmte Routen testen.

15.1.1 Ping-Test

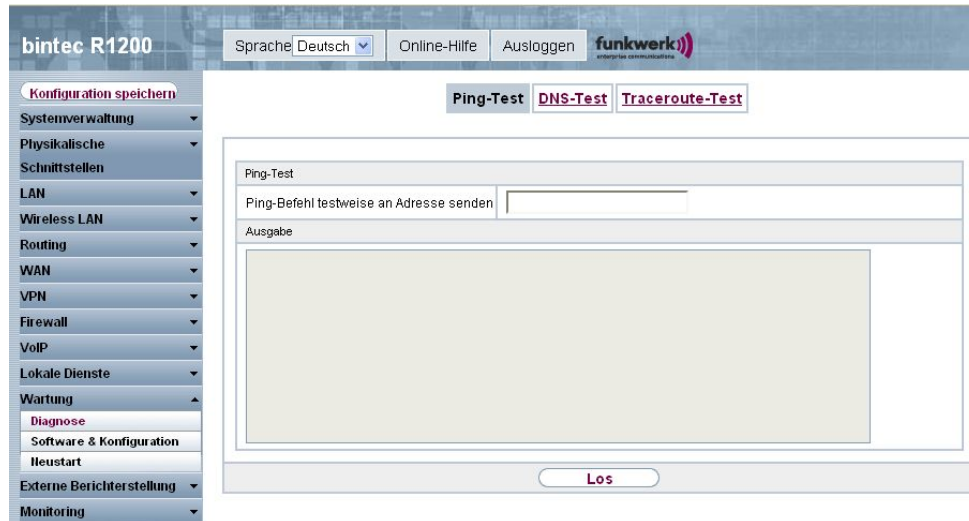


Abb. 194: **Wartung** -> **Diagnose** -> **Ping-Test**

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 Drücken der **Los**-Schaltfläche wird der Ping-Test gestartet.

15.1.2 DNS-Test

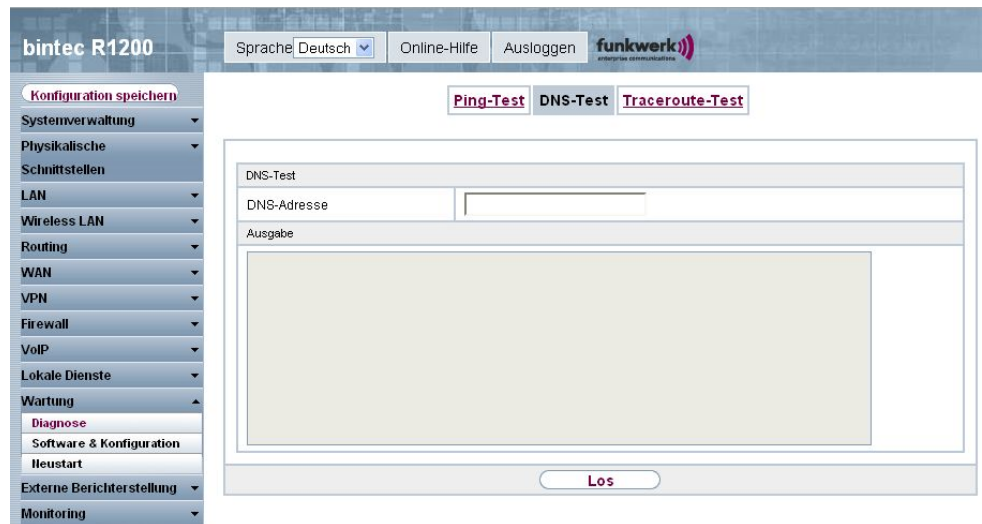


Abb. 195: **Wartung -> Diagnose -> DNS-Test**

Mit dem DNS-Test können Sie überprüfen, ob der Domänenname eines bestimmten Hosts richtig aufgelöst wird. Das **Ausgabe-Ergebnisse**-Feld zeigt die Meldungen des DNS-Tests an. Durch Eingabe des Domänennamens, der getestet werden soll, in **DNS-Adresse** und Drücken der **Los**-Schaltfläche wird der DNS-Test gestartet.

15.1.3 Traceroute-Test

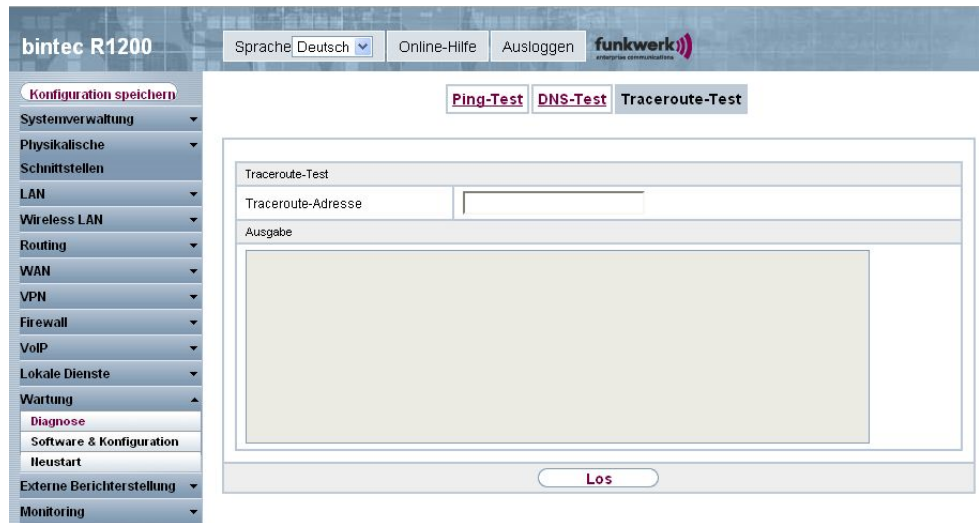


Abb. 196: **Wartung -> Diagnose -> Traceroute-Test**

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 Drücken der **Los**-Schaltfläche wird der Traceroute-Test gestartet.

15.2 Software & Konfiguration

15.2.1 Optionen

Über dieses Menü können Sie den Softwarestand Ihres Gerätes, Ihre Konfigurationsdateien sowie die Sprachversionen des **Funkwerk Configuration Interfaces** verwalten.

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.funkwerk-ec.com. Hier finden Sie auch aktuelle Dokumentationen.



Wichtig

Wenn Sie ein Software-Update durchführen, beachten Sie unbedingt die dazugehörigen Release Notes. Hier sind alle Änderungen beschrieben, die mit der neuen Systemsoftware eingeführt werden.

Die Folge von unterbrochenen Update-Vorgängen (z. B. Stromausfall während des Updates) könnte sein, dass Ihr Gerät nicht mehr bootet. Schalten Sie Ihr Gerät nicht aus, während die Aktualisierung durchgeführt wird.

In seltenen Fällen ist zusätzlich eine Aktualisierung von BOOTmonitor und/oder Logic empfohlen. In diesem Fall wird ausdrücklich in den entsprechenden Release Notes darauf hingewiesen. Führen Sie bei BOOTmonitor oder Logic nur ein Update durch, wenn Funkwerk Enterprise Communications 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 **Funkwerk Configuration Interfaces**. 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.

The screenshot shows the web interface for a bintec R1200 device. At the top, there's a header with 'bintec R1200', a language dropdown set to 'Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. A left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung' (expanded to 'Diagnose', 'Software & Konfiguration', 'Neustart'), 'Externe Berichterstellung', and 'Monitoring'. The main content area is titled 'Optionen' and contains a table for 'Aktuell installierte Software' with columns for component name and version. Below this is a section for 'Optionen zu Software und Konfiguration' with an 'Aktion' dropdown menu set to 'Keine Aktion' and a 'Los' button.

Abb. 197: **Wartung** -> **Software & Konfiguration** -> **Optionen**

Das Menü **Wartung** -> **Software & Konfiguration** -> **Optionen** besteht aus folgenden Feldern:

Felder im Menü Konfigurationsmanagement **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.
SHDSL-Logik	Zeigt die aktuelle Version der SHDSL-Logik 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 Konfigurationsmanagement **Optionen zur Software und Konfiguration**

Feld	Beschreibung
Aktion	Wählen Sie die Aktion aus, die Sie ausführen möchten. Mögliche Werte: <ul style="list-style-type: none"> • <i>Keine Aktion</i> (Standardwert):

Feld	Beschreibung
	<ul style="list-style-type: none"> • <i>Konfiguration importieren</i>: Die Konfigurationsdatei, die Sie in Dateiname auswählen, wird in den Flash-Speicher transferiert. Hinweis: Zum Aktivieren kopieren Sie die Konfiguration in die Datei <i>boot</i> bzw. benennen Sie sie um und starten Sie Ihr Gerät neu. • <i>Sprache importieren</i>: Sie können weitere Sprachversionen des Funkwerk Configuration Interfaces auf Ihr Gerät einspielen. Die Dateien können Sie vom Download-Bereich auf www.funkwerk-ec.com auf Ihren PC herunterladen und von da aus in Ihr Gerät einspielen. • <i>Systemsoftware aktualisieren</i>: Sie können eine Aktualisierung der Systemsoftware, der ADSL-Logik und des BOOTmonitors initiieren. • <i>Konfiguration exportieren</i>: Die Konfigurationsdatei Aktueller Dateiname im Flash wird zu Ihrem lokalen Host transferiert. Wenn Sie die Los-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. • <i>Konfiguration mit Statusinformation exportieren</i>: Die aktive Konfiguration aus dem RAM wird auf Ihren lokalen Host übertragen. Wenn Sie die Los-Schaltfläche drücken, erscheint ein Dialog, in dem Sie den Speicherort auf Ihrem PC auswählen und den gewünschten Dateinamen eingeben können. • <i>Kopieren</i>: Die Konfigurationsdatei im Feld Name der Quelldatei wird als Name der Zieldatei gespeichert. • <i>Umbenennen</i>: Die Konfigurationsdatei im Feld Datei auswählen wird zu Neuer Dateiname umbenannt. • <i>Konfiguration löschen</i>: Die Konfiguration im Feld Datei auswählen wird gelöscht. • <i>Datei löschen</i>: Die Datei im Feld Datei auswählen wird gelöscht.
Verschlüsselung der Konfiguration	<p>Nur für Aktion = <i>Konfiguration importieren, Konfiguration exportieren, Konfiguration mit Statusinformationen exportieren</i>. Wählen Sie aus, ob die Daten der gewählten Aktion verschlüsselt werden sollen.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p>

Feld	Beschreibung
	<p>Standardmäßig ist die Funktion nicht aktiv.</p> <p>Wenn die Funktion aktiviert ist, können Sie in das Textfeld das Passwort eingeben.</p>
Dateiname	<p>Nur für Aktion = <i>Konfiguration importieren, Sprache importieren, Systemsoftware aktualisieren</i>. Geben Sie den Dateipfad und -namen der Datei ein, oder wählen Sie die Datei mit Durchsuchen... über den Dateibrowser aus.</p>
Quelle	<p>Nur für Aktion = <i>Systemsoftware aktualisieren</i></p> <p>Wählen Sie die Quelle für 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 Funkwerk-Server</i>: Die Datei liegt auf dem offiziellen Funkwerk-Update-Server.
URL	<p>Nur für Quelle = <i>HTTP Server</i></p> <p>Hier geben Sie die URL des Update-Servers ein, von dem die Systemsoftware-Datei geladen werden soll.</p>
Aktueller Dateiname im Flash	<p>Für Aktion = <i>Konfiguration exportieren</i> Wählen Sie die Konfigurationsdatei aus, die exportiert werden soll.</p>
Zertifikate und Schlüssel einschließen	<p>Für Aktion = <i>Konfiguration exportieren, Konfiguration mit Statusinformationen exportieren</i> Wählen Sie aus, ob die gewählte Aktion auch für Zertifikate und Schlüssel gelten soll.</p> <p>Mit Auswahl von <i>Aktiviert</i> wird die Funktion aktiv.</p> <p>Standardmäßig ist die Funktion aktiv.</p>
Name der Quelldatei	<p>Nur für Aktion = <i>Kopieren</i> Wählen Sie die Quelldatei aus, die kopiert werden soll.</p>

Feld	Beschreibung
Name der Zieldatei	Nur für Aktion = <i>Kopieren</i> Geben Sie den Namen der Kopie ein.
Datei auswählen	Nur für Aktion = <i>Umbenennen</i> , <i>Konfiguration löschen</i> oder <i>Datei löschen</i> Wählen Sie die Datei oder Konfiguration aus, die umbenannt bzw. gelöscht werden soll.
Neuer Dateiname	Nur für Aktion = <i>Umbenennen</i> Geben Sie den neuen Namen der Konfigurationsdatei ein.

15.3 Neustart

15.3.1 Systemneustart

In diesem Menü können Sie einen sofortigen Neustart Ihres Geräts auslösen. Nachdem das System wieder hochgefahren ist, müssen Sie das **Funkwerk Configuration Interface** 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 der Schaltfläche **Konfiguration speichern** bestätigen, so dass diese bei dem Neustart nicht verloren gehen.

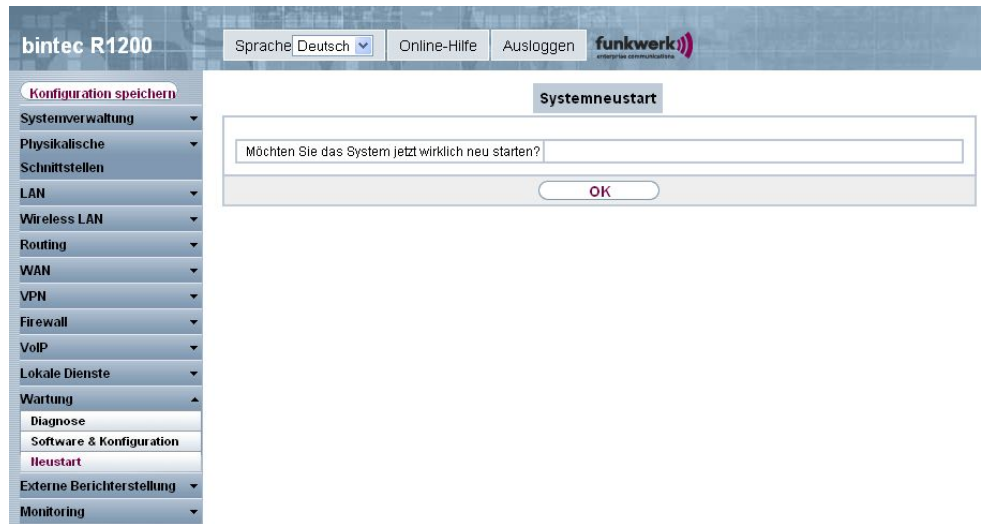


Abb. 198: Wartung -> Neustart -> Systemneustart

Wenn Sie Ihr Gerät neu starten wollen, aktivieren Sie die Option **Ja** bei **Möchten Sie das System jetzt wirklich neu starten?** Mit Drücken der **OK**-Schaltfläche wird der Neustart ausgeführt.

Kapitel 16 Externe Berichterstellung

16.1 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 (siehe **BRICKware** for Windows, abrufbar unter www.funkwerk-ec.com).

16.1.1 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.

16.1.1.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere Systemprotokoll-Server einzurichten.



Abb. 199: Externe Berichterstellung -> Systemprotokoll -> Syslog-Server -> Neu

Das Menü **Externe Berichterstellung -> Systemprotokoll -> Syslog-Server -> Neu** besteht aus folgenden Feldern:

Felder im Menü Syslog-Server 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) • <i>Alarm</i> • <i>Kritisch</i> • <i>Fehler</i> • <i>Warnung</i>

Feld	Beschreibung
	<ul style="list-style-type: none"> • <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 .</p> <p>Standardwert <i>local0</i>.</p>
Zeitstempel	<p>Wählen Sie das Format des Zeitstempels im Systemprotokoll aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keiner</i> (Standardwert): Keine Systemzeitangabe. • <i>Zeit</i>: Systemzeit ohne Datum. • <i>Datum & Uhrzeit</i>: Systemzeit mit Datum.
Protokoll	<p>Wählen Sie das Protokoll für den Transfer der Systemprotokoll-Nachrichten aus. Beachten Sie, dass der Syslog Server das Protokoll unterstützen muss.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>UDP</i> (Standardwert) • <i>TCP</i>
Nachrichtentyp	<p>Wählen Sie den Nachrichtentyp aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>System & Accounting</i> (Standardwert) • <i>System</i>

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

16.2 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 z. B. 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 überhaupt 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.

16.2.1 Schnittstellen

In diesem Menü können Sie die Funktion IP-Accounting für jede Schnittstelle einzeln konfigurieren.

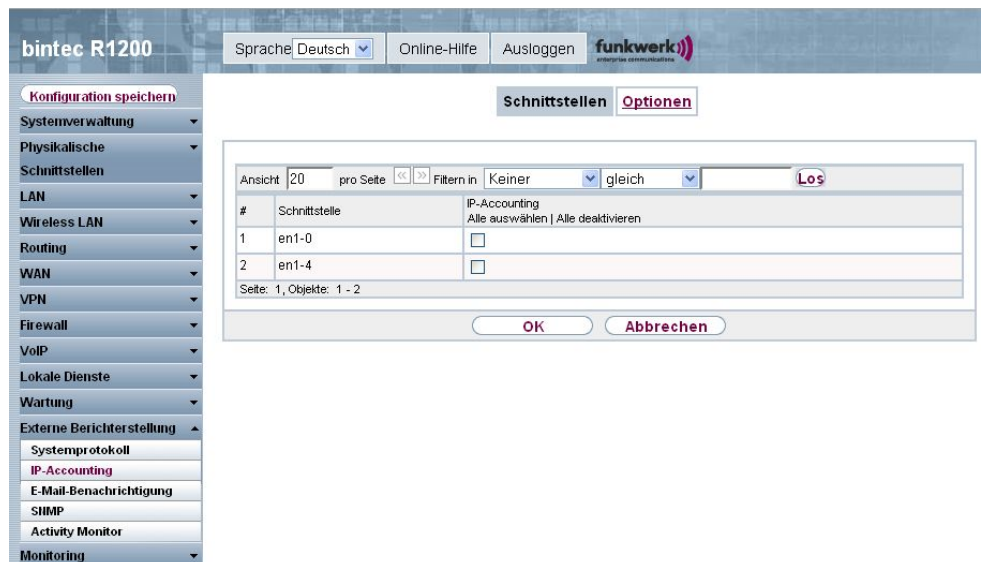


Abb. 200: Externe Berichterstellung -> IP-Accounting -> Schnittstellen

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.

16.2.2 Optionen

In diesem Menü konfigurieren Sie allgemeine Einstellungen für IP-Accounting.

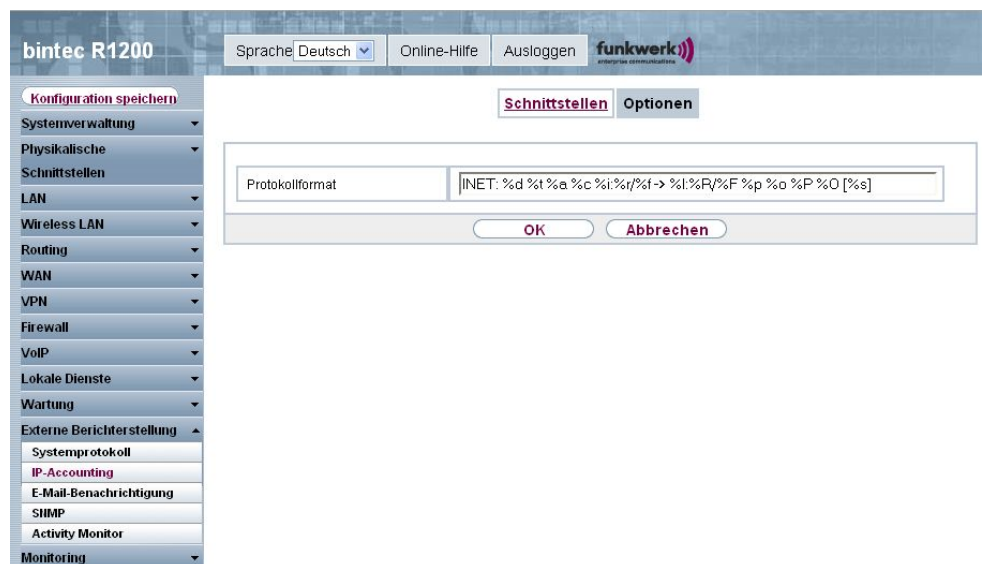


Abb. 201: Externe Berichterstellung -> IP-Accounting -> Optionen

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

Feld	Beschreibung
%c	Protokoll
%i	Quell-IP-Adresse
%r	Quellport
%f	Quell-Schnittstellen-Index
%l	Ziel-IP-Adresse
%R	Zielport
%F	Ziel-Schnittstellen-Index
%p	Ausgegangene Pakete
%o	Ausgegangene Oktetts
%P	Eingegangene Pakete
%O	Eingegangene Oktetts
%s	Laufende Nummer der Gebührenerfassungsmeldung
%%	%

Standardmäßig ist im Feld **Protokollformat** die folgende Formatanweisung eingetragen:

```
INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]
```

16.3 E-Mail-Benachrichtigung

Bisher war es schon möglich Syslog Meldungen vom Router an einen beliebigen Syslog-Host übertragen zu lassen. Mit der E-Mail-Benachrichtigung werden dem Administrator je nach Konfiguration Emails gesendet, sobald relevante Syslog Meldungen auftreten.

16.3.1 E-Mail-Benachrichtigungs-Server

Das Menü **E-Mail-Benachrichtigungs-Server** besteht aus folgenden Feldern:

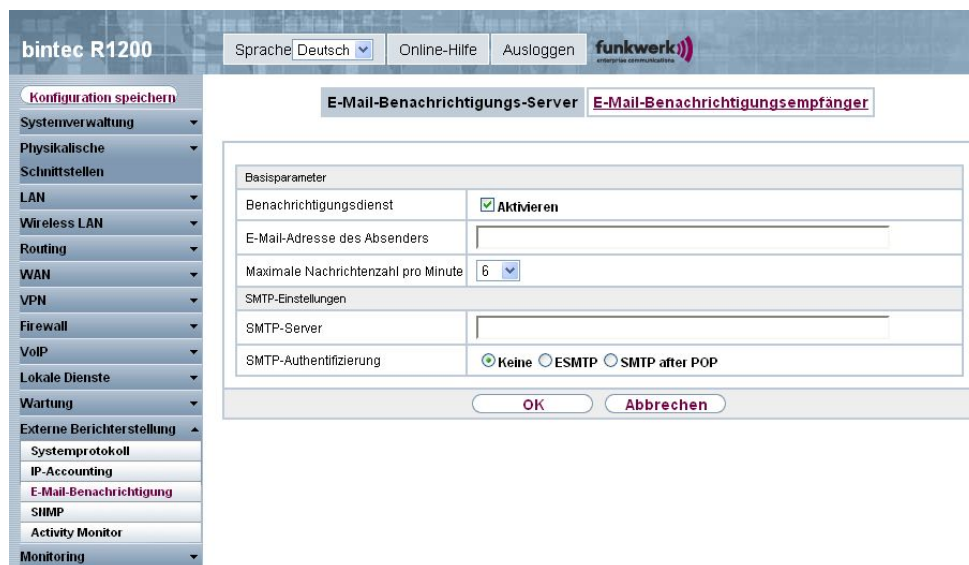


Abb. 202: Externe Berichterstellung -> E-Mail-Benachrichtigung -> E-Mail-Benachrichtigungs-Server

Das Menü **Externe Berichterstellung -> E-Mail-Benachrichtigung -> E-Mail-Benachrichtigungs-Server** besteht aus folgenden Feldern:

Felder im Menü E-Mail-Benachrichtigungs-Server Basisparameter

Feld	Beschreibung
Benachrichtigungsdienst	Aktivieren bzw. deaktivieren Sie die Funktion.
E-Mail-Adresse des Absenders	Geben Sie die Mailadresse ein, die in das Absenderfeld der Email eingetragen werden soll.
Maximale Nachrichtenzahl 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-Benachrichtigungs-Server SMTP-Einstellungen

Feld	Beschreibung
SMTP-Server	Geben Sie die Adresse (IP-Adresse oder gültiger DNS-Name) des Mailserver ein, der zum Versenden der Mails verwendet werden soll.

Feld	Beschreibung
	Die Eingabe ist auf 40 Zeichen begrenzt.
SMTP-Authentifizierung	<p>Leiten Sie die ankommenden Emails weiter.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Keine</i> (Standardwert): Die Emails werden nicht weitergeleitet. • <i>ESMTP</i>: Die Emails werden über SMTP zum Ziel weitergeleitet. • <i>SMTP after POP</i>: Die Emails werden mit dem POP von Provider abgeholt und über SMTP zum Ziel weitergeleitet.
Benutzername	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie den Name des Benutzers an.</p>
Passwort	<p>Nur wenn SMTP-Authentifizierung = <i>ESMTP</i> oder <i>SMTP after POP</i></p> <p>Geben Sie das Passwort des 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> <p>Damit der Mailserver Anfragen per POP3 beantworten kann, muss eine entsprechende POP3-Server-Software installiert sein.</p>
POP3-Timeout	<p>Nur wenn SMTP-Authentifizierung = <i>SMTP after POP</i></p> <p>Geben Sie ein, wie lange der Router nach einem entsprechenden Ereignis maximal warten darf, bevor das Versenden der Alert Mail erzwungen wird.</p> <p>Standardwert ist 600 Sekunden.</p>

16.3.2 E-Mail-Benachrichtigungsempfänger

Im Menü **E-Mail-Benachrichtigungsempfänger** wird eine Liste der Syslog Meldungen angezeigt.

16.3.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weiter E-Mail-Benachrichtigungsempfänger anzulegen.

The screenshot shows the 'bintec R1200' web interface. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Externe Berichterstellung', with 'E-Mail-Benachrichtigung' selected. The main content area is titled 'E-Mail-Benachrichtigungs-Server' and 'E-Mail-Benachrichtigungsempfänger'. The configuration form is titled 'E-Mail-Benachrichtigungsempfänger hinzufügen/bearbeiten' and contains the following fields:

- Empfänger: Text input field.
- Enthaltene Zeichenfolge: Text input field with a '(Wildcards)' label.
- Schweregrad: Dropdown menu set to 'Notfall'.
- Timeout für Nachrichten: Text input field with '60'.
- Anzahl Nachrichten: Text input field with '1'.
- Nachrichtenkomprimierung: Checkmark and 'Aktivieren' label.

Below the form is a 'Überwachte Subsysteme' section with a 'Subsystem' dropdown and a 'Hinzufügen' button. At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 203: Externe Berichterstellung -> E-Mail-Benachrichtigung -> E-Mail-Benachrichtigungsempfänger

Das Menü **Externe Berichterstellung -> E-Mail-Benachrichtigung -> E-Mail-Benachrichtigungsempfänger** besteht aus folgenden Feldern:

Felder im Menü E-Mail-Benachrichtigungsempfänger E-Mail-Benachrichtigungsempfänger hinzufügen/bearbeiten

Feld	Beschreibung
Empfänger	Geben Sie die Email-Adresse des Empfängers ein. Die Eingabe ist auf 40 Zeichen begrenzt.
Enthaltene Zeichenfolge	<p>Hier müssen Sie 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, ge-</p>

Feld	Beschreibung
	ben Sie lediglich "*" ein.
Schweregrad	<p>Wählen Sie den Schweregrad aus, auf dem der im Feld Enthaltene Zeichenfolge konfigurierte String vorkommen muss, damit eine E-Mail-Benachrichtigung ausgelöst wird.</p> <p>Mögliche Werte:</p> <p><i>Notfall</i> (Standardwert), <i>Alarm</i>, <i>Kritisch</i>, <i>Fehler</i>, <i>Warnung</i>, <i>Benachrichtigung</i>, <i>Informationen</i>, <i>Debug</i></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 dem Timeout.</p>
Anzahl Nachrichten	<p>Geben Sie die Anzahl an Syslog-Meldungen ein, die erreicht sein muss, ehe eine Benachrichtigungsmails 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, Defaultwert ist 0.</p>
Nachrichtenkomprimierung	<p>Wählen Sie aus, ob der Text des Benachrichtigungsmails verkürzt werden soll. Die Mail enthält dann die Syslog-Meldungen 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>

Felder im Menü E-Mail-Benachrichtigungsempfänger Überwachte Subsysteme

Feld	Beschreibung
Subsystem	<p>Wählen Sie die Subsysteme aus, die überwacht werden sollen.</p> <p>Fügen Sie mit Hinzufügen neue Subsysteme hinzu.</p>

16.4 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

16.4.1 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.

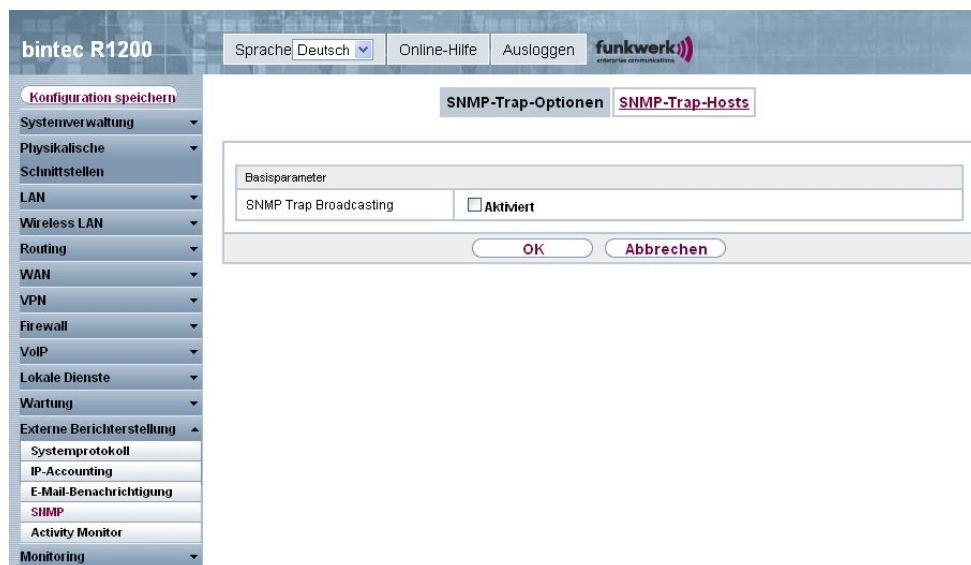


Abb. 204: Externe Berichterstellung -> SNMP -> SNMP-Trap-Optionen

Das Menü **Externe Berichterstellung -> SNMP -> SNMP-Trap-Optionen** besteht aus folgenden Feldern:

Felder im Menü SNMP-Trap-Optionen 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>Mögliche ist jeder ganzzahlige Wert.</p> <p>Standardwert ist 162 .</p>
SNMP-Trap-Community	<p>Nur wenn SNMP Trap Broadcasting aktiviert ist.</p>

Feld	Beschreibung
	<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 hier eine Zeichenkette mit 0 bis 255 Zeichen.</p> <p>Standardwert ist <code>snmp-Trap</code>.</p>

16.4.2 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.

16.4.2.1 Neu

Wählen Sie die Schaltfläche **Neu**, um weitere SNMP-Trap-Hosts einzurichten.

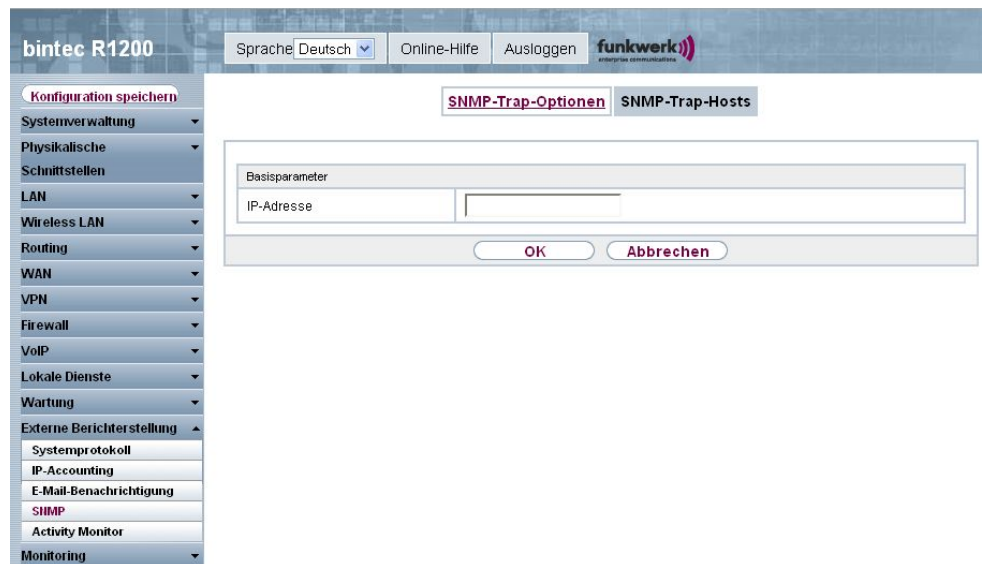


Abb. 205: Externe Berichterstellung -> SNMP -> SNMP-Trap-Hosts -> Neu

Das Menü **Externe Berichterstellung** -> **SNMP** -> **SNMP-Trap-Hosts** -> **Neu** besteht aus folgenden Feldern:

Felder im Menü SNMP-Trap-Hosts Basisparameter

Feld	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse des SNMP-Trap-Hosts ein.

16.5 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 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 (siehe **BRICKware for Windows**)

16.5.1 Optionen

The screenshot shows the configuration interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. A left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', and 'Externe Berichterstellung'. Under 'Externe Berichterstellung', 'Activity Monitor' is selected. The main content area is titled 'Optionen' and contains a 'Basisparameter' table with the following fields:

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	••••••••

At the bottom of the form are 'OK' and 'Abbrechen' buttons.

Abb. 206: Externe Berichterstellung -> Activity Monitor -> Optionen

Das Menü **Externe Berichterstellung -> Activity Monitor -> Optionen** besteht aus folgenden Feldern:

Felder im Menü Optionen Basisparameter

Feld	Beschreibung
Überwachte Schnittstellen	<p>Wählen Sie die Art der Informationen, die mit den UDP-Paketen zur Windows-Anwendung geschickt werden sollen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> • <i>Aus</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>

Feld	Beschreibung
	<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	Geben Sie das Aktualisierungsintervall (in Sekunden) ein. Mögliche Werte sind <i>0</i> bis <i>60</i> Standardwert ist <i>5</i> .
UDP-Zielport	Geben Sie die Port-Nummer für die Windows-Anwendung Activity Monitor ein. Standardwert ist <i>2107</i> (registriert durch IANA - Internet Assigned Numbers Authority).
Passwort	Geben Sie das Passwort für den Activity Monitor ein.


Kapitel 17 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.

17.1 Internes Protokoll

17.1.1 Systemmeldungen

Im Menü **Monitoring** -> **Internes Protokoll** -> **Systemmeldungen** wird eine Liste aller intern gespeicherter System-Meldungen angezeigt. Oberhalb der Tabelle finden Sie die konfigurierte **Maximale Anzahl der Syslog-Protokolleinträge** und das konfigurierte **Maximales Nachrichtenlevel von Systemprotokolleinträgen**. Diese Werte können im Menü **Systemverwaltung** -> **Globale Einstellungen** -> **System** verändert werden.

bintec R1200 Sprache **Deutsch** Online-Hilfe Ausloggen 

Konfiguration speichern

Systemverwaltung

- Systemverwaltung
- Physikalische
- Schnittstellen
 - LAN
 - Wireless LAN
 - Routing
 - WAN
 - VPN
 - Firewall
 - VoIP
 - Lokale Dienste
 - Wartung
 - Externe Berichterstellung
 - Monitoring**
 - Internes Protokoll**
 - IPSec
 - ISDN Modem
 - Schnittstellen
 - WLAN

Systemmeldungen

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

Maximale Anzahl der Syslog-Protokolleinträge

Maximales Nachrichtenlevel von Systemprotokolleinträgen **Informationen**

Ansicht pro Seite Filtern in

#	Datum	Zeit	Level	Subsystem	Nachricht
1	2005-01-25	00:39:56	Informationen	INET	APDISCD: 2 access points found on interface 1000
2	2005-01-25	00:39:46	Informationen	INET	APDISCD: discovery initiated on interface 1000
3	2005-01-25	00:23:50	Fehler	TTY	UMTS Ctl umtsctl_open(): can't open umts device!
4	2005-01-25	00:23:49	Informationen	USB	usb6-0-2: Sierra Wireless, Incorporated AirCard, rev 1.100.02
5	2005-01-25	00:23:49	Informationen	IPSec	init: starting...
6	2005-01-25	00:23:49	Informationen	IPSec	BinTec ipsecd version 3.0 Copyright (c) 1996-2008 by Funkwerk Enterprise Communications GmbH
7	2005-01-25	00:23:49	Informationen	IPSec	init: running
8	2005-01-25	00:23:49	Fehler	TTY	Modem answer to «AT+CPIN?» is 'SIM busy'
9	2005-01-25	00:23:49	Informationen	INET	ssh: pid 56 - listening on 0.0.0.0 port 22.
10	2005-01-25	00:23:48	Informationen	Konfiguration	system r1200 started at Tue Jan 25 0:23:48 2005
11	2005-01-25	00:23:45	Debug	USB	usb_create_dev: new unit addr 1, rev 100, class 9
12	2005-01-25	00:23:45	Debug	USB	subclass 0, proto 0, maxpkt 64, speed 2
13	2005-01-25	00:23:45	Debug	USB	usb_create_dev: setting device address=1
14	2005-01-25	00:23:45	Informationen	USB	usb6-0-1: NEC OHCI root hub, class 9/0, rev 1.00/1.00
15	2005-01-25	00:23:45	Informationen	USB	usb6-0-1: HUB with 1 port (1 removable), self-powered
16	2005-01-25	00:23:45	Debug	USB	usb_trap: rowno 1 - ev 0xffff
17	2005-01-25	00:23:45	Debug	USB	USB6-1-1: port=0 depth=0 (full-speed)
18	2005-01-25	00:23:45	Debug	USB	usb_create_dev: new unit addr 1, rev 100, class 9
19	2005-01-25	00:23:45	Debug	USB	subclass 0, proto 0, maxpkt 64, speed 2
20	2005-01-25	00:23:45	Debug	USB	usb_create_dev: setting device address=1

Seite: 1, Objekte: 1 - 20, Summe der Objekte: 26

Abb. 207: Monitoring -> Internes Protokoll -> Systemmeldungen

Werte in der Liste Systemmeldungen

Feld	Beschreibung
#	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.

17.2 IPSec

17.2.1 IPSec-Tunnel

Im Menü **Monitoring** -> **IPSec** -> **IPSec-Tunnel** wird eine Liste aller konfigurierter IPSec-Tunnel angezeigt.


The screenshot shows the web interface for a bintec R1200 device. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstattung', and 'Monitoring'. Under 'Monitoring', 'IPSec' is selected. The main content area displays the 'IPSec-Tunnel' configuration page. At the top, there are buttons for 'IPSec-Tunnel' and 'IPSec-Statistiken'. Below that, there is a section for 'Automatisches Aktualisierungsintervall' set to 300 Sekunden, with an 'Übernehmen' button. A table below shows the list of IPSec tunnels with columns: '#', 'Beschreibung', 'Entfernte IP-Adresse', 'Entfernte Netzwerke', 'Sicherheitsalgorithmus', 'Status', and 'Aktion'. The 'Status' column contains up and down arrows, and the 'Aktion' column contains a 'Los' button.

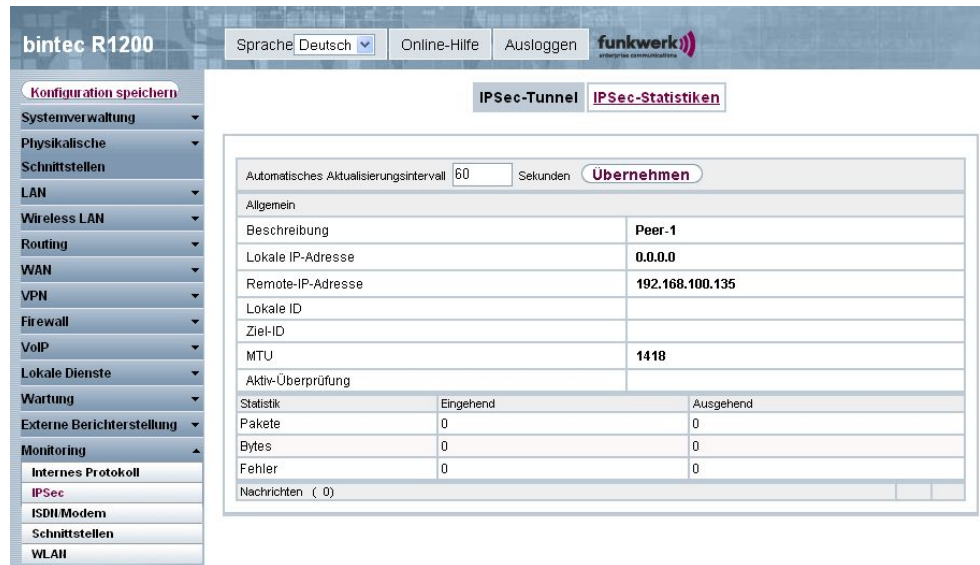
Abb. 208: **Monitoring** -> **IPSec** -> **IPSec-Tunnel**

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
#	Zeigt die laufende Nummer der IPSec-Verbindung an.
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 Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der IPSec-Verbindung geändert.

Durch Drücken der -Schaltfläche wird eine ausführliche Statistik zu der jeweiligen IPSec-Verbindung angezeigt.



The screenshot shows the bintec R1200 web interface. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. Under 'Monitoring', 'IPSec' is selected. The main content area shows the 'IPSec-Tunnel' configuration for 'Peer-1'. At the top, there is a language dropdown set to 'Deutsch', 'Online-Hilfe', and 'Ausloggen' buttons. Below that, there are tabs for 'IPSec-Tunnel' and 'IPSec-Statistiken'. A search icon is visible. The configuration table includes fields for 'Automatisches Aktualisierungsintervall' (60 Sekunden), 'Beschreibung' (Peer-1), 'Lokale IP-Adresse' (0.0.0.0), 'Remote-IP-Adresse' (192.168.100.135), 'Lokale ID', 'Ziel-ID', and 'MTU' (1418). A 'Statistik' table shows 0 packets, bytes, and errors for both incoming and outgoing traffic. A 'Nachrichten' section shows 0 messages.

Abb. 209: Monitoring -> IPSec -> IPSec-Tunnel -> 

Werte in der Liste IPSec-Tunnel

Feld	Beschreibung
Beschreibung	Hier wird die Beschreibung des Peers angezeigt.
Lokale IP-Adresse	Hier wird die WAN-IP-Adresse Ihres Geräts angezeigt.
Ziel-IP-Adresse	Hier wird die WAN-IP-Adresse des Verbindungspartners angezeigt.
Lokale ID	Hier wird die ID Ihres Geräts für diese IPSec-Verbindung angezeigt.
Ziel-ID	Hier wird die ID des Peers angezeigt.
Aushandlungsmodus	Hier wird der Aushandlungsmodus angezeigt.
Authentifizierungsmethode	Hier wird die Authentifizierungsmethode angezeigt.
MTU	Hier wird die aktuelle MTU (Maximum Transfer Unit) angezeigt.
Aktiv-Überprüfung	Hier wird die Aktiv-Überprüfungs-Methode angezeigt.
Statistik (Pakete, Bytes, Fehler)	Hier werden die Parameter der IKE (Phase 1) SAs angezeigt.
Nachrichten	Hier werden die Systemmeldungen zu diesem IPSec-Tunnel

Feld	Beschreibung
	angezeigt.

17.2.2 IPSec-Statistiken

Im Menü **Monitoring** -> **IPSec** -> **IPSec-Statistiken** werden statistische Werte zu allen IPSec-Verbindungen angezeigt.

The screenshot shows the bintec R1200 web interface. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar shows a menu with 'Monitoring' expanded to 'IPSec'. The main content area displays the 'IPSec-Statistiken' page. At the top of this page, there is a section for 'Automatisches Aktualisierungsintervall' set to '300 Sekunden' with a 'Übernehmen' button. Below this is a table for 'Lizenzen' showing 'In Verwendung' (0) and 'Maximal' (110). The 'IPSec-Tunnel' section shows a table with columns for 'Peers', 'Aktiv', 'Aktivieren', 'Blockiert', 'Ruhend', and 'Konfiguriert', with all values being 0. The 'SA's' section shows a table with columns for 'Hergestellt' and 'Gesamt', with values 0 for both. The 'Paketstatistiken' section shows a table with columns for 'Eingehend' and 'Ausgehend', with values 0 for both. The 'Gesamt' section shows a table with columns for 'Weitergeleitet', 'Verworfen', 'Verschlüsselt', and 'Fehler', with values 0 for all.

Abb. 210: **Monitoring** -> **IPSec** -> **IPSec-Statistiken**

Das Menü **Monitoring** -> **IPSec** -> **IPSec-Statistiken** besteht aus folgenden Feldern:

Felder im Menü IPSec-Statistiken Lizenzen

Feld	Beschreibung
IPSec-Tunnel	Zeigt die Anzahl der aktuell genutzten IPSec-Lizenzen (In Verwendung) und die Anzahl der maximal verwendbaren Lizenzen (Maximal) an.

Feld im Menü IPSec-Statistiken Peers

Feld	Beschreibung
Status	Zeigt die Anzahl der IPSec-Verbindungen gezählt nach Ihrem aktuellen Status an. <ul style="list-style-type: none"> • Aktiv: Aktuell aktive IPSec-Verbindungen.

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

17.3 ISDN/Modem

17.3.1 Aktuelle Anrufe

Im Menü **Monitoring** -> **ISDN/Modem** -> **Aktuelle Anrufe** wird eine Liste der bestehenden ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

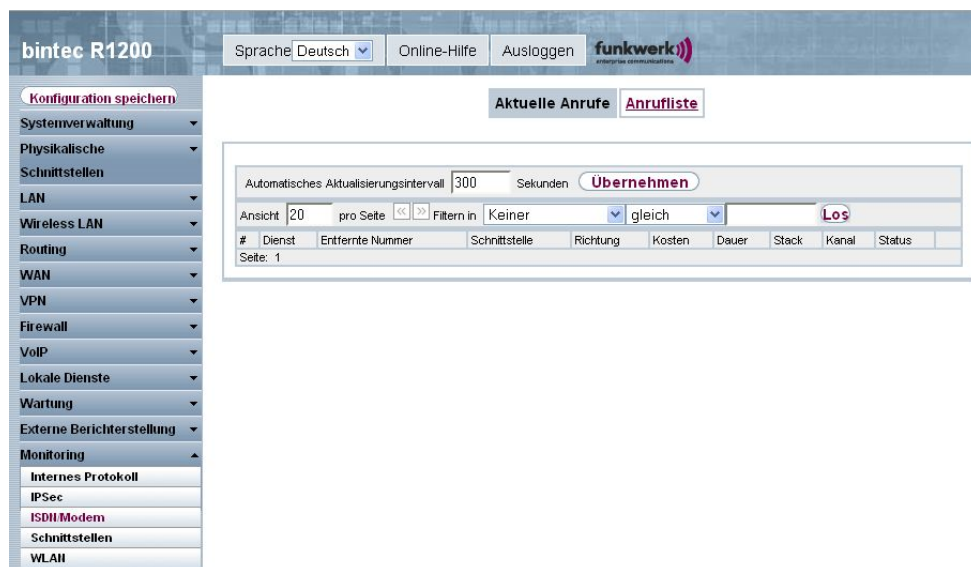


Abb. 211: Monitoring -> ISDN/Modem -> Aktuelle Anrufe

Werte in der Liste Aktuelle Anrufe

Feld	Beschreibung
#	Zeigt die laufende Nummer des ISDN-Verbindungseintrags an.
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden ist: <i>PPP, IPSEC, X.25, POTS.</i>
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: <i>Eingehend, Ausgehend.</i>
Kosten	Zeigt die Kosten der laufenden Verbindung an.
Dauer	Zeigt die Dauer der laufenden Verbindung an.
Stack	Zeigt den zugehörigen ISDN-Port (STACK) an.
Kanal	Zeigt die Nummer des ISDN-B-Kanals an.
Status	Zeigt den Status der Verbindung an: <i>null, c-initiated, ovl-send, oc-procd, c-deliverd, c-present, c-recvd, ic-procd, aktiv, discon-req, discon-ind, suspd-req, resum-req, ovl-recv.</i>

17.3.2 Anrufliste

Im Menü **Monitoring** -> **ISDN/Modem** -> **Anrufliste** wird eine Liste der letzten 20 seit dem letzten Systemstart abgeschlossenen ISDN-Verbindungen (eingehend und ausgehend) angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. Under 'Monitoring', 'ISDN/Modem' is selected. The main content area displays the 'Anrufliste' (call log) with a table of records. The table has columns: #, Dienst, Entfernte Nummer, Schnittstelle, Richtung, Kosten, Startzeit, and Dauer. The current view shows 20 records per page, filtered by 'Keiner'. There are also buttons for 'Aktuelle Anrufe' and 'Anrufliste'.

Abb. 212: Monitoring -> ISDN/Modem -> Anrufliste

Werte in der Liste Anrufliste

Feld	Beschreibung
#	Zeigt die laufende Nummer der ISDN-Verbindung an.
Dienst	Zeigt den Dienst an, zu bzw. von dem der Ruf verbunden war: <i>PPP, IPSEC, X.25, POTS.</i>
Entfernte Nummer	Zeigt die Rufnummer, die gewählt wurde (bei ausgehenden Rufen) bzw. von der aus angerufen wurde (bei eingehenden Rufen).
Schnittstelle	Zeigt Zusatzinformationen für PPP-Verbindungen an.
Richtung	Zeigt die Senderichtung an: <i>Eingehend, Ausgehend.</i>
Kosten	Zeigt die Kosten der Verbindung an.
Startzeit	Zeigt die Uhrzeit an, zu welcher der Ruf aus- bzw. einging.
Dauer	Zeigt die Dauer der Verbindung an.

17.4 Schnittstellen

17.4.1 Statistik

Im Menü **Monitoring** -> **Schnittstellen** -> **Statistik** werden die aktuellen Werte und Aktivitäten aller Geräte-Schnittstellen angezeigt.

The screenshot shows the 'bintec R1200' web interface. The left sidebar contains a navigation menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. Under 'Monitoring', 'Schnittstellen' is selected. The main content area is titled 'Statistik' and features a table with columns for '#', 'Beschreibung', 'Typ', 'Tx-Pakete', 'Tx-Bytes', 'Tx-Fehler', 'Rx-Pakete', 'Rx-Bytes', 'Rx-Fehler', 'Status', 'Nicht geändert seit', and 'Aktion'. The table lists two interfaces: 'en1-0' (Ethernet) and 'en1-4' (Ethernet). The 'en1-0' interface shows 529 Tx-Pakete, 431.71K Tx-Bytes, 0 Tx-Fehler, 417 Rx-Pakete, 65.72K Rx-Bytes, and 0 Rx-Fehler. The 'en1-4' interface shows 0 Tx-Pakete, 0 Tx-Bytes, 0 Tx-Fehler, 0 Rx-Pakete, 0 Rx-Bytes, and 0 Rx-Fehler. The 'Status' column shows a green circle with a plus sign for 'en1-0' and a red circle with a minus sign for 'en1-4'. The 'Aktion' column contains icons for status change (up/down arrows) and detail view (magnifying glass).

Abb. 213: Monitoring -> Schnittstellen -> Statistik

Durch Drücken der -Schaltfläche oder der -Schaltfläche in der Spalte **Aktion** wird der Status der Schnittstelle geändert. Über die -Schaltfläche können Sie die statistischen Daten für die einzelnen Schnittstellen im Detail anzeigen lassen.

Werte in der Liste Statistik

Feld	Beschreibung
#	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.

Feld	Beschreibung
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, für wie lang sich der Betriebszustand der Schnittstelle nicht geändert hat.
Aktion	Bietet die Möglichkeit den Status der Schnittstelle wie angezeigt zu ändern.

17.5 WLAN

17.5.1 WLAN1

Im Menü **Monitoring** -> **WLAN** -> **WLAN1** werden die aktuellen Werte und Aktivitäten der ersten WLAN-Schnittstelle angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The main content area displays the 'WLAN1' monitoring page. At the top, there are buttons for 'WLAN1', 'VSS', and 'Client Links'. Below this, there is a section for 'Automatisches Aktualisierungsintervall' set to 300 Sekunden, with an 'Übernehmen' button. The main data is presented in a table titled 'WLAN1 Statistik' with three columns: 'Mbit/s', 'Tx-Pakete', and 'Rx-Pakete'. The table lists various data rates from 54 Mbit/s down to 1 Mbit/s, with corresponding Tx and Rx packet counts. The 'Gesamt' row shows 0 for all three metrics. At the bottom of the table, there is an 'Erweitert' button. The left sidebar contains a navigation menu with options like 'Konfiguration speichern', 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', 'Monitoring', 'Internes Protokoll', 'IPSec', 'ISDI Modem', 'Schnittstellen', and 'WLAN'. The top navigation bar shows 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo.

Abb. 214: Monitoring -> WLAN -> WLAN1

Werte in der Liste WLAN1

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

Feld	Beschreibung
	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.

The screenshot shows the bintec R1200 web interface. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The Monitoring section is expanded to show WLAN. The main content area displays 'WLAN1' statistics. At the top, there are buttons for 'WLAN1', 'VSS', and 'Client Links'. Below this, there is a table with 12 rows of statistics. The table has columns for '#', 'Beschreibung', and 'Wert'. The values in the 'Wert' column are all 0. There is a 'Übernehmen' button above the table and a 'Zurück' button below it.

#	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. 215: Monitoring -> WLAN -> WLAN1 -> Erweitert

Werte in der Liste Erweitert

Feld	Beschreibung
#	Zeigt die laufende Nummer des Listeneintrags an.
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 versandte 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	Zeigt die Anzahl der erfolgreich empfangenen MSDUs an, die

Beschreibung	Bedeutung
Multicast-MSDUs	mit einer Multicast-Adresse versandt wurden.
Unicast MPDUs erfolgreich empfangen	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-Übertragung ohne ACK	Zeigt die Anzahl der gesendeten Frames an, für die kein Acknowledgement-Frame empfangen wurde.
Doppelt empfangene MSDUs	Zeigt die Anzahl von doppelt empfangenen MSDUs an.
CTS Frames als Antwort auf RTS empfangen	Zeigt die Anzahl der empfangenen CTS (Clear to send)-Frames an, die als Antwort auf RTS (Request to send) empfangen wurden.
Nicht entschlüsselbare MPDU 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 Empfangene Pakete	Zeigt die Anzahl der Frames an, die unvollständig oder fehlerhaft empfangen wurden.

17.5.2 VSS

Im Menü **Monitoring** -> **WLAN** -> **VSS** werden die aktuellen Werte und Aktivitäten der konfigurierten Drahtlosnetzwerke angezeigt.




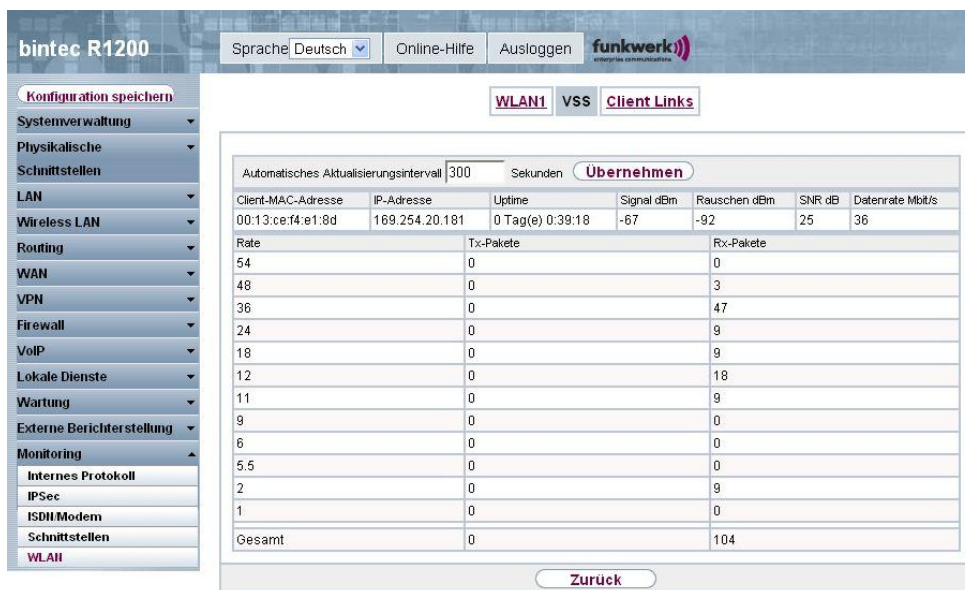
Abb. 216: Monitoring -> WLAN -> VSS

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	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
Datenrate Mbit/s	<p>Zeigt die aktuelle Übertragungsrate von diesem Client empfangener 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.



The screenshot shows the bintec R1200 web interface. The left sidebar contains a navigation menu with categories like Systemverwaltung, Physikalische, Schnittstellen, LAN, Wireless LAN, Routing, WAN, VPN, Firewall, VoIP, Lokale Dienste, Wartung, Externe Berichterstellung, and Monitoring. The Monitoring section is expanded, showing options for Internes Protokoll, IPSec, ISDN/Modem, Schnittstellen, and WLAN. The main content area displays the VSS (Verbundener Client) monitoring page. At the top, there are buttons for 'WLAN1', 'VSS', and 'Client Links'. Below this, there is a section for 'Automatisches Aktualisierungsintervall' set to 300 Sekunden, with an 'Übernehmen' button. The main data table shows the following information:

Client-MAC-Adresse	IP-Adresse	Uptime	Signal dBm	Rauschen dBm	SNR dB	Datenrate Mbit/s
00:13:ce:f4:e1:8d	169.254.20.181	0 Tag(e) 0:39:18	-67	-92	25	36
Rate		Tx-Pakete	Rx-Pakete			
54	0	0	0			
48	0	0	3			
36	0	0	47			
24	0	0	9			
18	0	0	9			
12	0	0	18			
9	0	0	9			
6	0	0	0			
5,5	0	0	0			
2	0	0	9			
1	0	0	0			
Gesamt	0	0	104			

At the bottom of the page, there is a 'Zurück' button.

Abb. 217: **Monitoring -> WLAN -> VSS -><Verbundener Client>->** 

Werte in der Liste VSS <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	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	Zeigt die Empfangsstärke des Rauschens in dBm an.
SNR dB	Signal to Noise Ratio (Signal-Rausch-Abstand) in dB stellt einen Indikator für die Qualität der Verbindung im Funk dar. Werte: <ul style="list-style-type: none"> > 25 dB exzellent 15 - 25 dB gut 2 - 15 dB grenzwertig 0 - 2 dB schlecht.

Feld	Beschreibung
Datenrate Mbit/s	Zeigt die aktuelle Übertragungsrates von diesem Client empfangener Daten in Mbit/s an. Folgende Übertragungsrates sind möglich: IEEE 802.11b: 11, 5.5, 2 und 1 Mbit/s; IEEE 802.11g/a: 54,48,36,24,18,12,9,6 Mbit/s. 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 diesem 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.

17.5.3 WDS

Im Menü **Monitoring** -> **WLAN** -> **WDS** werden die aktuellen Werte und Aktivitäten der konfigurierten WDS-Links angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar menu is expanded to 'Monitoring', with 'WLAN' selected. The main content area has tabs for 'WLAN', 'VSS', 'WDS', and 'Client Links'. The 'WDS' tab is active, displaying an 'Automatisches Aktualisierungsintervall' of 60 seconds and an 'Übernehmen' button. Below this is a 'WDS-Tabelle' with the following data:

WDS-Beschreibung	Entfernte MAC	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm	Rauschen dBm	Datenrate Mbit/s
wds1-0	00:00:00:00:00:00	0d 1h 50m 10s	0	0	0	0	0

Abb. 218: 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.

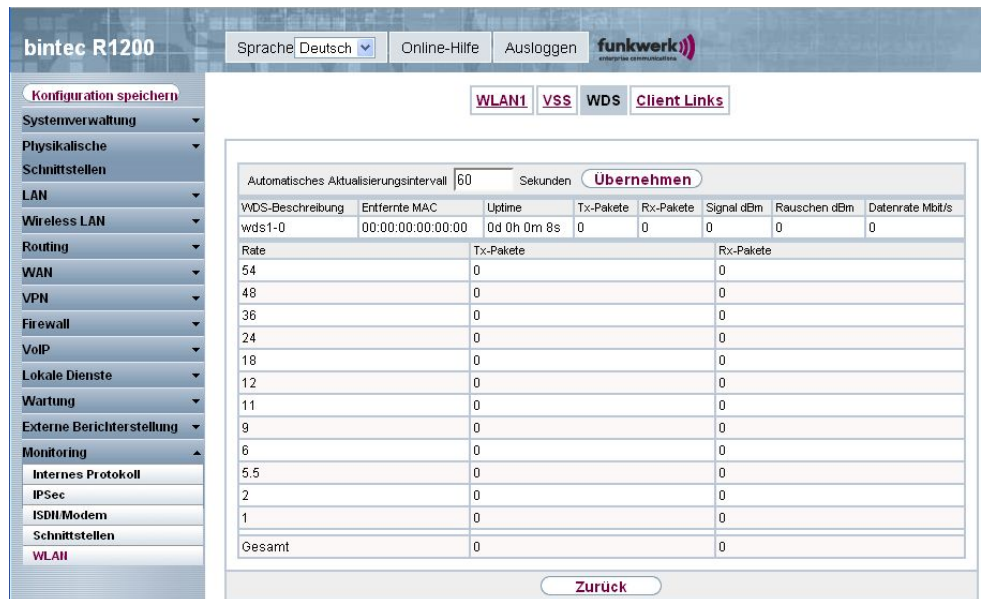
Feld	Beschreibung
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige WDS-Link aktiv ist.
Tx-Pakete	Zeigt die Gesamtzahl der gesendeten Pakete an.
Rx-Pakete	Zeigt die Gesamtzahl der erhaltenen Pakete an.
Signal dBm	Zeigt die Empfangsstärke des Signals in dBm an.
Rauschen dBm	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 **funkwerk**-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.



bintec R1200 Sprache **Deutsch** Online-Hilfe Ausloggen **funkwerk** enterprise communications

Konfiguration speichern

Systemverwaltung

Physikalische Schnittstellen

LAN

Wireless LAN

Routing

WAN

VPN

Firewall

VoIP

Lokale Dienste

Wartung

Externe Berichterstellung

Monitoring

Internes Protokoll

IPSec

ISDI Modem

Schnittstellen


WLAN

WLAN VSS WDS Client Links

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

WDS-Beschreibung	Entfernte MAC	Uptime	Tx-Pakete	Rx-Pakete	Signal dBm	Rauschen dBm	Datenrate Mbit/s
wds1-0	00:00:00:00:00:00	0d 0h 0m 8s	0	0	0	0	0
Rate			Tx-Pakete	Rx-Pakete			
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			
Gesamt			0	0			

Zurück

Abb. 219: 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	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.
Rate	Zeigt für jede der angegebenen Datenraten die Werte für Tx-Pakete und Rx-Pakete einzeln an.

17.5.4 Client Links

Im Menü **Monitoring** -> **WLAN** -> **Client Links** werden die aktuellen Werte und Aktivitäten der Client Links angezeigt.

The screenshot shows the web interface for a bintec R1200 device. The top navigation bar includes 'Sprache: Deutsch', 'Online-Hilfe', 'Ausloggen', and the 'funkwerk' logo. The left sidebar contains a menu with categories like 'Systemverwaltung', 'Physikalische Schnittstellen', 'LAN', 'Wireless LAN', 'Routing', 'WAN', 'VPN', 'Firewall', 'VoIP', 'Lokale Dienste', 'Wartung', 'Externe Berichterstellung', and 'Monitoring'. The 'Monitoring' section is expanded to show 'Internes Protokoll', 'IPSec', 'ISDN Modem', 'Schnittstellen', and 'WLAN'. The 'WLAN' section is selected, and the 'Client Links' sub-menu is active. The main content area shows a table with columns for 'Client Links', 'Beschreibung des Client Links', 'AP-MAC-Adresse', 'Uptime', 'Tx-Pakete', 'Rx-Pakete', 'Signal dBm', 'Rauschen dBm', and 'Datenrate Mbit/s'. The table lists one client link: 'WLAN1 ()' with a sub-entry 'sta1-0' having a MAC address of '00:a0:f9:09:68:b7', an uptime of '0d 0h 0m 7s', 0 Tx-Pakete, 1.85k Rx-Pakete, a signal strength of -70 dBm, a noise level of -96 dBm, and a data rate of 2 Mbit/s. There is an 'Übernehmen' button and a refresh icon next to the table.

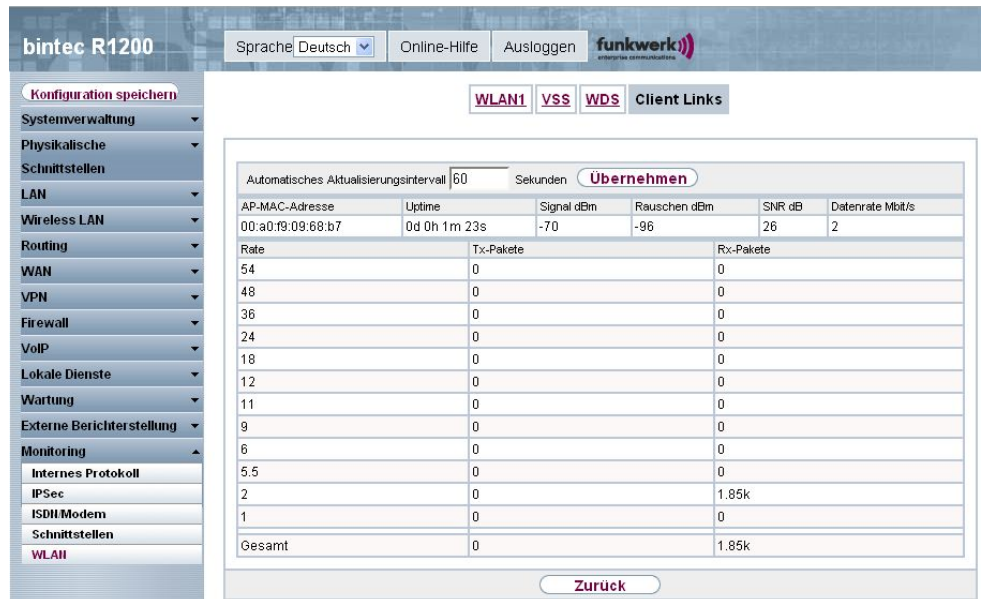
Abb. 220: Monitoring -> WLAN -> Client Links

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.
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.



bintec R1200 Sprache: Deutsch Online-Hilfe Ausloggen **funkwerk**

Konfiguration speichern

Systemverwaltung ▼
 Physikalische Schnittstellen
 LAN ▼
 Wireless LAN ▼
 Routing ▼
 WAN ▼
 VPN ▼
 Firewall ▼
 VoIP ▼
 Lokale Dienste ▼
 Wartung ▼
 Externe Berichterstellung ▼
 Monitoring ▲
 Internes Protokoll
 IPSec
 ISDN Modem
 Schnittstellen
 WLAN

WLAN1 **VSS** **WDS** **Client Links**

Automatisches Aktualisierungsintervall Sekunden **Übernehmen**

AP-MAC-Adresse	Uptime	Signal dBm	Rauschen dBm	SNR dB	Datenrate Mbit/s
00:a0:f9:09:68:b7	0d 0h 1m 23s	-70	-96	26	2
Rate	Tx-Pakete	Rx-Pakete			
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	1.85k			
1	0	0			
Gesamt	0	1.85k			

Zurück

Abb. 221: Monitoring -> WLAN -> Client Links -> 

Werte in der Liste Client Links

Feld	Beschreibung
AP-MAC-Adresse	Zeigt die MAC-Adresse des Client Link Partners an.
Uptime	Zeigt die Zeit in Stunden, Minuten und Sekunden an, die der jeweilige Client Link aktiv ist.
Signal dBm	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 Übertragungsrates 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.

Glossar

- Bit** Binary Digit. Kleinste Informationseinheit in der Computertechnik. Signale werden in den logischen Zuständen "0" und "1" dargestellt.
- Bündel** Die externen Anschlüsse größerer Telefonanlagen können zu Bündeln zusammengefasst werden. Bei der Einleitung eines externen Gespräches durch die Amtskennziffer oder bei automatischer Amtsholung wird beim Verbindungsaufbau ein für den Teilnehmer freigegebenes Bündel benutzt. Ist ein Teilnehmer für mehrere Bündel berechtigt, wird die Verbindung über das erste freigegebene Bündel aufgebaut. Ist ein Bündel belegt, wird das nächste freigegebene Bündel benutzt. Sind alle freigegebenen Bündel belegt, hört der Teilnehmer den Besetztton.
- Busy On Busy** Anruf auf einen besetzten Team-Teilnehmer. Hat ein Teilnehmer eines Teams den Hörer abgehoben oder führt ein Gespräch, können Sie entscheiden, ob weitere Anrufe für dieses Team signalisiert werden sollen. Die Erreichbarkeit eines Teilnehmers kann zwischen "Standard" und "Busy On Busy" (Besetzt bei Besetzt) umgeschaltet werden. In der Grundeinstellung steht sie auf Standard. Ist Busy on Busy für ein Team eingerichtet, so erhalten weitere Anrufer Besetzt signalisiert.
- DECT** Digital European Cordless Telecommunication. Europäischer Standard für schnurlose Telefone und schnurlose Telefonanlagen. Zwischen mehreren Handgeräten können kostenfreie interne Gespräche geführt werden. Ein weiterer Vorteil ist die erhöhte Abhörsicherheit (GAP).
- Dienste** Im Euro-ISDN gibt es so genannte Dienste-Indikatoren, deren Namen festgelegt sind. Teilweise haben diese nur noch historische Bedeutung. Generell sollte man für "echte" Telefonate den Dienst "Fernsprechen" auswählen. Falls diese Auswahl nicht funktioniert (Netzbetreiberabhängig), kann man es mit "speech", "audio 3k1Hz" oder "telephony 3k1Hz" weiterversuchen. Das Gleiche gilt für den Faxbetrieb. Auch hier gibt es den Sammelbegriff Fax sowie einige Spezialunterscheidungen. Rein technisch sind die Dienste Bits in einem Datenwort, die über eine Maske ausgewertet werden. Wenn man in der Maske mehrere Bits einschaltet, werden alle diese Dienste zur Weiterschaltung zugelassen. Bei einem Bit entsprechend nur der eine ausgewählte Dienst.
- Digitale Sprachübertragung** Durch die international genormte Puls Code Modulation (PCM) werden analoge Sprachsignale in einen digitalen Impulsstrom von 64

	<p>KBit/s umgewandelt. Vorteile: bessere Sprachqualität und geringere Störanfälligkeit als bei analoger Sprachübertragung.</p>
Digitale Vermittlungsstelle	<p>Ermöglicht durch computergesteuerte Koppelfelder den schnellen Verbindungsaufbau und die Aktivierung von Komfortleistungen wie Rückfragen, Anklopfen, Dreierkonferenz und Anrufweitschaltung. Seit Januar 1998 sind alle Vermittlungsstellen der T-Com digitalisiert.</p>
Direktruf	<p>Sie befinden sich außer Haus. Es gibt jedoch jemanden bei Ihnen zu Hause, der Sie im Bedarfsfall schnell und unkompliziert telefonisch erreichen soll (z. B. Kinder oder Großeltern). Da Sie für ein oder mehrere Telefone die Funktion Direktruf einrichten können, braucht lediglich der Hörer des entsprechenden Telefons abgehoben zu werden. Nach fünf Sekunden wählt die Telefonanlage automatisch die festgelegte Direktrufnummer, sofern Sie vorher nicht mit der Wahl einer anderen Nummer beginnen. Sie können in der Konfiguration Direktruf bis zu 12 Zielrufnummern eintragen. Eine Direktrufnummer ist jeweils nur von einem Teilnehmer nutzbar. Möchten Sie eine eingegebene Direktrufnummer ändern, können Sie die neue Direktrufnummer einfach eingeben, ohne die alte Direktrufnummer löschen zu müssen. Sie wird bei der Übertragung der geänderten Konfiguration zur Telefonanlage automatisch überschrieben.</p>
DISA	<p>Direct Inward System Access</p>
Download	<p>Datentransfer bei Online-Verbindungen, wobei Dateien von einem PC oder einem Datennetz-Server in den eigenen PC, Telefonanlage oder Endgerät "geladen" werden, um sie dort weiterzuverwenden.</p>
Dreierkonferenz	<p>Telefonieren zu dritt. Leistungsmerkmal im T-Net, im T-ISDN und in Ihrer Telefonanlage.</p>
DSL- und ISDN-Verbindungen	<p>Der Datentransfer zwischen dem Internet und Ihrer Telefonanlage erfolgt über ISDN- oder T-DSL. Die Telefonanlage ermittelt, zu welcher Gegenstelle ein Datenpaket geschickt werden soll. Damit eine Verbindung ausgewählt und aufgebaut werden kann, müssen Parameter für alle notwendigen Verbindungen festgelegt werden. Diese Parameter sind in Listen abgelegt, deren Zusammenspiel den Aufbau der richtigen Verbindung gestattet. Beim ISDN-Zugang wird von der Telefonanlage das PPP (Point-to-Point-Protocol) benutzt, beim Zugang über T-DSL das PPPoE (Point-to-Point-Protocol over Ethernet). Der Datenverkehr auf diesen beiden Internet-Verbindungen wird von der Telefonanlage getrennt überwacht.</p>

DSL-Modem	Spezielles Modem für die Datenübertragung mit Hilfe der DSL-Zugangstechnologie.
DSL-Splitter	Eine Breitbandanschlusseinheit (BBAE), umgangssprachlich Splitter, ist ein Gerät, das die Daten beziehungsweise Frequenzen verschiedener Anwendungen, die über eine Teilnehmeranschlussleitung oder einen Abschlusspunkt Linientechnik laufen, aufteilt und über getrennte Anschlüsse zur Verfügung stellt.
Durchsage	Sie möchten Ihre Mitarbeiter oder Ihre Familienmitglieder zu einer Besprechung oder zum Essen zusammenrufen? Sie könnten jeden einzelnen anrufen oder einfach die Durchsage-Funktion nutzen. Mit nur einem Anruf erreichen Sie alle durchsageberechtigten Telefone, ohne dass Ihre Gesprächspartner den Hörer der Telefone abheben müssen.
Durchsagefunktion	Leistungsmerkmal von Telefonanlagen. An geeigneten Telefonen (z. B. Systemtelefonen) lassen sich wie bei einer Sprechanlage Durchsagen tätigen.
100Base-T	Twisted-Pair-Anschluss, Fast Ethernet. Netzwerkanschluss für 100-MBit-Netze.
10Base-2	Thin-Ethernet-Anschluss. Netzwerkanschluss für 10-MBit-Netze mit dem Steckertyp BNC. Zum Anschluss von Geräten mit BNC-Buchsen werden T-Verbindungsstücke eingesetzt.
10Base-T	Twisted-Pair-Anschluss. Netzwerkanschluss für 10-MBit-Netze mit dem Steckertyp RJ45.
1TR6	Im deutschen ISDN verwendetes D-Kanal-Protokoll. Heute gängigeres Protokoll ist das DSS1.
3DES (Triple DES)	Siehe DES.
802.11a/g	Spezifiziert Datenraten von 54, 48, 36, 24, 18, 12, 9 und 6 Mbit/s und eine Arbeitsfrequenz im Bereich von 5 GHz (bei IEEE802.11a) bzw. 2,4 GHz (bei IEEE802.11g). IEEE802.11 g kann so konfiguriert werden, dass es zusätzlich zu 11b oder 11b und 11 kompatibel betrieben wird.
802.11b/g	Einer der IEEE Standards für drahtlose Netzwerk-Hardware. Produkte, die dem gleichen IEEE Standard entsprechen, können miteinander kommunizieren, selbst wenn sie von verschiedenen Hardware-Herstellern stammen. Der IEEE802.11b Standard spezifiziert Datenraten von 1, 2, 5,5 und 11 Mbit/s, eine Arbeitsfrequenz im Be-

reich von 2,4 bis 2,4835GHz und WEP Verschlüsselung. IEEE802.11 Funknetze werden auch Wi-Fi Netzwerke genannt.

A-Teilnehmer	Der A-Teilnehmer ist der Anrufer.
A-Telefonnummer unterdrücken (CLIR)	CLIP/CLIR: Calling Line Identification Presentation/Calling Line Identification Restriction
a/b-Schnittstelle	Zum Anschluss eines analogen Endgerätes. Bei einem ISDN-Endgerät (Terminaladapter) mit a/b-Schnittstelle wird ein angeschlossenes analoges Endgerät in die Lage versetzt, die unterstützten T-ISDN Leistungsmerkmale zu nutzen.
AAA	Authentication, Authorization, Accounting
Access List	Eine Regel, die eine Anzahl von Datenpaketen definiert, die vom Gateway übertragen bzw. nicht übertragen werden sollen.
Access Point	Eine aktive Komponente eines Netzwerks, das aus funkbasierten und optional zusätzlich aus kabelgebundenen Bestandteilen besteht. An einem Access Point (AP) können sich viele WLAN-Clients (Endgeräte) einbuchen und gegenseitig über den AP Daten austauschen. Bei optionalem Anschluss eines kabelgebundenen Ethernet, werden die Signale zwischen den beiden physikalischen Medien, dem funkbasierten Interface und dem kabelgebundenen Interface überbrückt (Bridging).
Accounting	Aufzeichnen von Verbindungsdaten, wie z. B. Datum, Uhrzeit, Verbindungsdauer, Gebühreninformation und Anzahl der übertragenen Datenpakete.
Active Probing	Active Probing macht sich den Umstand zu Nutze, dass Access Points dem Standard nach auf Anfragen eines Clients antworten sollen. Clients versenden so genannte Probe-Requests auf allen Kanälen und warten auf Antworten eines in der Nähe befindlichen Access Points. Im Antwortpaket steht dann die SSID des Funk-LANs und ob WEP-Verschlüsselung verwendet wird.
Ad Hoc Netzwerk	Ein Ad Hoc Netzwerk bezeichnet eine Anzahl von Computern, die jeweils mit einem Wireless Adapter ein unabhängiges 802.11 WLAN bilden. Ad Hoc Netze arbeiten unabhängig, ohne Access Point auf einer Peer-to-Peer Basis. Der Ad Hoc Modus wird auch als IBSS Modus bezeichnet (Independent Basic Service Set) und ist in kleinsten Netzen sinnvoll, z. B. wenn zwei Notebooks ohne Access Point miteinander vernetzt werden sollen.

ADSL	Asymmetric Digital Subscriber Line
AH	Authentication Header
Alphanumerisches Display	Anzeigeeinheit z. B. beim Systemtelefon T-Concept PX722, die außer Ziffern auch Buchstaben und weitere Zeichen darstellen kann.
Amtsberechtigung	Telefonanlagen unterscheiden die folgendem "Amtsberechtigungen". Diese können in der Konfiguration für jeden Teilnehmer individuell eingerichtet werden.
Analoge Anschlüsse	Zum Anschluss analoger Endgeräte wie Telefon, Telefax und Anrufbeantworter.
Analoge Endgeräte	Endgeräte, die Sprache oder andere Informationen analog übertragen, sind z. B. Telefon, Faxgerät, Anrufbeantworter und Modem.
Analoge Sprachübertragung	Für die Übermittlung von Sprache über das Telefon werden akustische Schwingungen in kontinuierliche elektrische Signale umgewandelt, die über ein Leitungsnetz übertragen werden (digitale Sprachübertragung).
Anklopfen	Mit dem Leistungsmerkmal "Anklopfen" sind Sie auch während eines Telefonats für andere erreichbar. Ruft Sie ein weiterer Teilnehmer an, während Sie telefonieren, hören Sie den Anklopfen im Hörer Ihres Telefons. Sie können dann entscheiden, ob Sie Ihr bisheriges Gespräch fortführen oder mit dem Anklopfenden sprechen wollen.
Anklopfsperr	Soll das Leistungsmerkmal Anklopfen nicht genutzt werden, schalten Sie den Anklopfschutz ein. Während Sie ein Telefongespräch führen, wird dann einem weiteren Anrufer der Besetztton übermittelt.
Anlagenanschluss	Point-to-Point (Punkt-zu-Punkt)
Anlagenrufnummer	Zu einem Anlagenanschluss gehören eine Anlagenrufnummer und ein Rufnummernband. Mit Hilfe der Anlagenrufnummer erreichen Sie die TK-Anlage. Über eine Rufnummer des Rufnummernbands wird dann ein bestimmtes Endgerät der TK-Anlage ausgewählt.
Anruf auf einen besetzten Teilnehmer	Busy on busy =Besetzt bei Besetzt
Anruf heranholen	Leistungsmerkmal von Telefonanlagen. Anrufe können an einem internen Endgerät entgegengenommen werden, das sich nicht in der aktiven Rufverteilung befindet.

Anrufbeantworter	Einen analogen Anrufbeantworter konfigurieren Sie unter "Endgerätetyp".
Anruferliste	Komfortable Telefone wie das Systemtelefon T-Concept PX722 bieten die Möglichkeit, Anrufwünsche während der Abwesenheit zu speichern.
Anruffilter	Leistungsmerkmal, z. B. vom Systemtelefon T-Concept PX722, von Komforttelefonen oder Anrufbeantwortern. Die Rufsignalisierung erfolgt nur bei bestimmten, vorher festgelegten Telefonnummern.
Anrufschutz	Ausschalten der akustischen Anrufsignalisierung: Ruhe vor dem Telefon.
Anrufvariante Tag / Nacht	Möglichkeit bei Telefonanlagen, die Rufverteilung über einen Kalender zu ändern. Nach Büroschluss ankommende Telefonanrufe werden zu einem personell noch besetzten Telefon oder zum Anrufbeantworter, Telefax weitergeleitet.
Anrufweitschaltung in der Telefonanlage	Die Telefonanlage gibt Ihnen mit dem Leistungsmerkmal der Anrufweitschaltung (AWS) die Möglichkeit, erreichbar zu bleiben, auch wenn Sie nicht in der Nähe Ihres Telefons sind. Dieses erreichen Sie durch automatisches Weiterleiten von Anrufen an die gewünschte interne oder externe Telefonnummer. Mit dem Konfigurationsprogramm können Sie festlegen, ob die Anrufweitschaltung in der Telefonanlage oder in der Vermittlungsstelle erfolgen soll. Die Anrufweitschaltung in der Vermittlungsstelle können Sie nutzen, wenn bestimmte Leistungen für Ihren Anschluss aktiviert sind. Auskunft darüber erhalten Sie bei Ihrem Berater der T-Com.
Anrufweitschaltung in der Vermittlungsstelle	Die Möglichkeiten der Anrufweitschaltung in der Vermittlungsstelle können Sie nur über Keypad nutzen, wenn bestimmte Leistungen für Ihren Anschluss aktiviert sind. Auskunft darüber erhalten Sie beim Berater der T-Com. Die Vermittlungsstelle verbindet den anrufenden Teilnehmer mit einem von Ihnen festgelegten externen Teilnehmer.
Anschluss analoger Endgeräte	Die Leistungsmerkmale für analoge Endgeräte lassen sich nur mit Endgeräten nutzen, die mit dem MFV -Wahlverfahren wählen und eine R- bzw. eine Flash-Taste besitzen.
Anschluss von ISDN-Endgeräten	In die am internen ISDN-Bus angeschlossenen ISDN-Endgeräte muss die interne Telefonnummer des jeweiligen Anschlusses als MSN eingetragen werden und nicht die externe Telefonnummer (Mehrfachrufnummer). Siehe in der Bedienungsanleitung für die ISDN-Endgeräte: MSN eintragen. Beachten Sie bitte, dass nicht alle

im Handel angebotenen ISDN-Endgeräte die von der Telefonanlage bereitgestellten Leistungsmerkmale über ihre Tastenoberfläche nutzen können.

Anzeige der Telefonnummer des Anrufers	Voraussetzung für diese Leistung ist ein geeignetes Telefon. Die Übermittlung der Telefonnummer muss vom Anrufer freigeschaltet sein.
Anzeige und Ausgabe der Verbindungsdaten	Die Speicherung der Datensätze lässt sich über die Konfiguration für bestimmte oder auch alle Endgeräte festlegen. In der Werkseinstellung werden alle kommenden externen Verbindungen und alle von Ihnen eingeleiteten externe Gespräche gespeichert.
AOC-D	Anzeige während und am Ende der Verbindung.
AOC-D/E	Advice of Charge-During/End.
AOC-E	Anzeige nur am Ende der Verbindung.
ARP	Address Resolution Protocol
asynchron	Übertragungsverfahren, bei dem die Zeitabstände zwischen übertragenen Zeichen unterschiedlich lang sein können. Dadurch können Geräte miteinander kommunizieren, die nicht in gleichen Zeittakten arbeiten. Anfang und Ende der übertragenen Zeichen müssen durch Start- und Stop-Bits gekennzeichnet sein – im Gegensatz zu synchron.
ATM	Asynchronous Transfer Mode
Aufmerksamkeitston	Einblenden eines akustischen Signals in laufende Telefongespräche z. B. beim Anklopfen.
Aufschalten	Möglichkeit bei Telefonanlagen, sich in eine bestehende Gesprächsverbindung einzublenden. Dies wird akustisch durch einen Aufmerksamkeitston signalisiert.
Authentication	Überprüfung der Identität des Nutzers (Authentisierung).
Authorization	Auf der Basis der Identität (Authentication) kann der Nutzer auf bestimmte Dienste und Ressourcen zugreifen.
Automatische Amtsholung	Nach Abheben des Hörers an eines Telefons kann die Telefonnummer des Externteilnehmers sofort gewählt werden.
Automatische Wahlwiederholung	Leistungsmerkmal von Endgeräten. Im Besetztfall erfolgen automatisch mehrere Anwahlversuche.

- Automatischer Abbau der Internetverbindung (ShortHold)** Sie haben die Möglichkeit, ShortHold einzuschalten. Dabei legen Sie eine Zeit fest, nach der eine bestehende Verbindung getrennt wird, wenn kein Datentransfer mehr stattfindet. Wenn Sie hier die Zeit 0 eintragen ist ShortHold ausgeschaltet.
- Automatischer Rückruf** Komfortleistung bei Telefonen: Per Tastendruck oder Kennziffer fordert der Anrufer von einem besetzten Endgerät einen Rückruf an. Ist der gewünschte Teilnehmer nicht an seinem Platz oder kann er das Gespräch nicht annehmen, wird er automatisch mit dem Anrufer verbunden, sobald er sein Telefon das nächste Mal benutzt hat und den Hörer wieder auflegt.
- Automatischer Rückruf bei Besetzt** Diese Funktion ist nur mit Telefonen nutzbar, die Nachwahl erlauben! Ein automatischer Rückruf ist aus einer Rückfrageverbindung nicht möglich.
- Automatischer Rückruf bei Besetzt (CCBS)** Sie müssen dringend Ihren Geschäftspartner oder einen internen Teilnehmer erreichen. Bei einem Anruf auf dessen Anschluss hören Sie jedoch immer den Besetztton. Wenn Sie eine Mitteilung erhalten, dass der gewünschte Teilnehmer das Gespräch beendet hat, wären Ihre Chance, ihn zu erreichen sehr gut. Mit dem "Rückruf bei Besetzt" können Sie den besetzten Gesprächspartner sofort erreichen, wenn dieser am Ende seines Gespräches den Hörer auflegt. Ihr Telefon klingelt dann. Wenn Sie jetzt den Hörer abheben, wird automatisch eine Verbindung zum gewünschten Teilnehmer aufgebaut. Ein interner "Rückruf bei Besetzt" wird automatisch nach 30 Minuten gelöscht. Der externe "Rückruf bei Besetzt" wird nach einer von der Vermittlungsstelle vorgegebenen Zeit gelöscht (ca. 45 Minuten). Manuelles Löschen vor Ablauf der Zeit ist ebenfalls möglich.
- Automatischer Rückruf bei Nichtmelden (CCNR)** Sie müssen dringend Ihren Geschäftspartner oder einen internen Teilnehmer erreichen. Bei einem Anruf auf dessen Anschluss hören Sie zwar immer den Freiton, Ihr Partner ist jedoch nicht in der Nähe seines Telefons und hebt nicht ab. Mit dem "Rückruf bei Nichtmelden" können Sie den Teilnehmer sofort erreichen, wenn dieser ein Gespräch beendet hat oder den Hörer seines Telefons abhebt und wieder auflegt. Ihr Telefon klingelt dann. Wenn Sie jetzt den Hörer abheben, wird automatisch eine Verbindung zum gewünschten Teilnehmer aufgebaut.
- B-Kanal** Basiskanal eines ISDN-Basisanschlusses bzw. Primärmultiplexanschlusses zur Übertragung von Nutzinformationen (Sprache, Daten). Ein ISDN-Basisanschluss besitzt zwei B-Kanäle und einen D-Kanal. Ein B-Kanal hat eine Datenübertragungsrate von 64 kBit/s. Durch Kanalbündelung kann mit Ihrem Gateway die Datenübertra-

gungsrate bei einem ISDN-Basisanschluss auf bis zu 128 kBit/s gesteigert werden.

B-Telefonnummer unterdrücken (COLR)	COLP/COLR: Connected Line Identification Presentation/Connected Line Identification Restriction = Übermittlung der Telefonnummer des Anrufenden zum Angerufenen einschalten/unterdrücken. Mit diesem Leistungsmerkmal wird das Anzeigen der Telefonnummer des angerufenen Teilnehmers unterdrückt. Wird die Anzeige der B-Telefonnummer unterdrückt, wird nach Annahme eines Anrufes Ihre eigene Telefonnummer nicht zum Anrufenden übermittelt.
BACP/BAP	Bandwidth Allocation Control Protocols (BACP/BAP nach RFC 2125)
Basisanschluss	ISDN-Anschluss, der zwei Nutzkanäle (B-Kanäle) von je 64 KBit/s und einen Steuerkanal (D-Kanal) mit 16 KBit/s umfasst. Die beiden Nutzkanäle können unabhängig voneinander für jeden im T-ISDN angebotenen Dienst genutzt werden. Man kann also z. B. telefonieren und zur gleichen Zeit faxen. Die T-Com bietet den Basisanschluss als Mehrgeräte- oder Anlagenanschluss an.
Bedienführung	Elektronische Bedienungsanleitung, die den Anwender per Display Schritt für Schritt zu gewünschten Funktionen eines Endgeräts wie z. B. Telefon, Anrufbeantworter oder Faxgerät führt (menügeführte Bedienung).
Block Cipher Modes	Blockorientierter Verschlüsselungsalgorithmus
Blowfish	Ein von Bruce Schneier entwickelter Algorithmus. Es handelt sich um eine block cipher mit einer Blockgröße von 64 Bit und einem Schlüssel mit variabler Länge (bis 448 Bits).
Bluetooth	Bluetooth ist eine drahtlose Übertragungstechnik, die verschiedene Geräte miteinander verbinden kann. Bluetooth ist dabei ein Kabelersatz zum Anschluss verschiedener Geräte, z. B. Notebook, PC, PDA, etc.. Diese Geräte können dank Bluetooth ohne eine feste Verbindung miteinander Daten austauschen. Zum Beispiel können PCs, Notebooks oder PDA Zugang zum Internet oder einem lokalen Netzwerk erlangen. Die Termine eines PDA können mit den Terminen auf dem PC synchronisiert werden, ohne dass hierfür eine Kabelverbindung erforderlich ist. Aufgrund der vielfältigen Anwendungsmöglichkeiten der Bluetooth-Technik werden die einzelnen Verbindungsarten zwischen den Geräten in Profiles unterteilt. Durch ein Profile wird der Dienst (die Funktion) festgelegt, den die einzelnen Bluetooth-Clients untereinander nutzen können.

BOD	Bandwith on Demand
BootP	Bootstrap Protocol
Bps	Bits pro Sekunde. Ein Maßstab für die Übertragungsrate.
BRI	Basic Rate Interface
Bridge	Netzwerkkomponente zum Verbinden gleichartiger Netze. Im Gegensatz zu einem Gateway arbeiten Bridges auf Schicht 2 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.
Broadcast	Broadcasts sind Rundrufe (Datenpakete), die an alle im Netz angeschlossenen Geräte gesendet werden, um Informationen im Netz auszutauschen. Normalerweise gibt es im Netz eine bestimmte Adresse (Broadcast-Adresse), die es allen Geräten ermöglicht, eine Nachricht als Broadcast zu interpretieren.
Browser	Programm zur Darstellung von Inhalten im Internet bzw. WorldWide-Web.
Bus	Ein Medium zur Datenübertragung für alle Geräte im Netz. Die Daten werden über den gesamten Bus verbreitet und von allen Geräten am Bus empfangen.
CA	Certificate Authority
Call Through	Unter Call Through versteht man die Einwahl über einen externen Anschluss in die Telefonanlage und die Weiterwahl aus der Telefonanlage über einen anderen externen Anschluss.
Called Party's Number	Nummer des Angerufenen.
Calling Party's Number	Nummer des Anrufers.
CAPI	Common ISDN Application Programming Interface
CAST	Ein 128-bit Verschlüsselungsalgorithmus mit ähnlicher Funktionalität wie DES. Siehe Block Cipher Modes.
CBC	Cipher Block Chaining

CCITT	Commite Consultatif International Telegraphique et Telephonique
CD (Call Deflection)	Weiterleiten von Anrufen. Mit diesem Leistungsmerkmal haben Sie die Möglichkeit, einen Anruf weiterzuleiten, ohne diesen selbst annehmen zu müssen. Leiten Sie einen Anruf zu einem externen Teilnehmer weiter, tragen Sie die anfallenden Verbindungskosten von Ihrem Anschluss zu dem Ziel der Anrufweiterleitung. Sie können dieses Leistungsmerkmal vom Systemtelefon nutzen, oder von ISDN-Telefonen, die diese Funktion unterstützen (siehe Bedienungsanleitung der Endgeräte). Weitere Hinweise zur Ausführung dieses Leistungsmerkmal mit dem Telefon entnehmen Sie bitte der Bedienungsanleitung.
Certificate	Zertifikat
CHAP	Challenge Handshake Authentication Protocol
CLID	Calling Line Identification (Rufnummernüberprüfung)
Client	Ein Client nutzt die von einem Server angebotenen Dienste. Clients sind in der Regel Arbeitsplatzrechner.
CLIP	Abkürzung für Calling Line Identification Presentation. Telefonnummernanzeige des Anrufenden.
CLIR	Abkürzung für Calling Line Identification Restriction. Zeitweise Unterdrückung der Übermittlung der Telefonnummer des Anrufenden.
COLR	Connected Line Identification Restriction (B-Telefonnummer unterdrücken). Mit diesem Leistungsmerkmal wird das Anzeigen der Telefonnummer des angerufenen Teilnehmers ermöglicht oder unterdrückt. Ist die Anzeige der B-Telefonnummer unterdrückt, wird nach Annahme eines Anrufes Ihre eigene Telefonnummer nicht zum Anrufenden übermittelt. Beispiel: Sie haben eine Rufumleitung zu einem anderen Endgerät eingerichtet. Hat dieses Endgerät das Unterdrücken der B-Telefonnummer eingeschaltet, sieht der Anrufende keine Telefonnummer im Display seines Endgerätes.
Configuration Manager	Windows-Applikation (ähnlich dem Windows-Explorer), die SNMP-Kommandos benutzt, um die Einstellungen Ihres Gateways abzufragen und vorzunehmen. Die Applikation wurde vor der BRICKware, Version 5.1.3, als DIME Browser bezeichnet.
CRC	Cyclic Redundancy Check
CTI	Computer-Telephony Integration. Begriff für die Verbindung zwischen Telefonanlage und Server. Durch CTI können Funktionen der

	Telefonanlage von einem PC gesteuert bzw. ausgewertet werden.
D-Kanal	Steuerkanal eines ISDN-Basisanschlusses bzw. Primärmultiplexanschlusses. Der D-Kanal hat eine Datenübertragungsrate von 16 kBit/s. Außer dem D-Kanal besitzt jeder ISDN-Basisanschluss zwei B-Kanäle.
Datagramm	Ein in sich abgeschlossenes Datenpaket, das mit einem Minimum an Protokoll-Overhead im Netz weitergeleitet wird – ohne Quittierungsmechanismus.
Datenkompression	Methode, um übertragene Datenmengen zu verringern. Bei gleicher Übertragungsdauer kann so der Durchsatz erhöht werden. Bekannte Verfahren sind z. B. STAC, VJHC, MPPC.
Datenpaket	Ein Datenpaket dient der Übermittlung von Informationen. Jedes Datenpaket enthält eine vorgeschriebene Anzahl von Zeichen (Informationen und Steuerzeichen).
Datenübertragungsrates	Die Datenübertragungsrate gibt die Anzahl der Informationseinheiten pro Zeitabschnitt an, die zwischen Sender und Empfänger übertragen werden.
Datex-J	Abkürzung für Data Exchange Jedermann. Die Zugangsplattform zu T-Online. Lokale Einwahlknoten in jedem Ortsnetz. In einigen deutschen Großstädten gibt es zusätzliche Hochgeschwindigkeitszugänge über T-Net/T-Net-ISDN.
DCE	Data Circuit-Terminating Equipment
Default Gateway	Bezeichnet die Adresse des Routers, an den sämtlicher Verkehr gesendet wird, der nicht für das eigene Netzwerk bestimmt ist.
Denial-Of-Service Attack	Ein Denial-of-Service (DoS) Angriff ist ein Versuch, ein Gateway oder einen Host in einem LAN mit gefälschten Requests zu überfluten, so dass diese völlig überlastet sind. Das bedeutet das System oder ein bestimmter Dienst kann nicht mehr betrieben werden.
DES	Data Encryption Standard
DFÜ	Datenfernübertragung
DHCP	Dynamic Host Configuration Protocol
DIME	Desktop Internetworking Management Environment
DIME Browser	Alte Bezeichnung für Configuration Manager.

DLCI	In einem Frame Relay Netzwerk bezeichnet ein DLCI eine virtuelle Verbindung eindeutig. Beachten Sie, dass ein DLCI nur für das lokale Ende der Punkt-zu-Punkt-Verbindung von Bedeutung ist.
DMZ	DeMilitarized Zone
DNS	Domain Name System
DOI	Domain Of Interpretation
Domäne	Ein Domäne ist ein logischer Zusammenschluss von Geräten in einem Netzwerk. Im Internet Teil einer Namenshierarchie (z. B. bintec.de).
Dotted Decimal Notation	Die syntaktische Repräsentation für eine 32-Bit-Ganzzahl, die in vier 8-Bit-Zahlen in dezimaler Schreibweise geschrieben ist und durch Punkt unterteilt ist. Sie wird zur Darstellung von IP-Adressen im Internet verwendet, z. B. 192.67.67.20
Downstream	Datenübertragungsrate vom ISP zum Kunden.
DSA (DSS)	Digital Signature Algorithm (Digital Signature Standard).
DSL/xDSL	Digital Subscriber Line
DSS1	Digital Subscriber Signalling System
DSSS	Direct Sequence Spread Spectrum ist eine Funktechnologie, die ursprünglich für den militärischen Bereich entwickelt wurde und eine hohe Störsicherheit bietet, weil das Nutzsignal auf einen breiten Bereich gespreizt wird. Das Signal wird mittels einer Spreizsequenz oder Chipping Code, bestehend aus 11 Chips auf 22MHz Breite gespreizt. Selbst wenn ein oder mehr Chips in der Übertragung gestört sind, kann aus den restlichen Chips die Information zuverlässig zurückgewonnen werden.
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi Frequency (Tonfrequenzwahlsystem)
Durchwahl	Leistungsmerkmal von größeren Telefonanlagen am Anlagenanschluss: Die Nebenstellen können gezielt von Extern angerufen werden.
Durchwahlbereich	Siehe Rufnummernband
Durchwahlnummer	Eine Durchwahlnummer (Extension) ist eine interne Rufnummer für

ein Endgerät oder ein Subsystem. Bei Anlagenanschlüssen ist die Durchwahlnummer in der Regel eine Rufnummer aus dem vom Telefonanbieter zugeteilten Rufnummernband. Bei Mehrgeräteanschlüssen kann es die MSN oder ein Teil der MSN sein.

Dynamische IP Adresse

Im Gegensatz zu einer statischen IP Adresse wird die dynamische IP Adresse temporär per DHCP zugeordnet. Netzwerk Komponenten wie Web-Server oder Drucker besitzen in der Regel statische IP Adressen, Clients wie Notebooks oder Workstations erhalten meist dynamische IP Adressen.

E-Mail

Electronic Mail

E1/T1

E1: Europäische Variante des ISDN-Primärmultiplexanschlusses mit 2,048 MBit/s, die auch als E1-System bezeichnet wird.

EAZ

Endgeräteauswahlziffer

ECB

Electronic Code Book mode

ECT

Explizit Call Transfer = Externes Vermitteln. Mit diesem Leistungsmerkmal können zwei externe Verbindungen vermittelt werden, ohne die beiden B-Kanäle des Amtsanschlusses zu blockieren.

Eigene Telefonnummer für das nächste Gespräch festlegen

Falls Sie z. B. am späten Abend aus Ihrem privaten Bereich - vielleicht dem Wohnzimmer - noch geschäftlich telefonieren wollen, können Sie Ihre geschäftliche Telefonnummer für dieses Gespräch als gehende Mehrfachrufnummer (MSN) definieren. Der Vorteil liegt zum einen darin, dass die Verbindung unter der ausgewählten MSN kostenmäßig erfasst wird und zum anderen kann Ihr Gesprächspartner Sie an der übermittelten MSN erkennen. Bevor Sie eine externe Wahl beginnen, können Sie festlegen, welche Ihrer Telefonnummern zur Vermittlungsstelle und zum externen Gesprächspartner mitgesendet werden soll. Die Auswahl erfolgt über den Telefonnummern-Index.

Eigene Telefonnummer unterdrücken

Temporäres Ausschalten der Übermittlung der eigenen Telefonnummer.

Einstellungen zurücksetzen (Reset)

Ein Reset der Telefonanlage ermöglicht es Ihnen, Ihre Anlage wieder in einen definierten Ausgangszustand zu bringen. Dieses kann nötig sein, wenn unerwünschte Konfigurationen zurückgenommen oder die Telefonanlage neu programmiert werden soll.

Einwahlparameter

Legen Sie die Einwahlparameter fest, d.h. Sie geben die Einwahlrufnummer des Providers ein und legen fest:

Empfangsabruf	Funktion von Faxgeräten, um bei anderen Faxgeräten oder von Faxdatenbanken bereitgestellte Dokumente "abzuholen".
Encapsulation	Enkapsulierung von Datenpaketen in ein bestimmtes Protokoll, um die Datenpakete über ein Netzwerk zu übertragen, das den ursprünglichen Protokolltyp nicht direkt unterstützt (z. B. NetBIOS über TCP/IP).
Encryption	Bezeichnet die Verschlüsselung von Daten, z. B. MPPE.
Erfassen der externen Verbindungsdaten	In der Werkseinstellung werden alle, sowohl gehende als auch kommende über Ihre Telefonanlage geführten externen Verbindungen erfasst und in Form von Verbindungsdatensätzen gespeichert.
Erweiterte Wahlwiederholung	Eine gewählte Telefonnummer wird in einem Speicher des Telefons "geparkt". Sie kann später wieder gewählt werden, auch wenn zwischendurch mit anderen Telefonnummern telefoniert worden ist.
ESP	Encapsulating Security Payload
ESS	Der Extended Service Set bezeichnet mehrere BSS (mehrere Access Points) die ein einzelnes logisches Funknetz bilden.
Ethernet	Ein lokales Netzwerk, das alle Geräte im Netz (Rechner, Drucker, etc.) über ein Twisted-Pair- oder Koaxialkabel verbindet.
Ethernet-Anschlüsse	Die 4 Anschlüsse sind gleichberechtigt über einen internen Switch herausgeführt. An die Anschlussbuchsen können Netzwerkclients direkt angeschlossen werden. Die Ports sind als 100/BaseT voll-duplex, autosensing, auto MDIX abwärtskompatibel zu 10/Base T realisiert. Hier können IP-Softclients mit SIP-Standard auf PCs mit Netzwerkkarte oder bis zu 4 SIP-Telefone direkt angeschlossen werden.
Eumex Recovery	Sollte während des Ladens einer neuen Firmware die Stromversorgung der Telefonanlage unterbrochen werden, sind alle Funktionen der Telefonanlage gelöscht.
Euro-ISDN	Harmonisiertes, in Europa standardisiertes ISDN, beruhend auf dem Signalisierungsprotokoll DSS1, zu dessen Einführung sich Netzbetreiber in über 20 europäischen Staaten verpflichtet haben. In Deutschland ist das Euro-ISDN - nach dem nationalen Vorläufersystem 1 TR6 - inzwischen eingeführt.
Eurofile-Transfer	Kommunikationsprotokoll für den Austausch von Dateien zwischen zwei PCs über ISDN mittels ISDN-Karte (File-Transfer) oder über dafür vorbereitete Telefone oder Telefonanlagen.

Fall Back: Priorität der Internet-Provider-Einträge	Die Priorität der Internet-Provider-Einträge wird nach der Reihenfolge festgelegt, in der sie in die Liste eingetragen werden. Der erste Eintrag einer DSL-Verbindung ist der Standardzugang. Sollte über den Standardzugang nach einer vorgegebenen Anzahl von Versuchen, kein Verbindungsaufbau möglich sein, wird die Verbindung über den zweiten Eintrag und die folgenden Einträge versucht. Wenn auch der letzte Eintrag auf der Liste nicht zu einem erfolgreichen Verbindungsaufbau führt, wird der Vorgang bis zu einer erneuten Anfrage abgebrochen. Wenn der Fall Back eintritt, und alle übrigen ISP's nur durch Wahlverbindungen zu erreichen sind, können beide B-Kanäle belegt sein. Im Falle einer Kanalbündelung sind Sie dann für die Dauer dieser Verbindung nicht zu erreichen.
Fax	Kurzform für Telefax.
Fernabfrage	Anrufbeantworterfunktion. Aus der Ferne Nachrichten abhören, meist in Verbindung mit Möglichkeiten wie Nachrichten löschen oder Ansagen ändern.
Ferndiagnose/Fernwartung	Einige Endgeräte und Telefonanlagen werden komfortabel von T-Service Stützpunkten aus über die Telefonleitung betreut bzw. gewartet. Spart in vielen Fällen den Einsatz eines Servicetechnikers vor Ort.
Feststation	Zentraleinheit von schnurlosen Telefongeräten. Es gibt zwei verschiedene Ausführungen: Die einfache Feststation dient zum Aufladen der Handgeräte. Bei den so genannten Komforttelefonen ist die Feststation gleichzeitig als Telefon nutzbar, die Handgeräte werden über separate Ladestationen aufgeladen.
Feststellen böswilliger Anrufer (Fangen)	Dieses Leistungsmerkmal müssen Sie bei der T-Com beauftragen. Dort wird man Sie auch über die weitere Vorgehensweise informieren. Wenn Sie während eines Gespräches oder nach Beendigung des Gespräches durch den Anrufer (Sie hören den Besetzt-Ton aus der Vermittlungsstelle) die Kennziffer 77 wählen, wird die Telefonnummer des Anrufers in der Vermittlungsstelle gespeichert. ISDN-Telefone können für dieses Leistungsmerkmal auch eigene Funktionen nutzen. Weitere Hinweise zur Ausführung dieser Funktion entnehmen Sie bitte der Bedienungsanleitung.
Festverbindung	Standleitung (leased line)
FHSS, Frequency Hopping Spread Spectrum	Frequenzspreizung wird in einem FHSS System durch ständig nach bestimmten Sprungmustern wechselnde Frequenzen erreicht. Im Gegensatz zu DSSS Systemen gibt es hier keine fest eingestellte Frequenz, sondern einstellbare Sprungmuster (hopping patterns).

Die Frequenz wird innerhalb einer Sekunde sehr häufig gewechselt.

File-Transfer

Datenübertragung von einem Computer zu einem anderen, z. B. nach dem Eurofile-Transfer-Standard.

Filter

Ein Filter besteht aus einer Anzahl von Kriterien (z. B. Protokoll, Port-Nummer, Quell- und Zieladresse). Anhand dieser Kriterien wird ein Paket aus dem Datenstrom ausgesondert. Mit einem so bestimmten Paket kann dann in spezifischer Weise verfahren werden. Zu diesem Zweck wird mit dem Filter eine bestimmte Aktion verbunden. Dadurch entsteht eine Filterregel.

Firewall

Bezeichnet die Summe der Schutzmechanismen für das lokale Netzwerk gegen Zugriffe von außen. Mit Ihrem Gateway stehen Schutzmechanismen wie NAT, CLID, PAP/CHAP, Access-Listen etc. zur Verfügung.

Firmware

Software Code, der alle Funktionen eines Gerätes beinhaltet. Dieser Code wird in einen PROM (Programmable Read Only Memory) geschrieben und bleibt dort auch nach Abschalten des Gerätes erhalten. Firmware kann durch den Benutzer erneuert werden, wenn eine neue Software Version verfügbar ist (Firmware Upgrade).

First-Level Domain

Englische Bezeichnung für den letzten Teil eines Namens im Internet. Bei www.t-com.de lautet die First-Level Domain de und bezeichnet in diesem Fall Deutschland.

Flash-Taste

Die Flash-Taste bei Telefonen entspricht der R-Taste. R ist die Abkürzung für Rückfrage. Die Taste unterbricht die Leitung für einen kurzen Moment, um bestimmte Funktionen wie z. B. Rückfrage über die Telefonanlage einzuleiten.

Follow-me

Leistungsmerkmal von Telefonanlagen zur Rufumleitung von Gesprächen am Zieltelefon.

Fragmentierung

Prozess, durch den ein IP-Datagramm in kleiner Teile getrennt wird, um die Bedingungen eines physikalischen Netzes zu erfüllen. Der umgekehrte Prozess wird Reassembly genannt.

Frame

Einheit der Information, die über eine Datenverbindung gesendet wird.

Frame Relay

Eine Packet Switching Methode, die kleinere Pakete und weniger Fehlerprüfung beinhaltet als das traditionelle Packet Switching wie X.25. Aufgrund seiner Eigenschaften wird Frame Relay für schnelle WAN-Verbindungen mit dichtem Traffic verwendet.

Freecall	Telefonnummer. Bisher Service 0130. Seit dem 1. Januar 1998 werden diese Telefonnummern auf freecall 0800 umgestellt.
Freisprechen	Ermöglicht freihändiges Telefonieren bei Telefonen mit eingebautem Mikrofon und Lautsprecher. Weitere Personen im Raum können so am Gespräch teilnehmen.
FTP	File Transfer Protocol
Full Duplex	Betriebsart, bei der beide Kommunikationspartner gleichzeitig bidirektional kommunizieren können.
Funktionstasten	Mit Telefonnummern oder Netzfunktionen belegbare Tasten an Telefonen.
G.991.1	Datenübertragungsempfehlung für HDSL
G.991.2	Datenübertragungsempfehlung für SHDSL
G.992.1	Datenübertragungsempfehlung für ADSL Siehe auch G.992.1 Annex A und G.992.1 Annex B.
G.992.1 Annex A	Datenübertragungsempfehlung für ADSL: ITU-T G.992.1 Annex A
G.992.1 Annex B	Datenübertragungsempfehlung für ADSL: ITU-T G.992.1 Annex B
G.SHDSL	Siehe G.991.2.
Gateway	Aus-/Einfahrt, Übergangspunkt
Gehende Durchwahlsignalisierung	Die "gehende Durchwahlsignalisierung" ist für interne Anschlüsse am Anlagenanschluss vorgesehen, denen keine explizite Durchwahl zugeordnet wurde. Bei einem Anruf nach extern wird die unter gehende Durchwahlsignalisierung eingetragene Durchwahlnummer mit gesendet.
Gehende Telefonnummer	Sofern Sie die Übermittlung Ihrer Telefonnummern nicht unterdrückt haben und das Telefon Ihres Gesprächspartners die CLIP-Funktion unterstützt, kann Ihr Gesprächspartner die Telefonnummer des Anschlusses, von dem aus Sie telefonieren, im Display seines Telefons sehen. Diese bei einem Ruf nach extern übermittelte Telefonnummer wird als gehende Telefonnummer bezeichnet.
Gesprächskostenkonto	Sie können hier für einen Teilnehmer ein "Gesprächskostenkonto" einrichten. Jedem Teilnehmer kann damit auf seinem persönlichen "Gesprächskostenkonto" eine maximal zur Verfügung stehende Anzahl von Einheiten in Form eines Limits zugeteilt werden. Damit Ein-

	heiten abgebucht werden, ist "Kostenlimit" aktiv zu schalten. Sind die Einheiten verbraucht, sind keine Gespräche nach extern mehr möglich. Interne Gespräche können jederzeit weiter geführt werden. Die Abbuchung des Kontos erfolgt jeweils nach Beendigung eines Gespräches.
Half Duplex	Bidirektionale Kommunikationsmethode, bei der zu einem Zeitpunkt nur gesendet oder empfangen werden kann. Wird auch Simplex genannt.
Halten einer Verbindung	Ein Telefongespräch auf Wartestellung schalten, ohne die Verbindung zu verlieren (Rückfragen/Makeln).
Halten in der Telefonanlage	Bei den Leistungsmerkmalen "Während eines Gespräches einen weiteren Gesprächspartner anrufen" und "Mit zwei Gesprächspartnern abwechselnd sprechen" (Makeln) werden beide B-Kanäle des ISDN-Anschlusses benötigt. Über den zweiten B-Kanal Ihrer Telefonanlage sind Sie dann von extern nicht erreichbar und können selbst nicht extern telefonieren. In dieser Einstellung hört ein gehaltener externer Gesprächspartner die Wartemusik der Telefonanlage.
Handgerät	Mobile Komponente bei schnurlosen Telefongeräten. Bei digitaler Übertragung kann auch zwischen den Handgeräten telefoniert werden (DECT).
hashing	Der Vorgang des Ableitens einer Nummer, hash genannt, von einer Zeichenfolge. Ein Hash ist im allgemeinen viel kürzer als der Textfluss, von dem er abgeleitet wurde. Der Hashing-Algorithmus ist so gestaltet, dass mit ziemlich geringer Wahrscheinlichkeit ein Hash generiert wird, der mit einem anderen Hash, der aus einer Textfolge mit unterschiedlicher Bedeutung generiert wurde, übereinstimmt. Verschlüsselungsvorrichtungen benutzen Hashing, um sicherzustellen, dass Eindringlinge übermittelte Nachrichten nicht verändern können.
HDLC	High Level Data Link Control
HDSL	High Bit Rate DSL
HDSL2	High Bit Rate DSL, Version 2
Headset	Kombination aus Kopfhörer und Mikrofon als nützliche Hilfe für alle, die viel telefonieren müssen und dabei die Hände für Notizen frei haben wollen.
Heranholen von Ru-	Ein externer Anruf wird nur bei Ihrem Kollegen signalisiert. Da Sie

fen (Pick up)	sich in verschiedenen Teams befinden, ist das nicht verwunderlich. Sie können nun verschiedene Gruppen von Teilnehmern bilden, in denen das Heranholen Rufen möglich ist. Ein Ruf kann nur von Teilnehmern/Endgeräten der gleichen Pick up Gruppe herangeholt werden. Das Zuordnen der Teilnehmer in Pick up Gruppen ist unabhängig von den jeweiligen Einstellungen in der Team-Anrufzuordnung Tag und Nacht.
HMAC	Hashed Message Authentication Code
HMAC-MD5	Hashed Message Authentication Code - benutzt den Message - Digest-Algorithmus Version 5.
HMAC-SHA1	Hashed Message Authentication Code - benutzt den Secure-Hash-Algorithm Version 1.
Hook-Flash	Die Nutzung der Komfortleistungen Rückfragen, Makeln, Dreierkonferenz im T-Net und bestimmter Leistungsmerkmale einiger Telefonanlagen sind nur mit der Hook-Flash-Funktion (langer Flash) der Signaltaste am Telefon möglich. Bei modernen Telefonen ist diese Taste mit "R" bezeichnet.
Hörerlautstärke	Regelung der Lautstärke im Telefonhörer.
Host-Name	Bezeichnet in IP-Netzen einen Namen, der anstelle einer zugehörigen Adresse benutzt wird. Ein Host-Name besteht aus einer ASCII-Zeichenfolge, die den Host eindeutig kennzeichnet.
HTTP	HyperText Transfer Protocol
Hub	Netzwerkkomponente, mit der mehrere Netzwerkkomponenten zu einem lokalen Netz zusammengeschlossen werden (sternförmig).
IAE	ISDN-Anschlusseinheit ISDN-Anschlussdosen.
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value
IEEE	Das Institute of Electrical and Electronics Engineers (IEEE). Ein großer weltweiter Zusammenschluss von Ingenieuren. Arbeitet ständig an Standards und Normen, um das Zusammenspiel verschiedenster Geräte zu gewährleisten.
IETF	Internet Engineering Task Force
Index	Der Index von 0...9 ist fest vorgegeben. Jede eingetragene externe

Mehrfachrufnummer wird einem Index zugeordnet. Diesen Index benötigen Sie beim Einrichten von Leistungsmerkmalen über die Kennziffern eines Telefons, z. B. Einrichten einer "Anrufweiterechaltung in der Vermittlungsstelle" oder "Telefonnummer für das nächste externe Gespräch festlegen".

- Infrastruktur Modus** Ein Netzwerk im Infrastruktur Modus ist ein Netzwerk, das mindestens einen Access Point als zentrale Kommunikations- und Steuerstelle beinhaltet. 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 solches Netzwerk wird auch BSS (Basic Service Set) genannt, ein Netzwerk, das aus mehreren BSS besteht wird ESS (Extended Service Set) genannt. Die meisten Funknetze arbeiten im Infrastruktur Modus, um Verbindung mit dem verkabelten Netz herzustellen.
- Interne Telefonnummern** Ihre Telefonanlage verfügt über einen festen internen Telefonnummernplan.
- Internet** Das Internet besteht aus einer Reihe von regionalen, lokalen und Universitätsnetzen. Für Datenübertragung im Internet wird das Protokoll IP verwendet.
- Internet Time Sharing** Ermöglicht mehreren Nutzern gleichzeitig über eine ISDN-Verbindung im Internet zu surfen. Die Informationen werden zeitversetzt von den einzelnen Computern abgefragt.
- Interngespräche** Kostenfreie Verbindung zwischen Endgeräten einer Telefonanlage.
- Internkennziffer übertragen** Erhalten Sie bei Abwesenheit an Ihrem Anschluss einen internen Anruf z. B. vom Teilnehmer mit der internen Telefonnummer 22, wird seine interne Telefonnummer in der Anruferliste Ihres Telefons gespeichert. Da Ihr Anschluss aber werkseitig auf automatische Amtsholung eingestellt ist, müssten Sie für einen Rückruf zunächst ** wählen, um den internen Wählton zu erhalten, und dann die 22. Ist "Internkennziffer übertragen" aktiv, wird ** vor die 22 gesetzt und der Rückruf kann automatisch aus der Anruferliste heraus erfolgen.
- Internrufton** Besondere Signalisierung an Telefonanlagen zur Unterscheidung von Intern- und Externanrufen.
- Intranet** Lokales, unternehmensinternes Computernetz auf der Basis von Internettechnologien, das die gleichen Internetdienste bereitstellt, wie z. B. E-Mail-Versand und Homepages.

IP	Internet Protocol
IP-Adresse	In einem IP-Netzwerk der erste Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 192.168.1.254. Siehe auch Netzmaske.
IPComP	IP payload compression
IPCONFIG	Ein Hilfsmittel, das unter Windows Computern verwendet wird, um die eigenen IP Einstellungen zu überprüfen oder zu ändern.
IPoA	IP over ATM
ISDN	Integrated Services Digital Network
ISDN-Adresse	Die Adresse eines ISDN-Gerätes, welche aus einer ISDN-Nummer besteht gefolgt von weiteren Ziffern, die sich auf ein spezifisches Endgerät beziehen, z. B. 47117.
ISDN-Basisanschluss	Teilnehmeranschluss beim ISDN. Der Basisanschluss besteht aus zwei B-Kanälen und einem D-Kanal. Außer dem Basisanschluss gibt es noch den Primärmultiplexanschluss. Die Schnittstelle zum Teilnehmer wird über den sogenannten So-Bus geschaffen.
ISDN-BRI	ISDN Basic Rate Interface
ISDN-Dynamic	Dieses Leistungsmerkmal setzt die Installation des T-ISDN Speedmanagers voraus! Wenn Sie gerade im Internet surfen, und zum Download zwei B-Kanäle nutzen, sind Sie telefonisch von Extern nicht mehr erreichbar. Da die Signalisierung eines weiteren Anrufes über den D-Kanal erfolgt, hat Ihre Telefonanlage, je nach Einstellung, die Möglichkeit, einen B-Kanal gezielt abzuschalten und Sie können das Gespräch annehmen.
ISDN-Intern/-Extern	Alternative Bezeichnung für den S0-Bus.
ISDN-Karte	Adapter für den Anschluss eines PCs an den ISDN-Basisanschluss. Technisch unterscheidet man aktive und passive Karten. Aktive ISDN-Karten verfügen über einen eigenen Prozessor, der Kommunikationsvorgänge unabhängig vom PC-Prozessor abwickelt und somit keine Ressourcen benötigt. Eine passive ISDN-Karte hingegen nutzt Ressourcen des PCs.
ISDN-Login	Funktion Ihres Gateways. Über ISDN-Login ist Ihr Gateway fernkonfigurier- und wartbar. ISDN-Login funktioniert bereits bei Gateways im Auslieferungszustand, sobald sie mit einem ISDN-Anschluss verbunden und so über eine Rufnummer erreichbar sind.

ISDN-Nummer	Die Netzwerkadresse der ISDN-Schnittstelle, z. B. 4711.
ISDN-PRI	ISDN Primary Rate Interface
ISDN-Router	Ein Router, der nicht über Netzwerkanschlüsse verfügt, aber gleiche Funktionen zwischen PC, ISDN und dem Internet bereitstellt.
ISO	International Standardization Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union
IWV	Abkürzung für Impulswahlverfahren. Herkömmliches Wahlverfahren im Telefonnetz. Wählziffern werden durch eine definierte Anzahl von Gleichstromimpulsen dargestellt. Das Impulswahlverfahren wird durch das Mehrfrequenzwahlverfahren (MFV) abgelöst.
Kalender	Mit der Zuweisung eines Kalender erfolgt die Umschaltung zwischen den Anrufzuordnungen Tag und Nacht. Für jeden Wochentag kann eine beliebige Tag-/ Nachtschaltzeit gewählt werden. Ein Kalender verfügt über jeweils vier Schaltzeiten, die jedem einzelnen Wochentag gezielt zugewiesen werden können.
Kanalbündelung	Channel Bundling
Key Escrow	Hinterlegte Schlüssel können von der Regierung eingesehen werden. Besonders die U.S.-Regierung schreibt Schlüsselhinterlegung vor, um zu verhindern, dass Verbrechen durch Datenverschlüsselung getarnt werden.
Kombigerät	Ist ein analoger Endgeräteanschluss der Telefonanlage als „Multifunktionsport“ für Kombigeräte eingerichtet, werden alle Anrufe unabhängig vom Dienst angenommen. Bei einer Amtsholung über Kennziffern können unabhängig von der Konfigurierung des analogen Anschlusses die Dienstkennungen „analoge Telefonie“ oder „Telefax Gruppe 3“ mit gesendet werden. Bei Wahl der 0 wird die Dienstkennung „analoge Telefonie“ mit gesendet.
Komfortanschluss	T-ISDN Basisanschluss mit umfangreichem Leistungsangebot: Anklöpfen, Anrufweilerschaltung, Dreierkonferenz, Gesprächskostenanzeige am Ende der Verbindung, Rückfragen/Makeln, Telefonnummernübermittlung. Im Komfortanschluss sind als Standard drei Mehrfachrufnummern enthalten.
Komfortleistungen	Leistungsmerkmale der Netze T-Net und T-ISDN wie Anzeige der Telefonnummer des Anrufers, Rückruf bei Besetzt, Anrufweiter-

schaltung, veränderbare Anschluss-Sperre, veränderbare Telefonnummernsperre, Verbindung ohne Wahl und Übermittlung von Tarifinformationen. Die Verfügbarkeit ist abhängig vom Standard der angeschlossenen Endgeräte.

Konferenzschaltung	Leistungsmerkmal von Telefonanlagen: Mehrere interne Gesprächsteilnehmer können gleichzeitig telefonieren. Es sind auch mit externen Gesprächspartnern, Dreierkonferenzen möglich.
Konfiguration der Telefonanlage mit dem PC	Eine wichtige Voraussetzung für die erfolgreiche Übertragung Ihrer Konfiguration zur Telefonanlage ist, dass Sie eine Verbindung zwischen PC und Telefonanlage eingerichtet haben. Sie haben die Möglichkeit über die Ethernet-Verbindung LAN.
Konfiguration der Telefonanlage mit dem Telefon	Sie können Ihre Telefonanlage - allerdings eingeschränkt - auch mit einem Telefon programmieren. Hinweise zur Programmierung Ihrer Telefonanlage mit dem Telefon entnehmen Sie bitte der beiliegenden Bedienungsanleitung.
Kurzwahl	Jeder der bis zu 300 Telefonnummern des Telefonbuches kann ein Kurzwahl-Index (000...299) zugeordnet werden. Diesen Kurzwahl-Index wählen Sie dann anstelle der langen Telefonnummer. Beachten Sie dass über die Kurzwahl gewählte Telefonnummern ebenfalls der Wahlregel unterliegen.
LAN	Local Area Network (Lokales Netzwerk)
LAPB	Link Access Procedure Balanced
Lauthören	Funktion bei Telefonen mit eingebauten Lautsprechern: Per Tastendruck können im Raum anwesende Personen ein Telefongespräch mithören.
Layer 1	Schicht 1 des ISO-OSI-Modells, die Bitübertragungsschicht.
LCD	Liquid-Crystal Display (Flüssigkristallbildschirm), ist ein Bildschirm, bei dem spezielle Flüssigkristalle zur Bilddarstellung genutzt werden.
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
Lease Time	Unter "Lease Time" versteht man die Zeit, in der ein Rechner seine ihm zugewiesene IP-Adresse behält, ohne mit dem DHCP-Server "Rücksprache" halten zu müssen.

Letzter Zugriff	Der letzte Zugriff durch den T-Service wird gespeichert und in der Konfiguration angezeigt.
LLC	Link Layer Control
MAC-Adresse	Jedes Gerät im Netz ist über eine feste Hardware-Adresse (MAC-Adresse) definiert. Die Netzwerkkarte eines Geräts bestimmt diese weltweit eindeutige Adresse.
Makeln	Makeln erlaubt es, zwischen zwei externen bzw. internen Gesprächspartnern hin- und her zu schalten, ohne dass der wartende Teilnehmer mithören kann.
Man-in-the-Middle Attack	Die Verschlüsselung mittels öffentlicher Schlüssel setzt den Austausch der öffentlichen Schlüssel voraus. Während des Austausches kann der ungeschützte Schlüssel leicht abgefangen werden und eröffnet so die Möglichkeit eines "man-in-the-middle"-Angriffs. Der Angreifer kann früh seinen eigenen Schlüssel setzen, so dass ein Schlüssel, der dem "man-in-the-middle" bekannt ist, anstelle des eigentlich gewollten Schlüssels des richtigen Kommunikationspartners verwendet wird.
MD5	Siehe HMAC-MD5
Mehrfachrufnummer (MSN)	Multiple Subscriber Number
Mehrgeräteanschluss	Point-to-Multipoint (Punkt-zu-Mehrpunkt)
Mehrgeräteanschluss	Basisanschluss im T-ISDN mit standardmäßig drei Telefonnummern und zwei Leitungen. Der Anschluss der ISDN-Endgeräte erfolgt direkt am Netzabschluss (NTBA) oder am ISDN-Internanschluss einer Telefonanlage.
Mehrgeräteanschluss für die Telefonanlage	Ihre von der T-Com mit der Auftragsbestätigung erhaltenen Mehrfachrufnummern tragen Sie in der Konfiguration in die dort vorgesehenen Tabellenfelder ein. In der Regel erhalten Sie drei Mehrfachrufnummern, können jedoch bis zu zehn Telefonnummern je Anschluss beantragen. Mit der Eintragung der Telefonnummern erfolgt neben der Zuordnung zu einem "Index" gleichzeitig die Zuordnung zu einem Team. Beachten Sie bitte, dass alle Telefonnummern zunächst dem Team 00 zugeordnet werden. In das Team 00 wiederum sind werkseitig die internen Telefonnummern 10, 11 und 20 eingetragen. Anrufe von extern werden somit an den in Team00 eingetragenen Anschlüssen mit den internen Telefonnummern 10, 11 und

	20 signalisiert.
MFV	Mehrfrequenzwahlverfahren
MIB	Management Information Base
Mikrofonstumm- schaltung	Taste zum Abschalten des Mikrofons. Der Gesprächspartner am Telefon kann dann die im Raum geführten Rückfragen nicht mithören.
Mitschneiden von Telefongesprächen	Leistungsmerkmal eines Anrufbeantworters. Erlaubt die Aufnahme eines Gespräches auch während des Telefonats.
Mixed Mode	Der Access Point akzeptiert WPA sowie WPA2.
MLPPP	Multilink-PPP
Modem	Modulator/Demodulator
MPDU	MAC Protocol Data Unit - jedes Informationspaket, das auf dem Funkmedium ausgetauscht wird inclusive Management-Frames und fragmentierten MSDUs.
MPPC	Microsoft Point-to-Point Compression
MPPE	Microsoft Point-to-Point Encryption
MSDU	MAC Service Data Unit - ein Datenpaket, ohne Berücksichtigung von Fragmentierung im WLAN.
MSN	Multiple Subscriber Number
MSSID	Siehe SSID
MTU	Maximum Transmission Unit
Multicast	Eine spezifische Form des Broadcasts, bei dem gleichzeitig eine Nachricht an eine definierte Benutzergruppe übertragen wird.
Multiprotokollgate- way	Gateway, der mehrere Protokolle routen kann, z. B. IP, X.25 etc.
Music On Hold (MOH,Wartemusik)	Ihre Telefonanlage verfügt über zwei interne Wartemusik-Melodien. Bei Auslieferung ist die interne Melodie 1 aktiv. Sie können zwischen den Melodien 1 und 2 wählen oder die Wartemusik inaktiv schalten.
MWI	Übermittlung einer vorliegenden Sprachnachricht aus einer Nachrichtenbox, z. B. T-NetBox oder MailBox an ein entsprechendes

	Endgerät. Der Nachrichteneingang am Endgerät wird z. B. durch eine Leuchtdiode signalisiert.
NAT	Network Address Translation
NDIS WAN	NDIS WAN ist eine Microsoft-Erweiterung dieses Standards in Bezug auf Wide Area Networking (WAN). Der NDIS WAN CAPI-Treiber erlaubt die Nutzung des ISDN-Controllers als WAN-Karte. Der NDIS WAN Treiber ermöglicht die Nutzung eines DFÜ-Netzwerkes unter Windows. NDIS ist die Abkürzung für Network Device Interface Specification und stellt einen Standard für die Anbindung von Netzwerkkarten (Hardware) an Netzprotokolle (Software) dar.
Nebenstelle	Bezeichnet bei Telefonanlagen das mit der Anlage verbundenen Endgerät (z. B. Telefon). Jede Nebenstelle kann auf die Anlagenleistungen zugreifen und mit anderen Nebenstellen kommunizieren.
NetBIOS	Network Basic Input Output System
Netsurfen	"Entdeckungsreise" auf der Suche nach interessanten Angeboten in weit verzweigten Datennetzen wie T-Online. Vor allem bekannt aus der Welt des Internets.
Netz-Direkt (Keypad-Funktionen)	Mit Hilfe der Funktion "Netz-Direkt" (Keypad) können Sie durch die Eingabe einer Tastenfolge auch von Ihrem ISDN- oder analogen Telefon aus aktuelle T-ISDN Funktionen nutzen. Fragen Sie hierzu beim Kundenberater der T-Com nach und lassen Sie sich die entsprechenden Kennziffern geben (z. B. Anrufwefterschaltung in der Vermittlungsstelle).
Netzabschluss (NTBA)	Mit Netzabschluss bezeichnet man in der Telekommunikation den Punkt, an dem einem Endgerät der Zugang zu einem Kommunikationsnetz bereitgestellt wird.
Netzadresse	Eine Netzadresse bezeichnet die Adresse eines gesamten lokalen Netzwerks.
Netzmaske	In einem IP-Netzwerk der zweite Teil der Adresse, mit der sich ein Gerät im Netzwerk identifiziert, z. B. 255.255.255.0. Siehe auch IP-Adresse.
Netzwerk	Ihre Telefonanlage verfügt über einen DSL-Router, damit ein oder mehrere PCs schnell im Internet surfen und downloaden können.
NMS	Network Management Station
Notizbuchfunktion	Während eines Telefonats kann eine Telefonnummer in den Zwi-

schenspeicher des Telefons eingegeben werden, um sie später anzuwählen.

Notrufnummern	Der Fall der Fälle tritt ein und Sie müssen dringend Polizei, Feuerwehr oder eine andere Telefonnummer telefonisch erreichen. Zu allem Überfluss sind alle Anschlüsse belegt. Sie haben jedoch Ihrer Telefonanlage die Telefonnummern mitgeteilt, die im Notfall erreichbar sein müssen. Wählen Sie nun eine dieser Notrufnummern, wird dies von der Telefonanlage erkannt und automatisch ein B-Kanal des T-ISDN für Ihren Notruf freigeschaltet. Notrufe unterliegen keinen Einschränkungen durch Konfigurationen. Ist für einen Anschluss "Telefonieren mit Vorwahlziffer eingestellt", wird der interne Anschluss belegt. Wählen Sie, um nach extern telefonieren zu können, vorab die 0 und dann die gewünschte Notrufnummer.
NT	Network Termination
NTBA	Network Termination for Basic Access
NTP	Network Time Protocol
Nutzkanal	Entspricht einer Telefonleitung im T-Net. Beim T-ISDN sind im Basisanschluss zwei Nutzkanäle mit je 64 KBit/s Datenübertragungsrate enthalten.
OAM	Operations and Maintenance
Offline	Vom englischen "off-line" (ohne Verbindung). Verbindungsloser Betriebszustand, z. B. des PCs.
Online	Vom englischen "on-line" (in Verbindung). Zum Beispiel der Zustand der Verbindung eines PCs mit Datennetzen oder beim Datenaustausch von PC zu PC.
Online Pass	Teil der Zertifizierungsdienste der T-Com für das Internet. Digitaler Ausweis für das Internet. Mit dem OnlinePass kann sich ein Internethalter als Kunde bei einem Unternehmen ausweisen.
Online-Banking	Begriff für die elektronische Kontoführung z. B. über T-Online.
Online-Dienste	Leistungen, die über Kommunikationsdienste wie T-Online und Internet rund um die Uhr verfügbar sind.
Ortsvermittlungsstelle (OVst)	Vermittlungsknoten eines öffentlichen Telefon-Ortsnetzes, der den Anschluss von Endsystemen unterstützt.
OSI-Modell	OSI = Open System Interconnection (offene Kommunikationssysteme)

	me)
OSPF	Open Shortest Path First
PABX	Private Automatic Branch Exchange (Nebenstellenanlage)
Paketvermittlung	Packet Switching
PAP	Password Authentication Protocol
Parken	Das Gespräch wird in der Vermittlungsstelle vorübergehend gehalten. Prinzipieller Unterschied zum Halten: Das Gespräch wird unterbrochen, der Hörer kann z. B. aufgelegt werden. Anwendbar für Makeln. Möglich im T-Net, im T-ISDN und bei Telefonanlagen. Das Endgerät muss mit MFV und R-Taste ausgestattet sein.
PBX	Private Branch Exchange
PCMCIA	Die PCMCIA (Personal Computer Memory Card International Association) ist eine 1989 gegründete Industrievereinigung, die Kreditkartengroße I/O Karten vertritt, wie z. B. WLAN Karten.
PGP	Pretty Good Privacy
PH	Packet Handler
PIN	Persönliche Identifikationsnummer
Ping	Packet Internet Groper
PKCS	Public-Key Cryptography Standards
Port	Ein-/Ausgang
POTS	Plain Old Telephone System
PPP	Point-to-Point Protocol
PPP-Authentisierung	Sicherheitsmechanismus. Authentisierung durch ein Passwort im PPP.
PPPoA	Point to Point Protocol over ATM
PPPoE	Point to Point Protocol over Ethernet
PRI	Primary Rate Interface
Primärmultiplexan-	Teilnehmeranschluss beim ISDN. Der Primärmultiplexanschluss be-

schluss	steht aus einem D-Kanal und 30 B-Kanälen (Europa). (In Amerika: 23 B-Kanäle und ein D-Kanal.) Außer dem Primärmultiplexanschluss gibt es noch den ISDN-Basisanschluss.
Protokoll	Protokolle werden verwendet, um Art und Weise eines Informationsaustausches zwischen zwei Systemen zu definieren. Protokolle steuern und regeln den Ablauf einer Datenkommunikation auf verschiedenen Ebenen (Decodierung, Adressierung, Wegwahl im Netz, Kontrollmechanismen, etc.).
Proxy ARP	ARP = Address Resolution Protocol
Prüfsummenfeld	Frame Check Sequence (FCS)
PSN	Packet Switched Network
PSTN	Public Switched Telephone Network
Punkt-zu-Mehrpunkt	Point-to-Multipoint
Punkt-zu-Punkt	Point-to-Point
PVID	Port VLAN ID
R-Taste	Telefone, die mit der R-Taste (Rückfragetaste) ausgestattet sind, eignen sich auch für den Anschluss an Telefonanlagen. Bei modernen Telefonen löst die R-Taste die Hook-Flash-Funktion aus. Sie ist für die Nutzung der Leistungsmerkmale im T-Net wie Rückfragen/Makeln und Dreierkonferenz erforderlich.
RADIUS	Remote Authentication Dial-In User Service
RADSL	Rate-adaptive Digital Subscriber Line
RAS	Remote Access Service
Raumüberwachung (akustisch)	Um das Leistungsmerkmal "Raumüberwachung" nutzen zu können, muss in dem zu überwachenden Raum das Telefon über eine Kennziffer zur Raumüberwachung freigegeben und der Hörer abgehoben oder Freisprechen eingeschaltet sein. Legen Sie den Hörer des Telefons im zu überwachenden Raum auf oder schalten Sie das Freisprechen aus, ist die Raumüberwachung beendet und das Leistungsmerkmal wieder ausgeschaltet.
Raumüberwachung von externen Telefonen	Mit dieser Funktion kann eine Raumüberwachung von einem externen Telefon aus erfolgen.

Raumüberwachung von internen Telefonen	Sie können von einem internen Telefon Ihrer Telefonanlage einen Raum akustisch überwachen. Die Einrichtung erfolgt mit den in der Bedienungsanleitung beschriebenen Telefonprozeduren. Lesen Sie bitte zu den hier beschriebenen Funktionen auch die entsprechenden Hinweise in der Bedienungsanleitung.
Real Time Clock (RTC)	Hardware-Uhr mit Pufferbatterie
Remote	Entfernt, nicht lokal.
Remote Access	Nicht lokaler Zugriff, siehe Remote.
Remote-CAPI	bintec-eigene Schnittstelle für CAPI.
Repeater	Ein Gerät, das elektische Signale von einer Kabelverbindung zur anderen überträgt, ohne Routing-Entscheidungen zu treffen oder Paketfilterung vorzunehmen. Vergleiche Bridge und Router.
RFC	Spezifikationen, Vorschläge, Ideen und Richtlinien, das Internet betreffend, werden in Form von so genannten RFCs (Request For Comments) veröffentlicht.
Rijndael (AES)	Rijndael (AES) wurde als AES ausgewählt aufgrund der schnellen Schlüsselgenerierung, der niedrigen Speichererfordernisse und der hohen Sicherheit gegenüber Angriffen. Weitere Informationen zu AES, siehe http://csrc.nist.gov/encryption/aes .
RIP	Routing Information Protocol
RipeMD 160	RipeMD 160 ist eine kryptographische Hash-Funktion mit 160 Bit. Es gilt als sichereren Ersatz für MD5 und RipeMD.
RJ45	Stecker bzw. Buchse für maximal acht Adern. Anschluss für digitale Endgeräte.
Roaming	In einem mehrzelligen WLAN können sich Clients frei bewegen und sich bei der Bewegung durch Funkzellen von einem Access Point abmelden und neu auf einem anderen Access Point anmelden, ohne dass der Benutzer dies bemerkt. Diese Fähigkeit wird Roaming genannt.
Router	Geräte, die unterschiedliche Netze auf der Schicht 3 des OSI-Modells verbinden und Informationen von einem Netz in das andere weiterleiten (routen).
RSA	Der RSA-Algorithmus (benannt nach seinen Erfindern Rivest, Sha-

mir, Adleman) basiert auf der Schwierigkeit, große natürliche Zahlen zu faktorisieren. Daher benötigt man eine sehr hohe Datenverarbeitungskapazität und viel Zeit, um einen RSA Schlüssel abzuleiten.

RTSP	Real-Time Streaming Protocol
Rückfrage	Bietet die Möglichkeit, nach dem Anklopfen das erste Gespräch zu halten und ein neues Gespräch entgegenzunehmen.
Rückruf bei Besetzt	Leistungsmerkmal im T-ISDN, in Telefonanlagen und im T-Net. Eine Verbindung wird automatisch hergestellt, sobald der Besetztstatus am Zielanschluss aufgehoben ist. Nach Freiwerden des Anschlusses erfolgt die Signalisierung beim Anrufer. Sobald dieser dann seinen Hörer abhebt, wird die Verbindung automatisch hergestellt. Zuvor muss jedoch der Rückruf vom Anrufer an seinem Endgerät aktiviert werden.
Rückruf bei Nicht-melden	Sie rufen bei einem gewünschten Gesprächspartner an und der Angerufene meldet sich nicht. Mit "Rückruf bei Nichtmelden" ist das für Sie in Zukunft kein Problem. Denn durch diese Komfortleistung stellen Sie die Verbindung jetzt ohne erneute Wahl her. Immer, wenn Sie nicht selbst telefonieren, erfolgt ein erneuter Verbindungsaufbau zum gewünschten Gesprächspartner - maximal 180 Minuten lang.
Rufnummernband	(Durchwahlbereich)
Rufumleitung	Auch: Anrufweiterleitung oder Anrufweiserschaltung. Ein ankommender Anruf wird an einen vorgegebenen Telefon-, Internet- oder Mobilfunkanschluss weitergeleitet.
Rufverteilung	Bei Telefonanlagen Anrufe bestimmten Endgeräten zugeordnet werden.
Rufzustellung bei Besetzt	Ablehnen
Ruhe vor dem Telefon	Anrufschutz
S0-Anschluss	Siehe ISDN-Basisanschluss.
S0-Bus	Sämtliche ISDN-Anschlussdosen und der NTBA beim ISDN-Mehrgeräteanschluss. Jeder So-Bus besteht aus einem vieradrigen Kabel. Die Leitungen/ Kabel übertragen die digitalen ISDN-Signale. Hinter der letzten ISDN-Anschlussdose wird der So-Bus mit einem Abschlusswiderstand terminiert. Der So beginnt beim NTBA und kann bis zu 150 m lang sein. Es lassen sich beliebige ISDN-Geräte

daran betreiben. Gleichzeitig können allerdings immer nur zwei Geräte den So verwenden, da nur zwei B-Kanäle zur Verfügung stehen.

S0-Schnittstelle	International standardisierte Schnittstelle für ISDN-Einrichtungen. Diese Schnittstelle wird netzseitig vom NTBA bereitgestellt. Nutzerseitig ist die Schnittstelle sowohl für den Anschluss einer Telefonanlage (Anlagenanschluss) als auch für den Anschluss von bis zu acht ISDN-Endgeräten (Mehrgeräteanschluss) vorgesehen.
S2M-Anschluss	Siehe Primärmultiplexanschluss.
SAD	Die SAD (=Security Association Database) enthält Informationen über die Sicherheitsvereinbarungen, wie z. B. AH oder ESP Algorithmen und Schlüssel, Sequenznummern, Protokollmodi und SA-Lebensdauer. Für ausgehende IPsec- Verbindungen weist ein SPD-Eintrag auf einen Eintrag im SAD hin, d.h. die SPD legt fest, welche SA angewendet werden muss. Für eingehende IPsec-Verbindungen wird in der SAD abgerufen, wie das Paket weiterverarbeitet werden soll.
SDSL	Symmetric Digital Subscriber Line
Server	Ein Server bietet Dienste an, die von Clients in Anspruch genommen werden. Oft versteht man unter Server einen bestimmten Rechner im LAN, z. B. DHCP-Server.
ServerPass	Teil der Zertifizierungsdienste der T-Com für das Internet. Digitaler Ausweis eines Unternehmens. Mit dem ServerPass bestätigt die T-Com, dass ein Server im Internet zu einem bestimmten Unternehmen gehört und dies durch die Vorlage des Handelsregisterauszugs belegt wurde.
Service 0190	Sprachmehrwertdienst der T-Com zur gewerblichen Verbreitung privater Informationsdienstleistungen. Die Leistungen der T-Com beschränken sich auf die Bereitstellung der technischen Infrastruktur und auf die Abwicklung des Inkassos für die Informationsanbieter. Der Zugang zu den bereitgestellten Informationen erfolgt über die bundesweit einheitliche Telefonnummer 0190 und über eine 6-stellige Telefonnummer. Informationsangebote: Unterhaltung, Wetter, Finanzen, Sport, Gesundheit, Support- und Service-Hotlines.
Service 0700	Sprachmehrwertdienst der T-Com. Ermöglicht die Entgegennahme von Anrufen unter einer bundeseinheitlichen, standortunabhängigen Telefonnummer, die mit den Ziffern 0700 beginnt. Kostenfreie Wei-

terleitung im nationalen Festnetz. Erweiterung mit Vanity möglich.

Service 0900	Sprachmehrwertdienst der T-Com. Löst den Service 0190 ab.
Servicenummer 0180	Sprachmehrwertdienst 0180call der T-Com zur Entgegennahme von Anrufen unter einer bundeseinheitlichen, standortunabhängigen Telefonnummer, beginnend mit den Ziffern 0180.
Setup Tool	Menügesteuertes Tool zur Konfiguration Ihres Gateways. Das Setup Tool kann verwendet werden, sobald ein Zugang zum Gateway (seriell, ISDN-Login, LAN) besteht.
SHA1	Siehe HMAC-SHA.
SHDSL	Single-Pair High-Speed
Shorthold	Bezeichnet die definierte Zeit, nach der eine Verbindung abgebaut wird, wenn keine Daten mehr übertragen werden. Der Shorthold lässt sich statisch (feste Zeit) und dynamisch (in Abhängigkeit von Gebühreninformationen) einrichten.
Sicherungsschicht	Data Link Layer (DLL)
Signalisierung	Signalisierung gleichzeitig: Alle zugeordneten Endgeräte werden gleichzeitig gerufen. Ist ein Telefon besetzt, kann angeklopft werden.
SIP	Session Initiation Protocol
SMS	Short Message Service
SMS Server Telefonnummern	An Ihre Telefonanlage können Sie SMS-fähige Telefone anschließen und damit das Leistungsmerkmal SMS im Festnetz der T-Com nutzen. SMS werden über den SMS Server der T-Com an den jeweiligen Empfänger weitergeleitet. Um eine SMS mit einem SMS-fähigen Endgerät versenden zu können, muss die Telefonnummer 0193010 des SMS Servers der Empfängernummer vorangestellt werden. Diese Telefonnummer ist bereits in Ihrer Telefonanlage gespeichert, so dass sich eine manuelle Eingabe der Server Telefonnummer erübrigt bzw. vom Telefon nicht mitgesendet werden muss. Damit Sie SMS an Ihrem SMS-fähigen Festnetztelefon empfangen können, müssen Sie sich einmalig beim SMS Service der Deutschen Telekom registrieren lassen. Das Senden von SMS ist kostenpflichtig. Das Empfangen von SMS ist kostenfrei.
SMS-Empfang	Haben Sie ein SMS-fähiges Endgerät angeschlossen, können Sie entscheiden, ob für den betreffenden Anschluss der SMS-Empfang

erlaubt sein soll. Werkseitig ist kein SMS-Empfang eingerichtet. Damit Sie mit Ihrem SMS-fähigen Endgerät SMS empfangen können, müssen Sie sich einmalig beim SMS Service der T-Com registrieren. Die einmalige Registrierung ist kostenfrei. Sie schicken einfach eine SMS mit dem Inhalt ANMELD an die Zielrufnummer 8888. Anschließend erhalten Sie vom SMS-Dienst der T-Com eine kostenlose Bestätigung der Registrierung. Mit einer SMS mit dem Inhalt ABMELD an die Zielrufnummer 8888 können Sie Ihr Gerät bzw. Ihre Telefonnummer auch wieder abmelden. Eingehende SMS werden dann vorgelesen. Welche Telefone SMS-fähig sind, erfahren Sie im nächsten T-Punkt, unserer Kundenhotline 0800 330 1000 oder im Internet unter <http://www.t-com.de>.

SNMP	Simple Network Management Protocol
SNMP-Shell	Eingabeebene für SNMP-Kommandos.
SOHO	Small Offices and Home Offices
SPD	Die SPD (=Security Policy Database) definiert die Sicherheitsdienste, die für den IP-Traffic zur Verfügung stehen. Diese Sicherheitsdienste sind abhängig von Parametern wie Quelle und Ziel des Pakets, etc.
Sperrliste (Wahlbereiche)	Sie können für einzelne Teilnehmer eine Einschränkung der externen Wahl festlegen. Die in der Sperrwerk-Tabelle eingetragenen Telefonnummern können von den Endgeräten, die der Wahlkontrolle unterliegen, nicht gewählt werden. z. B. würde der Eintrag 0190 alle Verbindungen zu kostenintensiven Diensteanbietern verhindern.
SPID	Service Profile Identifier
Splitter	Der Splitter trennt am DSL-Anschluss Daten und Sprachsignale.
Spoofing	Technik zur Reduktion des Datenverkehrs (und damit zur Kostensparnis) insbesondere in WANs.
SSID	Als Service Set Identifier (SSID) oder auch Network Name bezeichnet man die Kennung eines Funknetzwerkes, das auf IEEE 802.11 basiert.
SSL	Secure Sockets Layer Eine von Netscape entwickelte, heute standardisierte Technologie, die im allgemeinen dazu verwendet wird, HTTP-Traffic zwischen einem Web Browser und einem Web Server zu sichern.
STAC	Datenkomprimierungsverfahren.

Standardanschluss	T-ISDN Basisanschluss mit den Leistungsmerkmalen Dreierkonferenz, Rückfragen/Makeln und Telefonnummernübermittlung. Im Standardanschluss sind drei Mehrfachrufnummern enthalten.
Statische IP Adresse	Im Gegensatz zu einer dynamischen IP Adresse eine fest eingestellte IP Adresse.
Subadressierung	Neben der Übertragung der ISDN-Telefonnummer können zusätzliche Informationen im Form einer Subadresse bereits beim Verbindungsaufbau über den D-Kanal vom Anrufer zum Angerufenen übertragen werden. Eine über die reine MSN hinausgehenden Adressierung, mit der z. B. mehrere unter einer Telefonnummer erreichbare ISDN-Endgeräte gezielt für einen Dienst angesprochen werden können. In dem angerufenen Endgerät - z.B einem PC - können auch verschiedene Applikationen angesprochen und ggf. ausgeführt werden. Das Leistungsmerkmal ist kostenpflichtig und muss beim Netzbetreiber gesondert beauftragt werden.
Subnetz	Ein Netzwerkschema, das einzelne logische Netzwerke in kleinere physikalische Einheiten teilt.
Subnetz Maske	Eine Methode um mehrere IP Netze in eine Reihe von Untergruppen oder Subnetze zu teilen. Die Maske ist ein Binärmuster, welches mit den IP Adressen im Netz passen muss. Standardmäßig ist die Subnet Mask 255.255.255.0. In diesem Fall können in einem Subnetz 254 verschiedene IP Adressen auftreten, von x.x.x.1 bis x.x.x.254.
Switch	LAN-Switches sind Netzwerkkomponenten, die der Funktion von Bridges oder sogar von Gateways ähnlich sind. Sie vermitteln Datenpakete zwischen Ein- und Ausgangs-Port. Im Gegensatz zu Bridges haben Switches allerdings mehrere Ein- und Ausgangs-Ports. Dadurch erhöht sich die Bandbreite im Netz. Switches können auch eingesetzt werden, um zwischen verschiedenen schnellen Netzen (z. B. 100MBit- und 10MBit-Netzen) zu übersetzen.
synchron	Übertragungsverfahren, bei dem Sender und Empfänger in genau gleichen Zeittakten arbeiten – im Gegensatz zu asynchron. Leerzeichen werden durch eine Pausencodierung überbrückt.
Syslog	Syslog dient als De-facto-Standard zur Übermittlung von Log-Meldungen in einem IP-Netzwerk. Syslog-Meldungen werden als unverschlüsselte Textnachricht über den UDP Port 514 gesendet und zentral gesammelt. Sie werden meist zum Überwachen von Computersystemen benutzt.

Systemtelefone	Zu modernen Telefonanlagen gehörendes Telefon, das – je nach Telefonanlage – mit einer Reihe von Komfortfunktionen und Sonder-tasten ausgestattet ist z. B. das T-Concept PX722.
T-DSL	Produktname der Deutschen Telekom AG für ihre DSL-Dienstleistungen und Produkte.
T-Fax	Produktbezeichnung für die Telefaxgeräte der T-Com.
T-ISDN	Telefonieren, Faxen, Datenübertragung, Online-Dienste - alles über ein Netz und über einen einzigen Anschluss: T-ISDN erschließt Ihnen faszinierende Leistungen mit vielen Vorteilen. Zum Beispiel mit einem Mehrgeräteanschluss - genau die passende Lösung für Familien oder kleine Firmen. Diese Anschlussvariante, bei der bereits die vorhandenen Telefonkabel genutzt werden können, kostet weniger als zwei Telefonanschlüsse, bringt Ihnen aber viel mehr an Qualität und Komfort. Zwei voneinander unabhängige Leitungen, damit Sie auch dann noch telefonieren, ein Fax empfangen oder im Internet surfen können, wenn gerade ein anderes Familienmitglied etwas länger plaudert. Drei oder mehr Telefonnummern, die Sie individuell Ihren Geräten zuordnen und bei Bedarf durch einfache Programmierung wieder anders verteilen können. Wobei man wissen muss, dass die meisten ISDN-Telefone mehrere Telefonnummern "verwalten" können. So lässt sich z. B. ein "zentrales" Telefon im Haushalt einrichten, damit Sie dort auf die Anrufe unter allen ISDN-Telefonnummern reagieren können. Zusätzlich bekommen Fax und Telefon im Arbeitszimmer je eine Telefonnummer - das Telefon für Tochter oder Sohn nicht zu vergessen. So ist jedes Familienmitglied ganz gezielt erreichbar. Ein feiner Komfort, der bestimmt so manchen "Reibungseffekt" beseitigt! Und was die Kosten betrifft, können Sie auf Wunsch in Ihrer Rechnung getrennt ausweisen lassen, welche Tarifeinheiten sich auf welcher ISDN-Telefonnummer summieren haben.
T-Net	Das digitale Telefonnetz der T-Com zum Anschluss analoger Endgeräte.
T-NetBox	Der Anrufbeantworter im T-Net und im T-ISDN. Die T-NetBox speichert bis zu 30 Nachrichten.
T-NetBox Telefonnummer	Tragen Sie hier die aktuelle T-NetBox-Telefonnummer ein, falls diese von der werkseitig eingetragenen 08003302424 abweicht. Sobald eine Sprach- oder Faxnachricht in Ihrer T-NetBox eingegangen ist, wird eine Benachrichtigung an Ihre Telefonanlage gesendet.
T-Online	Oberbegriff für die Online-Plattform der T-Com. Mit Leistungen wie

	E-Mail und Zugang zum Internet.
T-Online Software	Softwaredecoder der T-Com für alle gängigen Computersysteme, der den Zugang zu T-Online ermöglicht. Unterstützt alle Funktionen wie KIT, E-Mail und Internet mit einem Browser. Diese Software erhalten alle T-Online Nutzer kostenlos.
T-Service	Der T-Service führt sämtliche Installationsarbeiten und Konfigurationen der Telefonanlagen im Auftrag des Kunden aus. Durch Instandhaltungs- und Instandsetzungsarbeiten sorgt er jederzeit für eine optimale Gesprächs- und Datenübertragung.
T-Service Zugang	Der T-Service Zugang bietet Ihnen die Möglichkeit, Ihre Telefonanlage vom T-Service konfigurieren zu lassen. Rufen Sie den T-Service an! Lassen Sie sich beraten und geben Sie Ihre Konfigurationswünsche an. Der T-Service konfiguriert dann Ihre Telefonanlage aus der Ferne ohne Ihr weiteres Zutun.
TA	Terminal Adapter
TAE	Telekommunikationsanschlusseinheit
Tag/Nacht/Kalender	Sie legen fest, wie die Umschaltung der Anrufvariante Tag/Nacht erfolgen soll.
TAPI	Telephony Applications Programming Interface
TAPI-Konfiguration	Mit der TAPI-Konfiguration können Sie den TAPI-Treiber dem Programm, das diesen Treiber nutzt, anpassen. Sie können überprüfen, welche MSN einem Endgerät zugeordnet ist, können einen neuen Leitungsnamen festlegen und die Wählparameter einstellen. Konfigurieren Sie zuerst Ihre Telefonanlage. Anschließend müssen Sie die TAPI-Schnittstelle konfigurieren. Benutzen Sie das Programm "TAPI-Konfiguration".
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Terminal Equipment
TEI	Terminal Endpoint Identifier
Teilnehmer Name	Um Anschlüsse einfacher zu unterscheiden, können Sie für jeden internen Teilnehmer einen Teilnehmer-Namen vergeben.
Telefax	Bezeichnung für Fernkopieren zur originalgetreuen Übertragung von

Texten, Grafiken und Dokumenten über das Telefonnetz.

Telefonanlage	Der Leistungsumfang einer Telefonanlage ist herstellerspezifisch und ermöglicht unter anderem den Betrieb von Nebenstellen, kostenlose Interngespräche, Rückruf bei Besetzt und Konferenzschaltungen. Telefonanlagen übernehmen z. B. die Bürokommunikation (Sprach-, Text- und Datenübertragung).
Telefonbuch	Die Telefonanlage verfügt über ein internes Telefonbuch. Sie können bis zu 300 Telefonnummern mit den dazugehörigen Namen speichern. Auf das Telefonbuch der Telefonanlage können Sie mit einem funkwerk-Gerät (z. B. CS 410) zugreifen. Über die Konfigurationsoberfläche fügen Sie dem Telefonbuch Einträge hinzu.
Telematik	Telematik bezeichnet eine Kombination aus Telekommunikation und Computertechnik und beschreibt die Datenkommunikation zwischen Systemen und Geräten.
Telnet	Protokoll aus der TCP/IP-Protokollfamilie. Telnet ermöglicht die Kommunikation mit einem anderen entfernten Gerät im Netzwerk.
Terminaladapter	Gerät zur Schnittstellenanpassung. Hierdurch wird der Anschluss von unterschiedlichem Equipment an das T-ISDN ermöglicht. So dient der Terminaladapter a/b zum Anschluss analoger Endgeräte an die S0-Schnittstelle des ISDN-Basisanschlusses. Bereits vorhandene analoge Endgeräte mit Tonwahl können weiter betrieben werden.
TFE	Türfreisprecheinrichtung. Sie lässt sich an verschiedene Telefonanlagen anschalten. Über ein Telefon kann ein Türgespräch geführt und die Tür geöffnet werden.
TFE am analogen Anschluss	Ein analoger Anschluss kann für die Anschaltung eines Funktionsmoduls M06, zur Anschaltung einer Türfreisprecheinrichtung DoorLine eingerichtet werden.
TFE-Adapter	Das Funktionsmodul kann an einem analogen Anschluss Ihrer Telefonanlage installiert werden. Ist an Ihre Telefonanlage eine TFE (DoorLine) über ein Funktionsmodul angeschaltet, können Sie von jedem berechtigten Telefon aus mit einem Besucher an der Tür sprechen. Jedem Klingeltaster können Sie bestimmte Telefone zuordnen, die dann beim Betätigen des Klingeltasters klingeln. Die Signalisierung erfolgt bei analogen Telefonen im Takt des Türstellenrufes. Anstelle der internen Telefone kann auch ein externes Telefon für den Klingeltaster als Rufziel konfiguriert werden. Ihre Türsprechstelle kann bis zu 4 Klingeltaster besitzen. Der Türöffner kann

	während eines Türgespräches betätigt werden. Eine Betätigung ohne Türgespräch ist nicht möglich.
TFTP	Trivial File Transfer Protocol
Tiger 192	Tiger 192 ist ein relativ neuer und sehr schneller Hash-Algorithmus.
TK-Anlage	Telekommunikationsanlage
TLS	Transport Layer Security
Tonwahl	Mehrfrequenzwahlverfahren (MFV)
TTL	TTL bedeutet Time to Live und beschreibt die Zeit, in der ein Datenpaket zwischen den einzelnen Servern hin und her geschickt wird, bevor es verworfen wird.
Twofish	Twofish war ein möglicher Kandidat für AES (Advanced Encryption Standard). Er wird als ebenso sicher wie Rijndael (AES) angesehen, ist jedoch langsamer.
U-ADSL	Universal Asymmetric Digital Subscriber Line
Übertragungsrate	Die Anzahl der Bits pro Sekunde, die im T-Net oder im T-ISDN vom PC oder Faxgerät aus übertragen werden. Faxgeräte erreichen bis zu 14,4 KBit/s, Modems bis zu 56 KBit/s. Im ISDN ist Daten- und Fauxaustausch mit 64 KBit/s möglich. Bei T-DSL können bis zu 8 MBit/s empfangen und bis zu 768 KBit/s gesendet werden.
UDP	User Datagram Protocol
Umschaltbares Wahlverfahren	Möglichkeit, durch Schalter oder Tasteneingabe an Endgeräten wie Telefon oder Faxgerät zwischen Impulswahlverfahren und Mehrfrequenzwahlverfahren zu wechseln.
Umstecken am Bus (Parken)	Ermöglicht beim Mehrgeräteanschluss während des Telefongespräches das Umstecken der Endgeräteverbindung in eine andere ISDN-Anschlussdose.
Unterdrückung der Telefonnummer	Leistungsmerkmal in Telefonanlagen. Die Anzeige der Telefonnummer lässt sich fallweise ausschalten.
Update	Aktualisierung eines Softwareprogramms (Firmware der Telefonanlage). Ein Update ist die aktualisierte Version eines vorhandenen Softwareproduktes; man erkennt es an der geänderten Versionsnummer.

Upload	Datentransfer bei Online-Verbindungen, wobei Dateien von dem eigenen PC auf einen anderen PC oder zu einem Datennetzserver übertragen werden.
UPnP	Universal Plug and Play
Upstream	Datenübertragungsrate vom Kunden zum ISP.
URL	Universal/Uniform Resource Locator
USB	Universal Serial Bus
UUS1 (User to User Signalling 1)	Diese Funktion ist nur für Systemtelefone und ISDN-Telefone möglich.
V.11	ITU-T-Empfehlung für symmetrische Doppelstrom-Schnittstellenleitungen (bis zu 10 MBit/s).
V.24	CCITT- und ITU-T-Empfehlung, die die Schnittstelle zwischen einem Computer oder Terminal als Datenendeinrichtung (DTE) und einem Modem als Datenübertragungseinrichtung (DCE) definiert.
V.28	TU-T-Empfehlung für unsymmetrische Doppelstrom-Schnittstellenleitung.
V.35	ITU-T-Empfehlung für Datenübertragung mit 48 kBit/s im Bereich von 60 bis 108 kHz.
V.36	Modem für V.35.
V.42bis	Datenkomprimierungsverfahren.
V.90	ITU-Standard für 56 kBit-Analogmodems. Im Gegensatz zu den älteren V.34-Modems werden mit dem V.90-Standard Daten digital zum Kunden weitergesendet und müssen auf einer Modemseite (Provider) nicht zuerst von digital in analog umgewandelt werden, wie es bei V.34-Modems und früheren der Fall ist. Dadurch sind höhere Übertragungsraten möglich. Eine maximale Geschwindigkeit von 56 kBit/s kann nur unter optimalen Umständen erreicht werden.
Vanity	Buchstabenwahl
Variante Tag - Nacht	Sie möchten wichtige Anrufe für Ihr Home-Office nach Feierabend automatisch auf einen Anrufbeantworter umleiten, damit Sie nicht gestört werden? Dieses können Sie mit der Anrufzuordnung realisieren. Sie können jedem Teilnehmer zwei verschiedene Rufverteilungen (Anrufzuordnung Tag und Anrufzuordnung Nacht) zuweisen. In

den Anrufzuordnungen ist auch eine Anrufweitschaltung zu einem externen Teilnehmer einrichtbar, so dass Sie jederzeit erreichbar sein können. In der Anrufzuordnung Tag und Nacht wird also festgelegt, welche internen Endgeräte bei einem Anruf von extern klingeln sollen. Die Anrufzuordnung Tag und Nacht ist eine Tabelle, in der die ankommenden Rufe internen Teilnehmern zugeordnet werden.

VDSL	Very High Bit Rate Digital Subscriber Line (auch als VADSL oder BDSL bezeichnet)
Vermittlungsstelle	Knotenpunkt im öffentlichen Telekommunikationsnetz. Man unterscheidet zwischen Ortsvermittlungsstellen und Fernvermittlungsstellen.
VID	VLAN ID
VJHC	Van-Jacobsen-Header-Komprimierung
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
VSS	Virtual Service Set
Wahlkontrolle	Sie können in der Konfiguration für bestimmte Endgeräte eine Einschränkung der externen Wahl festlegen.
Wählverbindung	Eine Verbindung wird bei Bedarf durch Wählen einer Rufnummer aufgebaut, im Gegensatz zu einer Festverbindung.
Wahlvorbereitung	Bei einigen Telefonen mit Display kann man eine Telefonnummer zuerst eingeben, noch einmal kontrollieren und danach wählen.
WAN	Wide Area Network
WAN-Interface	WAN-Schnittstelle.
WAN-Partner	Gegenstelle, die über das WAN, z. B. ISDN, erreicht wird.
Wartemusik (Music On Hold, MOH)	Leistungsmerkmal bei Telefonanlagen. Während der Rückfrage oder des Weiterverbindens wird eine Melodie eingespielt, die der Wartende hört. Ihre Telefonanlage verfügt über zwei interne Melodien zur Auswahl.
Webmail	Dienst von T-Online, mit dem über einen Browser im Internet weltweit E-Mails versendet und empfangen werden können.

Webserver	Server, der Dokumente im HTML-Format zum Abruf über das Internet bereithält (WWW).
Wechselsprechen (nur ISDN-Teilnehmer)	Dieser Anschluss ist für ein ISDN-Telefon (nur Systemtelefone T-Concept PX722) mit Wechselsprechfunktion nutzbar. Rufen Sie ein ISDN-Telefon mit Wechselsprechfunktion an, schaltet dieses automatisch die Funktion Lauthören ein, damit sofort ein Gespräch erfolgen kann. Bitte beachten Sie die Hinweise in der Bedienungsanleitung des Telefons zur Funktion Wechselsprechen.
WEP	Wired Equivalent Privacy
Westernstecker	(auch RJ-45-Stecker) Für ISDN-Endgeräte verwendeter Stecker mit acht Kontakten. Von der US-Telefongesellschaft Western Bell entwickelt. Westerntelefonstecker für analoge Telefone haben vier oder sechs Kontakte.
WINIPCFG	Ein grafisches Tool unter Windows 95, 98 und Millennium, das die Win32 API verwendet, um IP Adresskonfiguration von Rechnern anzusehen und zu konfigurieren.
WLAN	Eine Gruppe von Computern, die drahtlos miteinander vernetzt sind (FunkLAN).
WMM	Wireless Multimedia
WPA	Wi-Fi-Protected Access
WPA - Enterprise	Wendet sich v. a. an die Bedürfnisse von Unternehmen und bietet sichere Verschlüsselung und Authentisierung. Verwendet 802.1x und das Extensible Authentication Protocol (EAP) und bietet damit eine effektive Möglichkeit der Anwender-Authentisierung.
WPA - PSK	Wendet sich an Privat-Anwender oder kleine Unternehmen, die keinen zentralen Authentisierungsserver betreiben. PSK steht für Pre-Shared Key und bedeutet, dass AP und Client eine feste, allen Teilnehmern bekannte beliebige Zeichenfolge (8 bis 63 Zeichen) als Basis für die Schlüsselberechnung im Funkverkehr verwenden.
WWW	World Wide Web
X.21	Die Empfehlungen aus X.21 definieren die physikalische Schnittstelle zwischen zwei Netzwerkkomponenten in einem Paketvermittlungnetz (z. B. Datex-P).
X.21bis	Die Empfehlungen aus X.21bis definieren die DTE/DCE-Schnittstelle zu synchronen Modems der V-Serie.

X.25	Protokoll, das die Schnittstelle von Netzwerkkomponenten zu einem Paketvermittlungsnetz definiert.
X.31	ITU-T-Empfehlung zur Integration von X.25-fähigen DTEs in ISDN (D-Kanal).
X.500	ITU-T Standards, die Benutzerverzeichnisdienste abdecken, vergleiche: LDAP. Beispiel: Das Telefonbuch ist das Verzeichnis, in dem man Personen anhand des Namens findet (anhand der Übereinstimmung mit dem Telefonverzeichnis). Das Internet unterstützt mehrere Datenbanken mit Informationen über Anwender, wie z. B. Email-Adressen, Telefonnummern und Postanschrift. Diese Datenbanken können durchsucht werden, um Informationen über einzelne Personen zu erhalten.
X.509	ITU-T Standards, die das Format der Zertifikate und Zertifikatanfragen und deren Verwendung definieren.
Zentraler Kurzwahl-speicher	Leistungsmerkmal von Telefonanlagen. Telefonnummern werden in der Telefonanlage gespeichert und können dann mit einer Tastenkombination von jedem angeschlossenen Telefon aus aufgerufen werden.
Zielwahlspeicher	Kurzwahlspeicher
Zugangscod	PIN oder Passwort
Zugriffsschutz	Über Filter kann verhindert werden, dass Außenstehende AUF die Daten der Rechnern Ihres LAN zugreifen können. Diese Filter stellen eine Basisfunktion einer Firewall dar.
Zuordnung	Ein externer Anruf kann bei internen Teilnehmern signalisiert werden. Die Einträge in der Variante "Tag" und der "Variante Nacht" können unterschiedlich sein.

Index

- 305 , 327
- Initialisierungssequenz des Modems
163
- Überwachte IP-Adresse 476
- #
- # 522 , 523 , 529 , 531
- #1, #2, #3 389
- A**
- Abfrage Intervall 261
- ACCESS_ACCEPT 151
- ACCESS_REJECT 151
- ACCESS_REQUEST 151
- ACCOUNTING_START 151
- ACCOUNTING_STOP 151
- ACL-Modus 222
- Administrativer Status 426
- Administrativer Status 333 , 412 , 420
, 428
- Adressbereich 405
- Adresse 405
- Adressmodus 193 , 309
- Adresstyp 405
- ADSL-Chipsatz 180
- ADSL-Logik 500
- ADSL-Modus 181
- ADSL-Sync-Type 181
- Aktion 229 , 229 , 397 , 463 , 500 ,
523 , 529
- Aktion auswählen 471
- Aktion wenn Lizenz nicht registriert
460
- Aktion wenn Server nicht erreichbar
460
- aktiv 266
- Aktiv-Überprüfung 524
- Aktive IPSec-Tunnel 127
- Aktive Sitzungen 127
- Aktualisierung aktivieren 450
- Aktualisierungs-URL 471
- Aktualisierungsintervall 452 , 519
- Aktualisierungspfad 452
- Aktualisierungstimer 253
- Aktuelle Geschwindigkeit/Aktueller Mo-
dus 166
- Aktuelle Systemprotokolle 128
- Aktuelle Systemzeit 134
- Aktueller Dateiname im Flash 500
- Alle Multicast-Gruppen 259
- Allgemeiner Name 387
- Andere Inaktivität 402
- Angerufene Adresse 426 , 430
- Angerufene Leitung 430
- Anrufende Adresse 426
- Anrufende Leitung 426
- Antenna Diversity 203
- Antwort 443
- Antwortintervall (Letztes Mitglied) 261
- Anzahl der Wählversuche 486
- Anzahl Nachrichten 513
- AP MAC Adresse 229
- AP-MAC-Adresse 538 , 538
- APN (Name des Access-Points) 163 ,
190
- Arbeitsspeichernutzung 127
- ARP Processing 219
- Association Advantage 212
- ATM PVC 280
- ATM-Dienstkategorie 312
- ATM-Schnittstelle 183 , 307
- Auf Client-Anfrage antworten 493
- Auf der Black List 465
- Auf der White List 465
- Ausgehende ISDN-Nummer 339 ,
377
- Ausgehende Leitung 428
- Ausgehende Nummer 485
- Ausgehender Proxy 420
- Ausgewählte Kanäle 212
- Ausgewählte Ports 378
- Aushandlungsmodus 524

Ausstehende Ende-
 zu-Ende-Anforderungen 316
 Ausstehende Segment-Anforderungen
 316
 Auswahl 406
 Authentifizierung 272 , 277 , 282 ,
 288 , 296 , 301 , 367 , 375
 Authentifizierung für PPP-Einwahl
 160
 Authentifizierungs-ID 416 , 420
 Authentifizierungsmethode 343 , 524
 Authentifizierungspasswort 489
 Authentifizierungstyp 153 , 157
 Automatische Ablehnung 240
 Automatische Konfiguration beim
 Start 169
 Autospeichermodus 389
 AUX-Portstatus 163

B

Bandbreite angeben 400
 Basierend auf Ethernet-Schnittstelle
 193
 Beacon Period 209
 Benachrichtigungsdienst 511
 Benutzerdefiniert 387
 Benutzerdefinierte Zeitschlitze 172
 Benutzername 269 , 275 , 280 , 285 ,
 294 , 299 , 365 , 372 , 420 , 450 ,
 468 , 511
 Berücksichtigen 255
 Beschreibung 175 , 269 , 275 , 280 ,
 285 , 294 , 299 , 307 , 320 , 323 ,
 326 , 333 , 343 , 351 , 360 , 365 ,
 372 , 380 , 383 , 393 , 404 , 405 ,
 406 , 407 , 410 , 412 , 416 , 420 ,
 426 , 430 , 432 , 443 , 457 , 471 ,
 523 , 524 , 529 , 531
 Beschreibung des Client Links 229 ,
 538
 Betriebsmodus 203
 Blockieren nach Verbindungsfehler
 für 272 , 277 , 282 , 288 , 296 ,
 301 , 367 , 375

blockiert 266
 Blockzeit 158 , 348
 BOSS 500
 BOSS-Version 127
 Bündeltyp 175

C

CA-Zertifikat 385
 CA-Zertifikate 348
 Cache-Größe 440
 Cache-Treffer 448
 Cache-Trefferrate (%) 448
 Callback 377
 Callback-Modus 288 , 301
 Channel Sweep 212
 Client MAC-Adresse 534
 Client-Modus 203
 Client-Typ 311
 Code 407
 Codec-Vorschlagssequenz 418 , 423
 Continuity Check (CC) Ende-zu-Ende
 317
 Continuity Check (CC) Segment 317
 CPU-Nutzung 127
 CRLs senden 358
 CTS Frames als Antwort auf RTS emp-
 fangen 531
 CW Max 209
 CW Max. 212
 CW Min 209
 CW Min. 212

D

Datei auswählen 500
 Dateikodierung 390 , 391
 Dateiname 500
 Datenrate Mbit/s 533 , 534 , 535 , 537
 , 538 , 538
 Datenverkehrspriorität 397
 Datum 522
 Dauer 527 , 528
 Details 523
 DH-Gruppe 343

- DHCP-Hostname 195 , 309
 - DHCP-MAC-Adresse 195 , 309
 - DHCP-Optionen 455
 - Dienst 178 , 242 , 397 , 527 , 528
 - Dienstmerkmal 178
 - Discovery Server freigeben 491
 - DNS-Anforderungen 448
 - DNS-Aushandlung 272 , 277 , 282 , 292 , 296 , 301 , 368 , 376
 - DNS-Server 445
 - DNS-Serverkonfiguration 439
 - DNS-Test 497
 - Domäne 445
 - Domänenname 439
 - Doppelt empfangene MSDUs 531
 - Downstream 181
 - Drahtloser Modus 208
 - Dritter Zeitserver 135
 - DSA-Schlüsselstatus 148
 - DSCP-/TOS-Wert 235
 - DSP-Modul 128
 - DTIM Period 209
 - Dynamische
 - RADIUS-Authentifizierung 357
- E**
- E-Mail 387
 - E-Mail-Adresse des Absenders 511
 - Echounterdrückung 419 , 424
 - ED Threshold 209 , 212
 - Eigene IP-Adresse per ISDN übertragen 339
 - Eingehende ISDN-Nummer 339 , 377
 - Eingehende Nummer 485
 - Eingehender Diensttyp 163 , 190
 - Eintrag aktiv 153 , 157
 - Einträge 291 , 304
 - Empfangene DNS-Pakete 448
 - Empfänger 513
 - Ende-zu-Ende-Sendeintervall 316
 - Endpunkttyp 414
 - Enkapsulierung 307
 - Entfernt Nummer 528
 - Entfernte GRE-IP-Adresse 380
 - Entfernte IP-Adresse 362 , 523
 - Entfernte IP-Adresse / Netzmaske 242
 - Entfernte MAC 535 , 537
 - Entfernte MAC-Adresse 225
 - Entfernte Netzwerke 523
 - Entfernte Nummer 527
 - Entfernte PPTP-IP-Adresse 277 , 372
 - Entfernter Benutzer (nur Einwahl) 285
 - Entfernter Hostname 360
 - Entfernter Port 414
 - Entferntes Netzwerk 242
 - Entfernung 209
 - Enthaltene Zeichenfolge 513
 - Entsprechender NAT-Eintrag für ausgehende Verbindung 242
 - Erfolgreich beantwortete Anfragen 448
 - Erfolgreich empfangene Multicast-MS-DUs 531
 - Erfolgreich übertragene Multicast-MS-DUs 531
 - Ergebnis der automatischen Konfiguration 169
 - Erkennungsmodus 187
 - Erlaubte Adressen 222
 - Erreichbarkeitsprüfung 154 , 348 , 354
 - Erweiterte Route 233
 - Erzeugung von Hintergrundrauschen (Comfort Noise Generation, CNG) 419 , 424
 - Escape-Zeichen des Modems 163
 - Ethernet-Schnittstellenauswahl 166
 - Externe Adresse 432
 - Externe IP-Adresse 242
 - Externer Dateiname 390 , 391
 - Externer Port 414
- F**
- Facility 506
 - Fehler 526
 - Fehlerhafte Empfangene Pakete 531
 - Filterregeln 400

Firewall Status 402
 Fragmentation Threshold 209 , 212
 Frame-Übertragung ohne ACK 531
 Frames ohne Tag verwerfen 198
 Frequenzband 203
 Funkmodul 203
 Für DNS-/WINS-Serverzuordnung zu
 verwendende IP-Adresse 440

G

Garbage Collection Timer 253
 Gateway 233 , 455 , 489
 Gefilterte EingangsSchnittstelle(n)
 460
 Gerätemodus 183
 Gesamt 526
 GPRS/UMTS-Schnittstelle 294
 GRE-Window-Anpassung 378
 GRE-Window-Größe 378
 Größe der Zero Cookies 357
 Gruppen-ID 476 , 477
 Gruppenbeschreibung 255
 Gültigkeit 416 , 420

H

Hashing-Algorithmen 147
 Hello-Intervall 362
 Hold Down Timer 253
 Host 445
 Host zuweisen 244
 Hostname 450
 HTTP 143
 HTTPS 143

I

IEEE 802.11d-Konformität 203
 IGMP Proxy 263
 IGMP-Status 264
 IKE (Phase 1) 526
 IKE (Phase 1) SAs 524
 Immer aktiv 269 , 275 , 280 , 285 ,
 294 , 299 , 365 , 372
 inaktiv 266

Informationen senden an 519
 Initial Contact Message senden 357
 Initialisierungssequenz des Modems
 190
 Interface Leads 187
 Interne IP-Adresse 414
 Interner Port 414
 Interner Zeitserver 135
 Intervall 478 , 482 , 483
 Intra-cell Repeating 219
 IP-Accounting 508
 IP-Accounting Meldungs-Format 509
 IP-Adressbereich 455
 IP-Adresse 250 , 309 , 310 , 443 ,
 457 , 489 , 506 , 518 , 533 , 534
 IP-Adresse / Netzmaske 193
 IP-Adressenvergabe 334
 IP-Adressmodus 271 , 276 , 281 , 287
 , 295 , 300 , 366 , 373
 IP-Komprimierung 354
 IP-Poolbereich 306 , 355
 IP-Poolname 306 , 355
 IP-Zuordnungspool 287 , 300 , 334
 IP-Zuordnungspool (IPCP) 366 , 373
 IPSec (Phase 2) 526
 IPSec aktivieren 356
 IPSec-Debug-Level 356
 IPSec-Tunnel 525
 ISDN Verwendung Extern 127
 ISDN Verwendung Intern 127
 ISDN-Diebstahlsicherungsdienst 485
 ISDN-Konfigurationstyp 169
 ISDN-Leitungsrahmenstruktur 172
 ISDN-Port 178
 ISDN-Switch-Typ 169 , 172

K

Kanal 203 , 229 , 527
 Kanalauswahl 172
 Kanalbündelung 290
 Kanäle scannen 212
 Kategorie 463
 Key Hash Payloads senden 358
 Knotenname 489

Komprimierung 146 , 321 , 324
 Konfigurationsschnittstelle 142
 Konfigurierte Geschwindigkeit/konfigurierter Modus 166
 Kontakt 130
 Kontrollmodus 329
 Kosten 527 , 528
 Kurzwahl 436

L

Land 387
 Layer 4-Protokoll 235
 Layer-2-Modus 187
 LCP-Erreichbarkeitsprüfung 272 , 277 , 282 , 296 , 301 , 321 , 324 , 327 , 367 , 375
 LDAP-URL-Pfad 393
 Lease Time 455
 Lebensdauer 343 , 351
 Leitungsgeschwindigkeit 163
 Leitungsgeschwindigkeitsintervall 183
 Leitungsmodus 183
 Letztes Schreibergebnis 489
 Level 506 , 522
 Lizenz gültig bis 462
 Lizenz-Status 462
 Lizenzschlüssel 139 , 462
 Lizenzseriennummer 139
 Lokale Adresse 432
 Lokale GRE-IP-Adresse 380
 Lokale ID 524
 Lokale IP-Adresse 233 , 271 , 276 , 281 , 287 , 295 , 300 , 320 , 323 , 326 , 334 , 362 , 366 , 373 , 380 , 524
 Lokale PPTP-IP-Adresse 277
 Lokale Zertifikatsbeschreibung 390 , 391
 Lokaler Hostname 360
 Lokaler ID-Typ 343
 Lokaler ID-Wert 343
 Lokales Zertifikat 343
 Long Retry Limit 209 , 212
 Loopback Ende-zu-Ende 316

Loopback-Segment 316
 Löschen/Editieren von allen Routing-Einträgen erlauben 239
 Low Latency Transmission 412

M

MAC-Adresse 193 , 309 , 457 , 489 , 533
 Mail-Exchanger (MX) 451
 Max Receive Lifetime 209
 Max Transmit MSDU Lifetime 209
 Max. Link-Entfernung 203
 Max. Receive Lifetime 212
 Max. Transmit MSDU Lifetime 212
 Max. Übertragungsrate 208
 Max. Zeitraum aktiver Scan 212
 Max. Zeitraum passiver Scan 212
 Maximale Antwortzeit 261
 Maximale Anzahl der Accounting-Protokolleinträge 130
 Maximale Anzahl der Einträge im Verlauf 460
 Maximale Anzahl der erneuten Einwählversuche 272 , 277 , 282 , 288 , 296 , 301
 Maximale Anzahl der IGMP-Statusmeldungen 261 , 264
 Maximale Anzahl der Syslog-Protokolleinträge 130
 Maximale Anzahl Wiederholungen 362
 Maximale Burst-Größe (MBS) 312
 Maximale Gruppen 264
 Maximale Nachrichtenzahl pro Minute 511
 Maximale Quellen 264
 Maximale TTL für negative Cacheeinträge 440
 Maximale TTL für positive Cacheeinträge 440
 Maximale Upload-Geschwindigkeit 329
 Maximale Upstream-Bandbreite 181
 Maximale Zeit zwischen Versuchen

362
 Maximales Nachrichtenlevel von Systemprotokolleinträgen 130
 Mbit/s 530
 Media Stream Termination 434
 Metrik 233
 Metrik-Offset für Aktive Schnittstellen 250
 Metrik-Offset für Inaktive Schnittstellen 250
 Min. Zeitraum aktiver Scan 212
 Min. Zeitraum passiver Scan 212
 Minimale Zeit zwischen Versuchen 362
 Mitglieder 404 , 410
 Modus 229 , 235 , 238 , 261 , 264 , 291 , 304 , 339 , 343 , 385
 Modus / Bridge-Gruppe 142
 Modus des D-Kanals 339
 MSDUs, die nicht übertragen werden konnten 531
 MSN 178
 MSN-Erkennung 178
 MTU 380 , 524
 Multicast-Gruppen-Adresse 259

N

Nachricht 522
 Nachrichten 524
 Nachrichtenkomprimierung 513
 Nachrichtentyp 506
 Name der Quelldatei 500
 Name der Zieldatei 500
 NAT aktiv 240
 NAT-Eintrag erstellen 271 , 276 , 281 , 287 , 295 , 300 , 366 , 373
 NAT-Traversal 348
 Negativer Cache 440
 Netzmaske 233 , 250 , 309 , 310 , 366 , 489
 Netzwerkname (SSID) 219 , 226 , 229
 Netzwerkqualität 190
 Netzwerktyp 233

Neue Zeit 135
 Neuer Dateiname 500
 Neues Datum 135
 Nicht entschlüsselbare MPDU erhalten 531
 Nicht geändert für 529
 Nicht-Mitglieder verwerfen 198
 Nitro Modus 208
 Nitro XM 208
 Nutzungsart 288 , 301
 Nutzungsbereich 203

O

OAM-Fluss-Level 315
 Organisation 387
 Organisationseinheit 387
 OSPF-Modus 292 , 321 , 324 , 327 , 368 , 376

P

Packetgröße 419 , 424
 Passwort 269 , 275 , 280 , 285 , 294 , 299 , 360 , 365 , 372 , 385 , 390 , 391 , 416 , 420 , 450 , 468 , 500 , 511 , 519
 Passwörter und Schlüssel als Klartext anzeigen 133
 Peak Cell Rate (PCR) 312
 Peer-Adresse 333
 Peer-ID 333
 Penalty-Wert 212
 PFS-Gruppe verwenden 351
 Phase-1-Profil 335
 Phase-2-Profil 335
 Physikalische Schnittstelle - Schnittstellendetails - Link 128
 Physikalische Verbindung 180
 Ping 143
 Ping-Test 496
 PMTU propagieren 354
 Poisoned Reverse 251
 Pool-Verwendung 455
 POP3-Server 511

POP3-Timeout 511
 Port 242 , 452
 Port-Verwendung 169 , 172 , 291 ,
 304
 Portname 169 , 172
 Portweiterleitungen 240
 Positiver Cache 440
 PPPoE-Ethernet-Schnittstellen 269
 PPPoE-Mode 269
 PPPoE-Schnittstelle für Mehrfachlinks
 269
 PPTP-Adressmodus 277
 PPTP-Inaktivität 402
 PPTP-Modus 372
 PPTP-Passthrough 240
 PPTP-Schnittstelle 275
 Preshared Key 220 , 227 , 333
 Primär 439 , 439
 Primärer DHCP-Server 458
 Primärer Zeitserver 135
 Priorität 153 , 157 , 428
 Privaten Schlüssel generieren 385
 Proposals 343 , 351
 Protokoll 242 , 407 , 412 , 414 , 416 ,
 420 , 452 , 506
 Protokollierte Aktionen 402
 Protokollierungslevel 146
 Provider 307 , 450
 Providername 452
 Proxy ARP 195
 Proxy-ARP 336
 Proxy-ARP-Modus 292 , 305 , 321 ,
 324 , 327 , 368 , 376
 Proxy-Schnittstelle 263
 PVID 198

Q

QoS anwenden 397
 Quell-IP-Adresse 235 , 478 , 482 ,
 483
 Quelle 397 , 471 , 500
 Quellport 235
 Quellportbereich 407
 Quellschnittstelle 235 , 259

R

RA-Signierungszertifikat 385
 RA-Verschlüsselungszertifikat 385
 RADIUS-Dialout 154
 RADIUS-Passwort 153
 Rate 534 , 537 , 538
 Rauschen dBm 533 , 534 , 535 , 537 ,
 538 , 538
 Realm 420
 Region 230
 Registrar 420
 Registrierung 416 , 420
 Regulierte Schnittstellen 478
 Reinigen 5
 Retransmission Timer 253
 RFC 2091-Variabler Timer 251
 RFC 2453-Variabler Timer 251
 Richtlinie 154 , 158
 Richtung 250 , 432 , 527 , 528
 RIP-UDP-Port 251
 Roaming-Profil 212
 Robustheit 261
 Routenankündigung 247
 Routeneinträge 271 , 276 , 281 , 287 ,
 295 , 300 , 320 , 323 , 326 , 334 ,
 366 , 373 , 380
 Routentimeout 253
 Routentyp 233
 RSA-Schlüsselstatus 148
 RSSI Advantage 212
 RTS Frames ohne CTS 531
 RTS Threshold 209 , 212
 Rufnummer 172 , 291 , 304 , 423 ,
 430
 ruhend 266
 Rx-Bytes 529
 Rx-Fehler 529
 Rx-Pakete 529 , 530 , 533 , 534 , 535
 , 537 , 538

S

SAs mit dem Status der ISP-

- Schnittstelle synchronisieren 357
- Scan-Intervall 212
- Scan-Schwelle 212
- SCEP-URL 385
- Schedule-Intervall 475
- Schlüssel verwenden 380
- Schlüsselwert 380
- Schnittstelle 145 , 187 , 198 , 233 ,
238 , 241 , 250 , 256 , 261 , 329 ,
400 , 445 , 450 , 455 , 476 , 479 ,
480 , 489 , 527 , 528
- Schnittstelle auswählen 471
- Schnittstelle ist UPnP-kontrolliert 493
- Schnittstelle zurücksetzen, um DNS-
Server zu erhalten 440
- Schnittstellenaktion 476 , 479 , 480
- Schnittstellenbeschreibung 142
- Schnittstellenmodus 193
- Schnittstellentyp 187 , 416
- Schutz 224
- Schweregrad 513
- Segment-Sendeintervall 316
- Sekundär 439 , 439
- Sekundärer DHCP-Server 458
- Sekundärer Zeitserver 135
- Sendeleistung 203
- Sequenznummern der Datenpakete
362
- Seriennummer 127
- Server 452
- Server aktivieren 469
- Server Timeout 154
- Server-IP-Adresse 153 , 157
- Serverfehler 448
- Session Border Controller Modus 434
- SHDSL-Logik 500
- SHDSL-Typ 183
- Short Retry Limit 209 , 212
- Sicherheitsalgorithmus 523
- Sicherheitsmodus 220 , 227
- Signal 229
- Signal dBm 533 , 534 , 535 , 537 ,
538 , 538
- SIM-Karte verwendet PIN 163 , 190
- SIP-Endpunkt-IP-Adresse 416
- SIP-Header-Feld(er) für
Anruferadresse 423
- SMTP-Authentifizierung 511
- SMTP-Server 511
- SNMP 143
- SNMP Read Community 133
- SNMP Trap Broadcasting 516
- SNMP Write Community 133
- SNMP-Listen-UDP-Port 150
- SNMP-Trap-Community 516
- SNMP-Trap-UDP-Port 516
- SNMP-Version 150
- SNR 229
- SNR dB 534 , 538
- Sortierreihenfolge 418 , 423
- Spezifische Ports 378
- SSH 143
- SSH-Dienst aktiv 146
- Staat/Provinz 387
- Stack 527
- Standard-Abwurfnebenstelle 434
- Standard-Ethernet für PPPoE-
Schnittstellen 309
- Standardmäßige Routenverteilung
251
- Standardroute 271 , 276 , 281 , 287 ,
295 , 300 , 320 , 323 , 326 , 334 ,
366 , 373 , 380
- Standort 130 , 387
- Startmodus 335
- Startzeit 473 , 528
- Status 476 , 479 , 482 , 523 , 525 ,
527 , 529
- Stopzeit 473
- Subnetz 405
- Subsystem 514 , 522
- Sustained Cell Rate (SCR) 312
- Switch-Port 166
- Systemadministrator-Passwort 132
- Systemadministrator-Passwort bestäti-
gen 132
- Systemdatum 127
- Systemlogik 500

- Systemname 130
- Systemzeit über ISDN aktualisieren 135
- T**
- TACACS+-Passwort 157
- Tag 463
- Taktsignal-Modus 172
- TCP-ACK-Pakete priorisieren 272 , 277 , 282 , 296 , 301 , 310 , 321 , 324 , 327 , 367 , 375
- TCP-Inaktivität 402
- TCP-Keepalives 146
- TCP-MSS-Clamping 195
- TCP-Port 158
- TCP-Port des CAPI-Servers 469
- Teilnehmer / Benutzername 416
- Telnet 143
- TFTP-Dateiname 471
- TFTP-Server 471
- Timeout 158 , 486
- Timeout bei Inaktivität 269 , 275 , 280 , 285 , 294 , 299 , 365 , 372
- Timeout der Sitzung 412
- Timeout für Nachrichten 513
- Traceroute-Test 498
- Traffic Shaping 400
- Transformation der gerufenen Adresse 428
- Transformation der rufenden Adresse 430
- Transmit Shaping 181
- Trigger 479 , 480
- Trunk-Leitung 428
- Trunk-Modus 420
- TTL 443
- Tunnelprofil 365
- Tx-Bytes 529
- Tx-Fehler 529
- Tx-Pakete 529 , 530 , 533 , 534 , 535 , 537 , 538
- Typ 307 , 407 , 426 , 529
- U**
- Überprüfung anhand einer Zertifizierungsperrliste (CRL) 383
- Überprüfung der Rückroute 238 , 336
- Übertragene MPDUs 531
- Übertragungsmodus 339
- Übertragungsrate 183
- Übertragungsschlüssel 220 , 224 , 227
- Überwachte IP-Adresse 478
- Überwachte Schnittstelle 479 , 480
- Überwachte Schnittstellen 485 , 519
- UDP-Inaktivität 402
- UDP-Port 154
- UDP-Quellport 362
- UDP-Quellportauswahl 370
- UDP-Zielport 362 , 370 , 519
- UMTS/HSDPA/HSUPA-Status 190
- Ungültige DNS-Pakete 448
- Unicast MPDUs erfolgreich empfangen 531
- Unicast MSDUs erfolgreich übertragen 531
- UPnP TCP Port 494
- UPnP-Status 494
- Upstream 181
- Uptime 127 , 533 , 534 , 535 , 537 , 538 , 538
- URL 500
- URL Pfadtiefe 460
- URL/IP-Adresse 465
- V**
- Verbindungstyp 187 , 285 , 365
- Verbunden 229
- Verschlüsselt 526
- Verschlüsselung 158 , 288 , 367 , 375
- Verschlüsselung der Konfiguration 500
- Verschlüsselungsalgorithmen 147
- Version in Empfangsrichtung 247
- Version in Senderichtung 247
- Versuche 478
- Verteilungsmodus 255
- Verteilungsrichtlinie 255

Verteilungsverhältnis 256
 Vertrauenswürdigkeit des Zertifikats erzwingen 383
 Verwaltungs-VID 200
 Verworfen 526
 Virtual Channel Connection (VCC) 312 , 315
 Virtual Path Connection (VPC) 315
 Virtuelle Kanal-Identifizier (VCI) 307
 Virtuelle Pfad-Identifizier (VPI) 307
 VLAN aktivieren 200
 VLAN ID 193
 VLAN Identifizier 197
 VLAN-Mitglieder 197
 VLAN-Name 197
 Vollständige IPSec-Konfiguration löschen 356
 Vorgegebene Übertragungsrate 183

W

Wähle analoge Schnittstelle 416
 Wähle ISDN-Schnittstelle 416
 Wählnummer 485
 Wahlpause 434
 WDS-Beschreibung 224 , 535 , 537
 Web-Filter aktivieren 460
 Weight of Age 212
 Weight of Penalty 212
 Weitergeleitet 526
 Weitergeleitete Anfragen 448
 Weiterleiten 445
 Weiterleiten an 445
 WEP Schlüssel 1 - 4 224
 WEP-Schlüssel 1-4 220 , 227
 Wert 531
 Wiederholungen 154
 Wildcard 451
 WLAN-Modul auswählen 471
 WMM 219
 WPA Cipher 220 , 227
 WPA-Modus 220 , 227
 WPA2 Cipher 220 , 227

X

X.31 (X.25 in D-Kanal) 171
 X.31 TEI-Dienst 171
 X.31 TEI-Wert 171
 X.75 Layer-2-Modus 175

Z

Zeit 522
 Zeitaktualisierungsintervall 135
 Zeitaktualisierungsrichtlinie 135
 Zeitbedingung 473
 Zeitplan (Start-/Stopzeit) 463
 Zeitschlitzauswahl 175
 Zeitschlitzbereich 175
 Zeitschlitzmatrix 175
 Zeitstempel 506
 Zeitverschiebung von GMT 135
 Zero Cookies verwenden 357
 Zertifikat ist ein CA-Zertifikat 383
 Zertifikate und Schlüssel einschließen 500
 Zertifikatsanforderungs-Payloads ignorieren 358
 Zertifikatsanforderungs-Payloads senden 358
 Zertifikatsanforderungsbeschreibung 385
 Zertifikatsketten senden 358
 Ziel 397
 Ziel-ID 524
 Ziel-IP-Adresse 233 , 482 , 483 , 524
 Zielport 235 , 244
 Zielportbereich 407
 Zielschnittstelle 259
 Zugeordnete Leitung 432
 Zugriff 468
 Zusammenfassend 387
 Zusätzliche Adernpaare 183