

Manual bintec RV Series

Copyright© Version 2.0, 2014 bintec elmeg GmbH

Legal Notice

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec elmeg-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.bintec-elmeg.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. bintec elmeg 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 bintec elmeg-Gateways finden Sie unter www.bintec-elmeg.com.

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

Marken

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

Richtlinien und Normen

Informationen zu Richtlinien und Normen finden Sie in den Konformitätserklärungen unter www.bintec-elmeg.com.

Wie Sie bintec elmeg GmbH erreichen

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

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

Internet: www.teldat.fr

Table of Contents

Chapter 1	Introduction	1
Chapter 2	About this guide.	2
Chapter 3	Installation.	5
3.1	Setting up and connecting	5
3.2	Cleaning.	8
3.3	Support information	8
Chapter 4	Reset	9
Chapter 5	Technical data	10
5.1	Scope of supply	10
5.2	General Product Features	10
5.3	LEDs	12
5.4	Connectors	13
5.5	Antenna connectors	14
5.6	Pin Assignments	15
5.6.1	Ethernet interface.	15
5.6.2	AUX interface	15
5.6.3	Wi-Fi connector and CELL connector	16
5.6.4	Power supply	17
5.7	Inserting the SIM card	17
5.8	WEEE information	20

Chapter 6	Basic configuration	22
6.1	Presettings	22
6.1.1	IP Configuration	22
6.1.2	Software update	23
6.2	System requirements	23
6.3	Preparation	23
6.3.1	Gathering data	23
6.3.2	Configuring a PC	25
6.3.3	Modify system password.	26
6.4	Setting up an internet connection	26
6.4.1	Internet connection over UMTS/LTE.	26
6.4.2	Other internet connections	27
6.4.3	Testing the configuration.	27
6.5	Setting up wireless LAN	28
6.6	Software Update	29
Chapter 7	Access and configuration.	30
7.1	Access Options.	30
7.1.1	Access via LAN	30
7.1.2	Access via the Serial Interface	33
7.1.3	Access over ISDN	35
7.2	Login	35
7.2.1	User names and passwords in ex works state	36
7.2.2	Logging in for Configuration	36
7.3	Configuration options	37
7.3.1	GUI (Graphical User Interface)	38
7.3.2	SNMP shell	48
7.4	BOOTmonitor	48

Chapter 8	Assistants	51
Chapter 9	System Management	52
9.1	Status	52
9.2	Global Settings	55
9.2.1	System	55
9.2.2	Passwords	58
9.2.3	Date and Time	59
9.2.4	System Licences	64
9.3	Interface Mode / Bridge Groups	66
9.3.1	Interfaces	68
9.4	Administrative Access	72
9.4.1	Access	72
9.4.2	SSH	73
9.4.3	SNMP	77
9.5	Remote Authentication	78
9.5.1	RADIUS	79
9.5.2	TACACS+	85
9.5.3	Options	88
9.6	Configuration Access	89
9.6.1	Access Profiles	89
9.6.2	Users	93
9.7	Certificates	97
9.7.1	Certificate List	97
9.7.2	CRLs	106
9.7.3	Certificate Servers	108
Chapter 10	Physical Interfaces	109

10.1	AUX	109
10.1.1	AUX	109
10.2	Ethernet Ports	111
10.2.1	Port Configuration	113
10.3	Serial Port	115
10.3.1	Serial Port	115
10.4	UMTS/LTE.	119
10.4.1	UMTS/LTE.	119
10.5	GPS	129
10.5.1	GPS Configuration	129
10.5.2	GEO Zones	131
Chapter 11	LAN	137
11.1	IP Configuration	137
11.1.1	Interfaces	137
11.2	VLAN	141
11.2.1	VLANs	143
11.2.2	Port Configuration	144
11.2.3	Administration	144
Chapter 12	Wireless LAN	146
12.1	WLAN.	147
12.1.1	Radio Settings	147
12.1.2	Wireless Networks (VSS)	157
12.1.3	Client Link	165
12.1.4	Bridge Links	169
12.2	Administration	170
12.2.1	Basic Settings	170

Chapter 13	Wireless LAN Controller	172
13.1	Wizard	172
13.1.1	Basic Settings	173
13.1.2	Radio Profile	174
13.1.3	Wireless Network	174
13.1.4	Start automatic installation	176
13.2	Controller Configuration	178
13.2.1	General	178
13.3	Slave AP configuration	180
13.3.1	Slave Access Points	181
13.3.2	Radio Profiles	185
13.3.3	Wireless Networks (VSS)	192
13.4	Monitoring	199
13.4.1	Active Clients	199
13.4.2	Wireless Networks (VSS)	200
13.4.3	Client Management	200
13.4.4	Neighbor APs	201
13.4.5	Rogue APs	202
13.4.6	Rogue Clients	203
13.5	Maintenance	204
13.5.1	Firmware Maintenance	204
Chapter 14	Networking	207
14.1	Routes	207
14.1.1	IPv4 Route Configuration	207
14.1.2	IPv4 Routing Table	214
14.1.3	Options	215
14.2	NAT.	216
14.2.1	NAT Interfaces	216

14.2.2	NAT Configuration	217
14.3	Load Balancing.	224
14.3.1	Load Balancing Groups	224
14.3.2	Special Session Handling	228
14.4	QoS	232
14.4.1	QoS Filter	232
14.4.2	QoS Classification	235
14.4.3	QoS Interfaces/Policies	238
14.5	Access Rules	245
14.5.1	Access Filter	247
14.5.2	Rule Chains	251
14.5.3	Interface Assignment	253
14.6	Drop In	254
14.6.1	Drop In Groups.	254
Chapter 15	Routing Protocols.	258
15.1	RIP	258
15.1.1	RIP Interfaces	258
15.1.2	RIP Filter	260
15.1.3	RIP Options	263
15.2	OSPF	265
15.2.1	Areas	267
15.2.2	Interfaces	269
15.2.3	Global Settings	271
Chapter 16	Multicast.	273
16.1	General	274
16.1.1	General	275
16.2	IGMP	275

16.2.1	IGMP	276
16.2.2	Options	278
16.3	Forwarding	280
16.3.1	Forwarding	280
16.4	PIM	281
16.4.1	PIM Interfaces	281
16.4.2	PIM Rendezvous Points	285
16.4.3	PIM Options	286
Chapter 17	WAN.	288
17.1	Internet + Dialup	288
17.1.1	PPPoE	290
17.1.2	PPTP	296
17.1.3	UMTS/LTE.	300
17.1.4	AUX	305
17.1.5	IP Pools	312
17.2	Leased Line	313
17.2.1	Interfaces	314
17.3	Real Time Jitter Control	320
17.3.1	Controlled Interfaces	320
Chapter 18	VPN	322
18.1	IPSec	322
18.1.1	IPSec Peers	323
18.1.2	Phase-1 Profiles	339
18.1.3	Phase-2 Profiles	348
18.1.4	XAUTH Profiles	353
18.1.5	IP Pools	355
18.1.6	Options	356
18.2	L2TP	359

18.2.1	Tunnel Profiles	360
18.2.2	Users	363
18.2.3	Options	369
18.3	PPTP	370
18.3.1	PPTP Tunnels	370
18.3.2	Options	377
18.3.3	IP Pools	378
18.4	GRE	379
18.4.1	GRE Tunnels	380
Chapter 19	Firewall	382
19.1	Policies	383
19.1.1	Filter Rules	383
19.1.2	QoS	387
19.1.3	Options	388
19.2	Interfaces	390
19.2.1	Groups	390
19.3	Addresses	391
19.3.1	Address List	391
19.3.2	Groups	392
19.4	Services	393
19.4.1	Service List	393
19.4.2	Groups	395
Chapter 20	VoIP	397
20.1	SIP	397
20.1.1	Options	397
20.2	RTSP	398
20.2.1	RTSP Proxy	398

Chapter 21	Local Services	400
21.1	DNS	400
21.1.1	Global Settings	402
21.1.2	DNS Servers	404
21.1.3	Static Hosts	406
21.1.4	Domain Forwarding	407
21.1.5	Cache	409
21.1.6	Statistics	410
21.2	HTTPS	411
21.2.1	HTTPS Server	411
21.3	DynDNS Client	412
21.3.1	DynDNS Update	412
21.3.2	DynDNS Provider	414
21.4	DHCP Server	416
21.4.1	IP Pool Configuration	416
21.4.2	DHCP Configuration	417
21.4.3	IP/MAC Binding	421
21.4.4	DHCP Relay Settings	422
21.5	Web Filter	423
21.5.1	General	424
21.5.2	Filter List	426
21.5.3	Black / White List	428
21.5.4	History	429
21.6	Scheduling	429
21.6.1	Trigger	430
21.6.2	Actions	435
21.6.3	Options	446
21.7	Surveillance	447
21.7.1	Hosts	447

21.7.2	Interfaces	450
21.7.3	Ping Generator	451
21.8	UPnP	453
21.8.1	Interfaces	453
21.8.2	General	454
21.9	HotSpot Gateway	455
21.9.1	HotSpot Gateway	457
21.9.2	Options	461
21.10	Wake-On-LAN	462
21.10.1	Wake-On-LAN Filter	462
21.10.2	WOL Rules	465
21.10.3	Interface Assignment	467
21.11	BRRP	468
21.11.1	Virtual Routers	469
21.11.2	VR Synchronisation	475
21.11.3	Options	476
Chapter 22	Maintenance	478
22.1	Diagnostics	478
22.1.1	Ping Test	478
22.1.2	DNS Test	479
22.1.3	Traceroute Test	479
22.2	Software & Configuration	480
22.2.1	Options	480
22.3	Reboot	485
22.3.1	System Reboot	485
Chapter 23	External Reporting	486
23.1	Syslog	486

23.1.1	Syslog Servers	486
23.2	IP Accounting	489
23.2.1	Interfaces	489
23.2.2	Options	489
23.3	Alert Service	491
23.3.1	Alert Recipient	491
23.3.2	Alert Settings	494
23.4	SNMP.	496
23.4.1	SNMP Trap Options.	496
23.4.2	SNMP Trap Hosts	497
Chapter 24	Monitoring.	499
24.1	Internal Log	499
24.1.1	System Messages	499
24.2	IPSec	500
24.2.1	IPSec Tunnels	500
24.2.2	IPSec Statistics.	502
24.3	Interfaces	503
24.3.1	Statistics	503
24.4	WLAN.	506
24.4.1	WLANx	506
24.4.2	VSS	508
24.5	Bridges	511
24.5.1	br<x>	511
24.6	HotSpot Gateway	512
24.6.1	HotSpot Gateway	512
24.7	QoS	512
24.7.1	QoS	512
24.8	OSPF	513

24.8.1 Status 513

24.8.2 Statistics 516

24.9 PIM 517

24.9.1 Global Status 517

24.9.2 Not Interface-Specific Status 519

24.9.3 Interface-Specific States 522

 Glossary. 525

 Index 553

Chapter 1 Introduction

The robust **bintec** routers **RV120-4G**, **RV120w**, **RV120w-4G** and **RV130w-4G** are specifically designed for use in tough, extreme environments (road and rail vehicles). The devices provide wireless for passengers and encrypted transmission for metrics (e. g. speed), image data (e. g. security cameras) and positioning signals (GPS).

Safety notices

The safety precautions supplied with your bintec router tell you what you need to consider when using your device.

Installation

How to connect your device is shown in [Setting up and connecting](#) on page 5. This chapter also tells you what preliminary tasks are necessary for configuration.

Configuration

How to get your device running is explained in [Basic configuration](#) on page 22. There we show you how to start up your device within a few minutes from a Windows PC with the help of a Configuration Wizard and how to install other useful online assistants. At the end of the chapter, you will be in a position to surf the Internet, send or receive e-mails and set up a connection to a partner network to access data at your company head office, for example.

Password

If you are already familiar with configuring bintec devices and want to get started right away, all you really need to know is the factory default user name and password.

User Name: *admin*

Password: *admin*



Note

Remember to change the password immediately when you log in to the device for the first time.

All the bintec devices are delivered with the same password. which means they are not protected against unauthorised access until you change the password.

How to change the passwords is described in chapter [Modify system password](#) on page 26.

Chapter 2 About this guide

This document is valid for bintec devices whose system software is version 9.1.8 and later.

The guide, which you have in front of you, contains the following chapters:





User's Guide - Reference

Chapter	Description
Introduction	You see an overview of the device:
About this guide	We explain the various components of this manual and how to use it.
Installation	This contains instructions for how to set up and connect your device.
Basic configuration	This chapter provides a step-by-step guide to the basic functions on your device.
Reset	This chapter explains how to reset your device to the ex works state.
Technical data	This section contains a description of all the device's technical properties.
Access and configuration	This includes explanations about the different access and configuration methods.
Assistants	This chapter describes all of the GUI configuration options. The chapters are arranged in the same sequence as the navigation menus in the GUI . The individual chapters also contain general explanations on the subsystem in question.
System Management	
Physical Interfaces	
LAN	
Wireless LAN	
Wireless LAN Controller	
Networking	
Routing Protocols	
Multicast	
WAN	

Chapter	Description
VPN	
Firewall	
VoIP	
Local Services	
Maintenance	
External Reporting	
Monitoring	
Glossary	The glossary contains a reference to the most important technical terms used in network technology.
Index	The index lists all the key terms for operating the device and all the configuration options and gives page numbers so they can be found easily.

To help you locate information easily, this user's guide uses the following visual aids:

List of visual aids

Symbol	Use
	Indicates practical information.
	Indicates general and important points.
	Indicates a warning of risk level "Attention" (points out possible dangers that may cause damage to property if not observed).
	Indicates a warning of risk level "Warning" (points out possible dangers that may cause physical injury or even death if not observed).

The following typographical elements are used to help you find and interpret the information in this user's guide:

Typographical elements

Typographical element	Use
•	Indicates lists.
Menu->Submenu	Indicates menus and sub-menus.

Typographical element	Use
File->Open	
non-proportional (Courier), e. g. ping 192.168.0.254	Indicates commands that you must enter as written.
bold, e.g. Windows Start menu	Indicates keys, key combinations and Windows terms.
bold, e. g. Licence Key	Indicates fields.
italic, e.g. <i>none</i>	Indicates values that you enter or that can be configured.
Online: blue and italic, e. g. www.bintec-elmeg.com	Indicates hyperlinks.

Chapter 3 Installation



Caution

Please read the safety notices carefully before installing and starting up your device. These are supplied with the device.

The device should only be installed by a qualified person, or it could get damaged or work incorrectly.

Avoid damp or dusty areas.

Avoid direct sunshine and other sources of heat.

Air should not be prevented from circulating naturally.

The device should not be placed close to any strong electromagnetic field.

3.1 Setting up and connecting



Caution

Wiring the ETH interfaces incorrectly may also cause your device to be damaged. The device's ETH interface should always be connected to the LAN interface on the computer/hub.



Note

All you need for this is the cable supplied with the equipment. You can purchase the appropriate antennae and power pack (starter kit) separately from www.bintec-elmeg.com.



Caution

Switch the device off before opening the housing. The power supply and data cable should be disconnected. When starting the device, always connect the data cable first and then the power supply, in order to avoid a power surge.

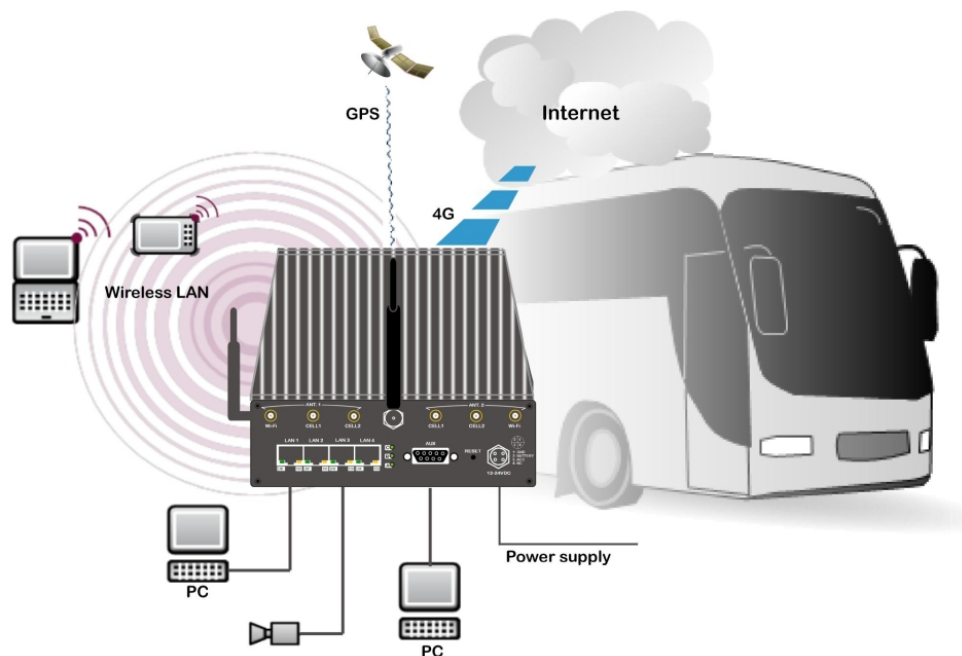


Fig. 2: Connection options

Set up and connect in the following sequence:

(1) LAN

To carry out a standard configuration of your device via Ethernet, connect the first 100 MBit switch port **LAN1** on your device to your LAN using the Ethernet cable supplied. The device automatically detects whether it is connected to a switch or directly to a PC.

(2) AUX

Using the RS-232 cable provided, connect the AUX jack to an external device (PC) to configure the device.

(3) Power connection

Connect the power plug provided with a suitable power cable. Now connect the 12-24V DC jack to the vehicle's battery. The power supply can be modified to meet the needs of the project concerned!

(4) Antennas

Screw the external antennae onto the connections provided for this purpose. Wi-Fi (**bintec RV120w-4G**, **bintec RV120w** and **bintec RV130w-4G**): Screw the WLAN antennae onto the Wi-Fi connectors to provide passengers with wireless Internet access.

CELL1/CELL 2 (**bintec RV120-4G**, **bintec RV120w-4G** and **bintec RV130w-4G**): Screw the LTE antennae onto the CELL connectors to establish an Internet connec-

tion to the wireless network.

GPS: Screw the GPS antenna onto the GPS connector to receive the GPS frequencies.

You can set up further connections as required:

- Other LANs/WANs

Connect any other terminals in your network to the remaining switch ports (**2, 3 or 4**) on your device using other Ethernet cables.

Installation

The devices should be mounted on the housing using brackets, or deployed horizontally. The brackets are pre-installed on the housing with six screws on the front side and rear side.

Make sure the device connections are accessible.

The device is now ready for configuration with the **GUI**. Chapter [Basic configuration](#) on page 22 provides a detailed step-by-step guide to the basic functions on your device.

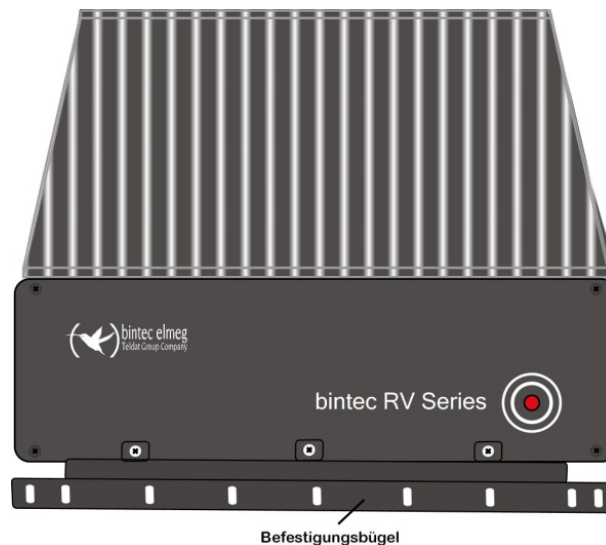


Fig. 3: Wall / ceiling installation

3.2 Cleaning

You can clean your device easily. Use a damp cloth or antistatic cloth. Do not use solvents. Never use a dry cloth; the electrostatic charge could cause electronic faults. Make sure that no moisture can enter the device and cause damage.

3.3 Support information

If you have any questions about your new product or are looking for additional information, the bintec elmeg GmbH Support Centre can be reached Monday to Friday between the hours of 9 am and 5 pm. They can be contacted as follows:

International Support Coordina- tion	Telephone: +49 911 9673 0 Fax: +49 911 688 0725
---	--

For detailed information about our support and service offers please visit our website at www.bintec-elmeg.com.

Chapter 4 Reset

In case of a misconfiguration or if you can no longer access your device, you can reboot it by pressing the Reset button on the backplate. If you still cannot access the device, you can delete the configuration via a serial connection: interrupt the boot sequence at the message `Press <sp> for boot monitor or any other key to boot system` and delete the configuration with (4) Delete Configuration.



Note

If you delete the boot configuration using the **GUI** (menu **Maintenance->Software & Configuration**), all passwords will also be reset and the current boot configuration deleted. The next time, the device will boot with the standard ex works settings.

You can now configure your device again as described from [Basic configuration](#) on page 22

.

Chapter 5 Technical data

This chapter summarises all of the device's hardware characteristics.

5.1 Scope of supply

Your device is supplied with the following parts:

Product name	Cable sets/mains unit/ other	Software	Documentation
bintec RV-Serie	Console cable or RS232 cable Power plug	Companion DVD	Safety notices (printed) User's Guide (on DVD) Installation poster



Note

You can purchase the appropriate antennae and power pack (starter kit) separately. The starter kit includes 2 LTE antennae, 2 Wi-Fi antennae and the power pack.

5.2 General Product Features

The general product features cover performance features and the technical prerequisites for installation and operation of your device.

The features are summarised in the following table:

General Product Features

Property	bintec RV-Serie
Dimensions and weights:	
Equipment dimensions without cable (L x W x H):	205 mm x 165 mm x 60 mm
Weight	approx. 1,500 g
Transport weight (incl. documentation, cables, packaging)	approx. 2000 g
Memory	64 MB SDRAM memory

Property	bintec RV-Serie
	16 MB FLASH memory 128 KB NVRAM memory
LEDs	12 (1x power, 4 x 2 Ethernet, 3 x function)
Power consumption of the device	7.5 watts to 8.5 watts
Voltage supply	From 12 - 24 V/DC vehicle battery
Mains connection	12 - 24 V/DC
Environmental requirements:	
Ambient temperature	- 30 °C to + 70 °C
Operating temperature	- 15 °C to + 65 °C
Relative atmospheric humidity	on: 8 % to 85 %; off: 5 % to 90 %
Room classification	Avoid damp and dusty locations.
Standards & Guidelines	SAE J1455-certified, mechanical protection against jolts, blows and vibration. Permit number 047081. Quality mark compliant with ECE vehicle regulations
Software supplied	DIME Manager
Documentation included	Safety advice, installation poster
Online documentation	User Guide on DVD

Available interfaces

	bintec RV 120-4G	bintec RV 120w	bintec RV 120w-4G	bintec RV 130w-4G
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100 MBit/s	Permanently installed (twisted pair only), 10/100 MBit/s	Permanently installed (twisted pair only), 10/100 MBit/s	Permanently installed (twisted pair only), 10/100 MBit/s
AUX (serial interface V.24)	RS232 interface	RS232 interface	RS232 interface	RS232 interface
Antennas:				
GPS antennas	SMA jack	SMA jack	SMA jack	SMA jack
LTE/UMTS antennas	SMA jack	-	SMA jack	SMA jack
WLAN interface	-	802.11a/b/g/h; 802.11n 2.4 GHz and 5 GHz	802.11a/b/g/h; 802.11n 2.4 GHz and 5 GHz	802.11a/b/g/h; 802.11n 2.4 GHz and 5 GHz
Available sockets:				
Ethernet interface	RJ45 socket	RJ45 socket	RJ45 socket	RJ45 socket

	bintec RV 120-4G	bintec RV 120w	bintec RV 120w-4G	bintec RV 130w-4G
AUX	9-pin Sub-D connector DB-9F	9-pin Sub-D connector DB-9F	9-pin Sub-D connector DB-9F	9-pin Sub-D connector DB-9F
GPS	SMA-F jack	SMA-F jack	SMA-F jack	SMA-F jack
LTE/UMTS (CELL)	RF SMA jack (CELL1)	-	RF SMA jack (CELL1)	RF SMA jack (CELL1/CELL2)
WLAN	-	2x RF SMA jack (Wi-Fi)	2x RF SMA jack (Wi-Fi)	2x RF SMA jack (Wi-Fi)

5.3 LEDs

The device LEDs provide information on certain activities and statuses of the device. The red power LED is on the front of the device.

The LEDs on the rear of the device are arranged as follows:



Fig. 4: Arrangement of LEDs

In operation mode, the LEDs display the following status information for your device:

LED status display

LED	Colour	Status	Information
Power	red	on	The power supply is connected.
LAN 1 to 4: LNK/100	green	on	Ethernet connection established.
	green	off	No Ethernet connection.
	green	flashing	Data transmission over Ethernet
	orange	on	100 Mbit/s, transmission rate.
	orange	off	10 Mbit/s transmission rate.
A	green	on	LTE-1 connection established.

LED	Colour	Status	Information
LTE module 1			
	green	off	No LTE-1 connection.
	green	flashing	Data transmission over LTE-1.
B Wi-Fi (WLAN)	green	on	WLAN connection established.
	green	off	No WLAN connection.
	green	flashing	Data transmission over WLAN.
C LTE module 2	green	on	LTE-2 connection established.
	green	off	No LTE-2 connection.
	green	flashing	Data transmission over LTE-2.

5.4 Connectors

All the connections are located on the back of the device.

The **bintec RV-Serie** devices have a 4-port Ethernet switch, an AUX interface, a GPS jack and connectors for external Wi-Fi and GSM antennas.

The connections are arranged as follows:

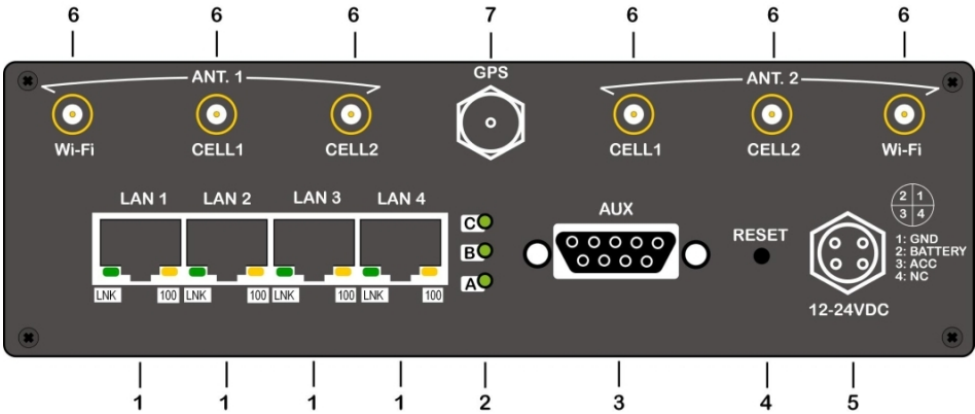


Fig. 5: **bintec RV-Serie** rear panel

bintec RV-Serie rear panel		
1	LAN 1 / LAN 2 / LAN 3 / LAN 4	Fast Ethernet 10/100 Mbit/s Base-T (RJ 45F)
2	Status LEDs (green)	A: Wireless WAN interface channel 0 B: Wireless WAN interface channel 1 C: Mini-PCI slot for an additional WLAN card
3	AUX	Serial console (DB-9F)
4	RESET	Reset button
5	12-24V DC	Jack for the 12 - 24 V/DC power supply and ignition control input
6	Antenna connectors	Wi-Fi: Wi-Fi antennas (bintec RV120w , bintec RV120w-4G and bintec RV130w-4G): CELL: 3/4G modules (bintec RV120-4G , bintec RV120w-4G and bintec RV130w-4G)
7	GPS	Connector for GPS antenna

5.5 Antenna connectors

The devices have connectors for a 3G/GPS antenna and a 3G/GSM antenna connector (**bintec RV120-4G** and **bintec RV120w-4G**). The **bintec RV130w-4G** has two 3G/GSM antenna connectors. **bintec RV120w-4G**, **bintec RV120w** and **bintec RV130w-4G** have one Wi-Fi antenna connector.

The graphic below shows the antenna connector assignment:



Fig. 6: Antenna assignment

5.6 Pin Assignments

5.6.1 Ethernet interface

The devices have four Ethernet interfaces with an integrated 4 port switch. This is used to connect individual PCs or other switches.

The connection is made via an RJ45 socket.

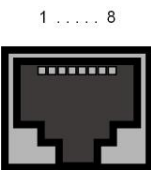


Fig. 7: 10/100/1000 Base-T Ethernet interface (RJ45 connector)

The pin assignment for the 10/100 Base-T Ethernet interface (RJ45 connector) is as follows:

RJ45 socket for LAN connection

Pin	Function
1	Tx+ (input)
2	Tx- (input)
3	Rx+ (output)
4	---
5	---
6	Rx- (output)
7	---
8	---

5.6.2 AUX interface

The **bintec RV-Serie** devices have a DB9 jack for connecting to external devices or for the serial connection.

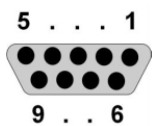


Fig. 8: DB9 jack

The pin assignment is as follows:

DB9 jack

Pin	Function
1	---
2	RxD (Receive Data)
3	TxD (Transmit Data)
4	---
5	GND (Ground)
6	---
7	---
8	---
9	---

5.6.3 Wi-Fi connector and CELL connector

The device has 4 RF SMA connectors (Wi-Fi and CELL connector).



Fig. 9: RF SMA jack

The RF SMA jack is arranged as follows:

RF SMA jack

Pin	Ant
internal	RF in/out
external	GND

5.6.4 Power supply

The device has a connector for the power supply.

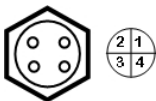


Fig. 10: 12-24 V/DC jack

The jack is arranged as follows:

12-24 V/DC jack

Pin	Ant
1	GND
2	Battery
3	ACC
4	NC

5.7 Inserting the SIM card

The devices have two card slots for SIM cards. Both card slots are inside the device. The card slots are labelled as SK1 (connector 1) and SK2 (connector 2). Where installations require a SIM card, at least one SIM card needs to be inserted. The SIM card may be inserted into either of the card slots. To configure a router, ensure that you select the corresponding card slot.

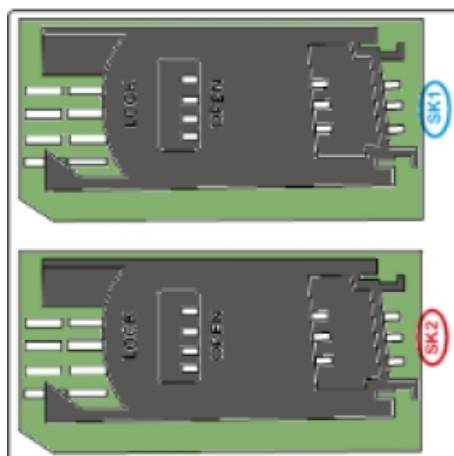


Fig. 11: Card slots SK1 and SK2



Caution

Disconnect the device from the power supply before you open the housing lid. When starting the device, always connect the data cable first and then the power supply.

When inserting the SIM card, protect yourself from electrostatic discharges (ESD).

Do not touch the contacts on the SIM card.

Proceed as follows to insert the SIM cards:

Figure 1

- Unscrew the two screws on the top corner at the front, and the two screws on the top corner at the back of the device, and lift up the housing lid.

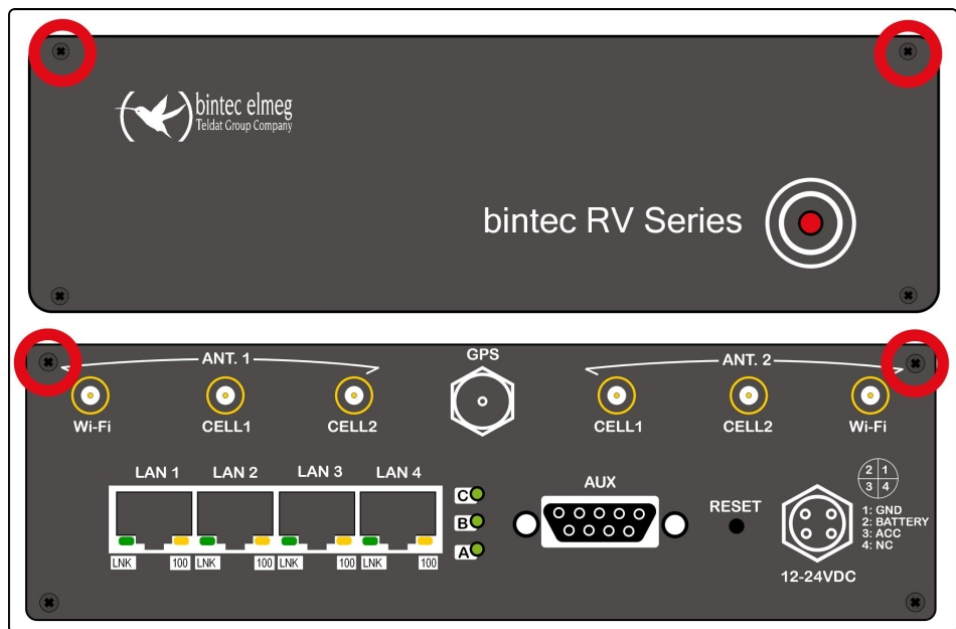




Fig. 12: Unscrew the housing lid (Figure 1)

Figure 2

- Open the card slot. To do this, push the card lock in the direction of the arrow  (OPEN) and lift the card slot slightly.
- Make sure that contacts on the SIM card are facing downwards.
- Push the SIM card into the card slot so that the bevelled edge of the card is facing upwards.
- Close the card slot. To do this, press the card slot downwards again to its original position.
- Push the card lock in the direction of the arrow  (LOCK). You will hear the card click into place.
- Replace the housing lid on the device. To do this, unscrew the two lower screws on the front or on the back of the device. Then screw all the screws back in.

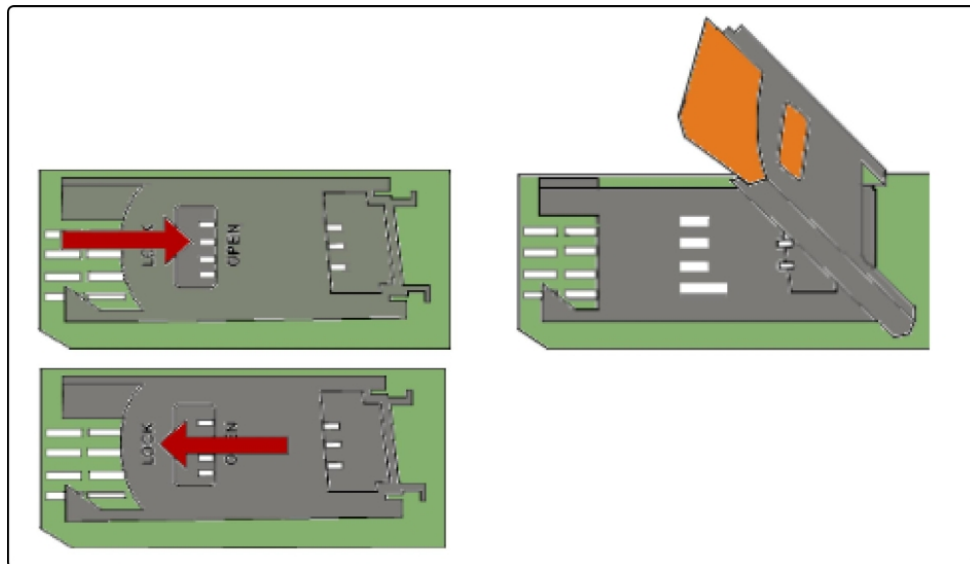


Fig. 13: Insert the SIM card (Figure 2)

5.8 WEEE information



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



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



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



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



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



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



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



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



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



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



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



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

Chapter 6 Basic configuration

You configure your device using the **GUI** (Graphical User Interface).

A few basic configurations are required for use as a gateway. In this chapter, you will learn how to prepare the configuration, which data you have to collect first, set up a WLAN, make adjustments to the PC configurations in the network if necessary, and test the connection when the configuration has been completed. Detailed knowledge of networks is not necessary. A detailed online help system gives you extra support.

The **Companion DVD** provided with the product includes all the tools that you need to configure and manage your device.

6.1 Presettings

6.1.1 IP Configuration

Your device is shipped with a pre-defined IP configuration:

- **IP Address:** *192.168.0.254*
- **Netmask:** *255.255.255.0*

Use the following access data to configure your device in an ex works state:

- **User Name:** *admin*
- **Password:** *admin*



Note

All bintec devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

How to change the passwords is described in [Modify system password](#) on page 26.

6.1.2 Software update

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You can easily perform an update with the **GUI** using the **Maintenance->Software & Configuration** menu.

For a description of the update procedure, see [Software Update](#) on page 29.

6.2 System requirements

For configuration of the device, your PC must meet the following system requirements:

- Microsoft Windows operating system Windows 2000 or higher; Windows XP SP3 requires the following hotfix: <http://support.microsoft.com/kb/953761>
- Internet Explorer Version 7 or 9 (security settings may need to be customised), Mozilla Firefox Version 4 or higher
- Installed network card (Ethernet)
- DVD drive
- Installed TCP/IP protocol
- High colour display (more than 256 colours) for correct representation of the graphics.

6.3 Preparation

To prepare for configuration, you need to...

- have the data for the basic configuration and the Internet connection to hand and also gather the data needed for connecting the required WLAN clients.
- Check whether the PC from which you want to perform the configuration meets the necessary requirements.

6.3.1 Gathering data

You can gather the main data for configuration with the **GUI** quickly, because you do not need any information that requires in-depth knowledge of networks.

In addition, you can have the device assign a valid IP configuration to all PCs, so time-consuming configuration of your LAN is not necessary. If necessary, you can use the sample values.

Before you start the configuration, you should gather the data for the following purposes:

- Basic configuration (obligatory if your device is in the ex works state)
- Internet access (optional)
- Wireless LAN (optional) with an independently configurable operating mode (Access Point or Access Client)

The following tables show examples of possible values for the necessary data. You can enter your personal data in the "Your values" column, so that you can refer to these values later when needed.

If you configure a new network, you can use the given example values for IP addresses and netmasks. In cases of doubt, ask your system administrator.

Basic configuration

For a basic configuration of your gateway, you need information that relates to your network environment:

Basic information

Access data	Example value	Your values
IP address of your gateway	192.168.0.254	
Netmask of your gateway	255.255.255.0	

Access Point mode

When you run your device in Access Point mode you can set up the wireless networks that you want on the **GUI** in the menu **Wireless LAN->WLAN->Wireless Networks (VSS)->New**. To do this, you need the following data:

Configuration of a wireless network (VSS)

Access data	Example value	Your values
Network Name (SSID)	default	
Security mode	WPA-PSK	
Preshared key	supersecret	

Access Client mode

When you run your device in Access Client mode you can set up the client links that you want on the **GUI** in the menu **Wireless LAN->WLAN->Client Link->Edit**. To do this, you need the following data:

IP configuration of the access client

Access data	Example value	Your values
Network Name (SSID)	<i>default</i>	
Security mode	<i>WPA-PSK</i>	
Preshared key	<i>supersecret</i>	

6.3.2 Configuring a PC

In order to reach your device via the network and to be able to carry out configuration, the PC used for the configuration has to satisfy some prerequisites.

- Make sure that the TCP/IP protocol is installed on the PC.
- Select the suitable IP configuration for your configuration PC.

The PC via which you want to configure the IP address for your device must be in the same network as your device.

Checking the Windows TCP/IP protocol

Proceed as follows to check whether you have installed the protocol:

- (1) Click the Windows Start button and then **Settings -> Control Panel -> Network Connections** (Windows XP) or **Control Panel -> Network and Sharing Center-> Change Adapter Settings** (Windows 7).
- (2) Click on **LAN Connection**.
- (3) Click on **Properties** in the status window.
- (4) Look for the **Internet Protocol (TCP/IP)** entry in the list of network components.

Installing the Windows TCP/IP protocol

If you cannot find the **Internet Protocol (TCP/IP)** entry, install the TCP/IP protocol as follows:

- (1) First click **Properties**, then **Install** in the status window of the **LAN Connection**.
- (2) Select the **Protocol** entry.
- (3) Click **Add**.
- (4) Select **Internet Protocol (TCP/IP)** and click on **OK**.
- (5) Follow the on-screen instructions and restart your PC when you have finished.

Allocating PC IP address

Allocate an IP address to your PC as follows:

- (1) Select **Internet Protocol (TCP/IP)** and click **Properties**.

- (2) Choose **Use following IP address** and enter a suitable IP address, the matching net-mask, your default gateway and your preferred DNS server.

If you run a DHCP server in your network, you can apply the default Windows setting **Obtain IP address automatically** and **Obtain DNS server address automatically**.

Your PC should now meet all the prerequisites for configuring your device.

6.3.3 Modify system password

All bintec devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. Make sure you change the passwords to prevent unauthorised access to your device!

Proceed as follows:

- (a) Go to the **System Management->Global Settings->Passwords** menu.
- (b) Enter a new password for **System Admin Password**.
- (c) Enter the new password again under **Confirm Admin Password**.
- (d) Click **OK**.
- (e) Store the configuration using the **Save configuration** button above the menu navigation.

Note the following rules on password use:

- The password must not be easy to guess. Names, car registration numbers, dates of birth, etc. should not be chosen as passwords.
- The password should contain at least one character that is not a letter (special character or number).
- The password should be at least 8 characters long.
- Change your password regularly, e.g. every 90 days.

6.4 Setting up an internet connection

You can use UMTS/LTE to connect your device to the Internet. If you are configuring other types of connection, the Internet wizard in the **GUI** will help you.

6.4.1 Internet connection over UMTS/LTE

Setting up an internet connection over UMTS/LTE requires an activated SIM card from your UMTS provider. Insert the card as described in [Inserting the SIM card](#) on page 17.

- (1) In the **GUI**, go to the menu **Assistants->Internet Access->Internet Connections->New**.
- (2) As the **Connection Type**, select *UMTS/LTE*.
- (3) Click **Next**.
- (4) Give the connection a **Description**, e. g. *LTE_Internet*.
- (5) Leave the **UMTS/LTE Interface** set to *UMTS-6-0*.
- (6) The other settings will depend on your Internet provider.
- (7) Under **Type** you can set up a user-defined connection or select one from a pre-defined template.
- (8) Once you have exited the wizard, save the configuration by clicking the **Save configuration** button above the menu navigation.

6.4.2 Other internet connections

In addition to a connection via a HSPA/UMTS connection, you can connect your device to the Internet using other types of connection, for example an external modem (e.g. a cable modem) or an external gateway. The corresponding wizard in the **GUI** provides support for configurations of this type. You will find the Internet wizards, and other wizards that make it easier to configure various applications, at the top of the menu tree under **Assistants**.

6.4.3 Testing the configuration

Once you have completed the configuration of your device, you can test the connection in your LAN and to the Internet.

Carry out the following steps to test your device:

- (1) Test the connection from any device in the local network to your device. Click **Run** in the Windows Start menu and enter `ping`, followed by a space and your router's IP address. `http://192.168.0.254`. A window appears with the text "Reply from...".
- (2) Test the Internet access by entering www.bintec-elmeg.com in the Internet browser. You will find news, updates and other documentation on the bintec elmeg GmbH website.



Note

Incorrect configuration of the devices in your LAN may result in unwanted connections and increased charges! Monitor your device and make sure it only sets up connections at the times you want it to. Watch the LEDs on your device (LED for ISDN, ADSL and the Ethernet interface to which you have connected WANs).

6.5 Setting up wireless LAN

Proceed as follows to use your device as an access point:

- (1) In the **GUI**, go to the menu **Assistants->Wireless LAN->Wireless LAN**.
- (2) Click **Change** to enable the WLAN.
- (3) Under **WLAN Scenario**, select *Access-Point Mode*.
- (4) Select a **Operation Band** that suits you.
- (5) Click **OK**.
- (6) Change the password under **Preshared Key**. This password gives you access to the WLAN.
- (7) Enable the **Use gateway as DHCP Server** option.
- (8) Under **IP Address Range**, enter a range that matches your **Gateway IP Address**, e. g. *192.168.0.1 - 192.168.0.70*.
- (9) Store the configuration using the **Save configuration** button above the menu navigation.

Configuring the WLAN Adapter under Windows XP

After installing the drivers for your WLAN card, Windows XP set up a new connection in the network environment. Proceed as follows to configure the Wireless LAN connection:

- (1) Click on **Start -> Settings** and double-click on **Network Connections -> Wireless Network Connection**.
- (2) On the left-hand side, select **Change Advanced Settings**.
- (3) Go to the **Wireless networks** tab.
- (4) Click **Add**.

Proceed as follows:

- (1) Enter a **Network Name**, e.g. *Client-1*.
- (2) Set **Network Authentication** to *WPA2-PSK*.
- (3) Set **Data Encryption** to *AES*.
- (4) Under **Network Key** and **Confirm Network Key**, enter the configured preshared key.
- (5) Exit each menu with **OK**.



Note

Windows XP allows several menus to be modified. Depending on the configuration, the path to the wireless network connection you want to configure may be different to that described above.

6.6 Software Update

New functions are continuously being added to bintec devices. bintec elmeg GmbH gives you these upgrades free of charge. With the **GUI**, it is easy to check for new software versions and install updates. An existing internet connection is needed for an automatic update.

Proceed as follows:

- (1) Go to the **Maintenance->Software & Configuration** menu.
- (2) Under **Action**, select *Update System Software* and, under **Source Location**, *Latest Software from Update Server*.
- (3) Confirm with **Go**.

Options

Currently Installed Software	
BOSS	V.9.1 Rev. 7 IPSec from 2013/08/01 00:00:00
System Logic	1.0
ADSL Logic	E.74.2.53
Software and Configuration Options	
Action	Update system software ▾
Source Location	Current Software from Update Server ▾

Go

The device will now connect to the bintec elmeg GmbH download server and check whether an updated version of the system software is available. If so, your device will be updated automatically. When installation of the new software is complete, you will be invited to re-start the device.



Caution

After confirming with **Go**, the update cannot be aborted. If an error occurs during the update, do not re-start the device and contact support.

Chapter 7 Access and configuration

This chapter describes all the access and configuration options.

7.1 Access Options

The various access options are presented below. Select the procedure to suit your needs.

There are various ways you can access your device to configure it:

- Via your LAN
- Via the serial interface
- Via an ISDN connection if your device supports ISDN)

7.1.1 Access via LAN

Access via one of the Ethernet interfaces of your device allows you to open the **GUI** in a web browser for configuration purposes and to access your device via Telnet or SSH.



Caution

If you carry out the initial configuration with the **GUI**, this can result in inconsistencies or malfunctions, as soon as you carry out additional settings using other configuration options. Therefore, it is recommended that the configuration is continued with the **GUI**. If you use SNMP shell commands, continue with this configuration method.

7.1.1.1 HTTP/HTTPS

With a current web browser, you can use the HTML interface to configure your device. For this, enter the following in your web browser's address field

- `http://192.168.0.254`
- or
- `https://192.168.0.254`

7.1.1.2 Telnet

Apart from configuration using a web browser, with a Telnet connection you can also access the SNMP shell and use other configuration options.

You do not need any additional software on your PC to set up a Telnet connection to your device: Telnet is available on all operating systems.

Proceed as follows:

Windows

- (1) Click **Run...** in the Windows Start menu.
- (2) Enter `telnet <IP address of your device>`.
- (3) Click **OK**.
A window with the login prompt appears. You are now in the SNMP shell of your device.
- (4) Continue with [Logging in for Configuration](#) on page 36.

Unix

You can also set up a Telnet connection on UNIX and Linux without any problem:

- (1) Enter `telnet <IP address of your device>` in a terminal.
A window with the login prompt appears. You are now in the SNMP shell of your device.
- (2) Continue with [Logging in for Configuration](#) on page 36.

7.1.1.3 SSH

In addition to the unencrypted and potentially viewable Telnet session, you can also connect to your device via an SSH connection. This is encrypted, so all the remote maintenance options can be carried out securely.

The following preconditions must be met in order to connect to the device via SSH:

- The encryption keys needed for the process must be available on the device.
- An SSH client must be installed on your PC.

Encryption keys

First of all, make sure that the keys for encrypting the connection are available on your device:

- (1) Log in to one of the types already available on your device (e.g. via Telnet - for login see [Login](#) on page 35).
- (2) Enter `update -i` for the input prompt. You are now in the Flash Management shell.
- (3) Call up a list of all the files saved on the device: `ls -al`.

If you see a display like the one below, the keys needed are already there and you can

connect to the device via SSH:

```
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 >
```



Note

The device generates a key pair for each of the algorithms (RSA and DSA), i.e. two files must be stored in the flash for each algorithm (see example at above).

If no keys are available, you have to generate these first. Proceed as follows:

- (1) Leave the Flash Management shell with `exit`.
- (2) Launch the **GUI** and log on to your device (see [Calling up GUI](#) on page 39).
- (3) Make sure that *Deutsch* is selected as the language.
- (4) Check the key status in the **System Management->Administrative Access->SSH** menu. If both keys are available, you'll see in both fields **RSA Key Status** and **DSA Key Status** the value *Generated*.
- (5) If one or both of these fields contains the value *Not generated*, you must generate the relevant key. To have the device generate the key, click **Generate**.
The device generates the corresponding key and stores it in the FlashROM. *Generated* indicates successful generation.
- (6) Make sure that both keys have been successfully generated. If necessary, repeat the procedure described above.

Login via SSH

Proceed as follows to log in on your device via SSH:

If you have made sure that all the keys needed are available on the device, you have to check whether an SSH client is installed on your PC. Most UNIX and Linux distributions install a SSH client by default. Additional software, e.g. PuTTY, usually has to be installed on

a Windows PC.

Proceed as follows to log in on your device via SSH:

UNIX

- (1) Enter `ssh <IP address of the device>` in a terminal.
The login prompt window appears. This is located in the SNMP shell of the device.
- (2) Continue with [Login](#) on page 35.

Windows

- (1) How an SSH connection is set up very much depends on the software used. Consult the documentation for the program you are using.
As soon as you have connected to the device, the login prompt window will appear.
You are now in the SNMP shell of your gateway.
- (2) Continue with [Login](#) on page 35.



Note

PuTTY requires certain settings for a connection to a bintec elmeg device. The support pages of <http://www.bintec-elmeg.com> include FAQs, which list the required settings.

7.1.2 Access via the Serial Interface

Each bintec elmeg gateway has a serial interface, with which a PC can be connected directly. The following chapter describes what you have to remember when setting up a serial connection and what you can do to configure your device in this way.

Access via the serial interface is ideal if you are setting up an initial configuration of your device and a LAN access is not possible via the pre-configured IP address (192.168.0.254/255.255.255.0).

Windows

If you are using a Windows PC, you need a terminal program for the serial connection, e.g. HyperTerminal. Make sure that HyperTerminal was also installed on the PC with the Windows installation. However, you can also use any other terminal program that can be set to the corresponding parameters (see below).

Proceed as follows to access your device via the serial interface:

- (1) In the Windows Start menu, click **Programs -> Accessories -> Communication -> HyperTerminal -> Device on COM1** (or **Device on COM2**, if you use the COM2 port

of your PC) to start HyperTerminal.

- (2) Press **Return** (at least once) after the HyperTerminal window opens.

A window with the login prompt appears. You are now in the SNMP shell of your device. You can now log in on your device and start the configuration.

Check

If the login prompt does not appear after you press **Return** several times, the connection to your device has not been set up successfully.

Therefore, check the COM1 or COM2 settings on your PC.

- (1) Click on **File ->Properties**.
- (2) Click **Configure** in the **Connect to** tab.
The following settings are necessary:
 - Bits per second: *9600*
 - Data bits: *8*
 - Parity: *open*
 - Stopbits: *1*
 - Flow control: *open*
- (3) Enter the values and click **OK**.
- (4) Make the following settings in the **Settings** tab:
 - Emulation: *VT100*
- (5) Click **OK**.

The changes to the terminal program settings do not take effect until you disconnect the connection to your device and then make the connection again.

If you use HyperTerminal, there may be problems with displaying umlauts and other special characters. If necessary, therefore, set HyperTerminal to *Autodetection* instead of *VT100*.

Unix

You will require a terminal program such as `cu` (on System V), `tip` (on BSD) or `minicom` (on Linux). The settings for these programs correspond to those listed above.

Example of a command line for using `cu`: `cu: cu -s 9600 -c/dev/ttyS1`

Example of a command line for using `tip`: `tip: tip -9600 /dev/ttyS1`

7.1.3 Access over ISDN

All devices that have an ISDN interface can be accessed and configured from another device via an ISDN call.

Access over ISDN with ISDN Login is especially recommended if your device is to be remotely configured or maintained. This is also possible even if your device is still in the ex works state. Access is then obtained with the aid of a device that is already configured or a PC with an ISDN card in the remote LAN. The device to be configured in your own LAN is reached via a number of the ISDN connection (e.g. 1234). This enables the administrator in the Remote LAN to configure your device remotely, for example.



Note

If you connect an unconfigured device to an ISDN connection in parallel to a PBX, the PBX cannot take any calls until an ISDN number is configured on the device.

Access over ISDN costs money. If your device and your computer are in the LAN, it is cheaper to access your device via the LAN or via the serial interface.

Your device in your LAN merely needs to be connected to the ISDN connection and switched on.

To reach your device over ISDN Login, proceed as follows:

- (1) Connect your device to the ISDN.
- (2) Log in as administrator on your device in the remote LAN in the usual way.
- (3) In the SNMP shell, type in `isdnlogin <number of the ISDN connection of your device>`, e.g. `isdnlogin 1234`.
- (4) The login prompt appears. You are now in the SNMP shell of your device.

Continue with [Logging in for Configuration](#) on page 36.

7.2 Login

With certain access data, you can log in on your device and carry out different actions. The extent of the actions available depend on the authorisations of the user concerned.

A login prompt appears first, regardless of how you access your device. You cannot view any information on the device or change the configuration without authentication.

7.2.1 User names and passwords in ex works state

In its ex works state, your device is provided with the following user names and passwords:

User names and passwords in ex works state

Login name	Password	Authorisations
admin	admin	Read and change system variables, save configurations; use GUI.
write	public	Read and write system variables (except passwords) (changes are lost when you switch off your device).
read	public	Read system variables (except passwords).

It is only possible to change and save configurations if you log in with the user name `admin`. Access information (user names and passwords) can also only be changed if you log in with the user name `admin`. For security reasons, passwords are normally shown on the Setup Tool screen not in plain text, but only as asterisks. The user names, on the other hand, are displayed as plain text.

The security concept of your device enables you to read all the other configuration settings with the user name `read`, but not the access information. It is therefore impossible to log in with `read`, read the password of the `admin` user and subsequently log in with `admin` and make changes to the configuration.



Caution

All bintec elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. How to change the passwords is described in [Passwords](#) on page 58.

Make sure you change the passwords to prevent unauthorised access to your device!

If you have forgotten your password, you must reset your device to the ex works state, which means your configuration will be lost.

7.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in [Access Options](#) on page 30.

GUI (Graphical User Interface)

Log in via the HTML surface as follows:

- (1) Enter your user name in the **User** field of the input window.
- (2) Enter your password in the **Password** field of the input window and confirm with **Return** or click the **Login** button.

The status page of the **GUI** opens in the browser.

SNMP shell

Log into the SNMP shell as follows:

- (1) Enter your user name e.g. `admin`, and confirm with **Return**.
- (2) Enter your user password, e.g. `admin`, and confirm with **Return**.

Your device logs in with the input prompt, e.g. `rs:>`. The login was successful. You are now in the SNMP shell.

To leave the SNMP shell after completing the configuration, enter `exit` and press **Return**.

7.3 Configuration options

This chapter first offers an overview of the various tools you can use for configuration of your device.

You can configure your device in the following ways:

- **GUI**
- Assistant
- SNMP shell commands



Note

The detailed help system of the Wizard will help you to clarify any questions you may have. Therefore the wizard will not be discussed in any greater detail in this document.

The configuration options available to you depend on the type of connection to your device:

Types of connections and configurations

Type of connection	Possible types of configuration
LAN	Assistant, GUI , shell command
Serial connection	Shell command

The following chapters describe the configuration based on **GUI**.

**Note**

To change the device configuration, you must log in with the user name `admin`. If you do not know the password, you cannot make any configuration settings. This applies to all types of configuration.

7.3.1 GUI (Graphical User Interface)

GUI is a web-based graphic user surface that you can use from any PC with an up-to-date Web browser via an HTTP or HTTPS connection.

With the **GUI** you can perform all the configuration tasks easily and conveniently. It is integrated in your device and is available in English. If required, other languages can be downloaded from the download area of www.bintec-elmeg.com and installed on your device. To do this, proceed as described in *Options* on page 480.

The settings you make with the **GUI** are applied with the **OK** or **Apply** button of the menu, and you do not have to restart the device.

If you finish the configuration and want to save your settings so that they are loaded as the boot configuration when you reboot your device, save these by clicking the **Save configuration** button.

You can also use the **GUI** to monitor the most important function parameters of your device.

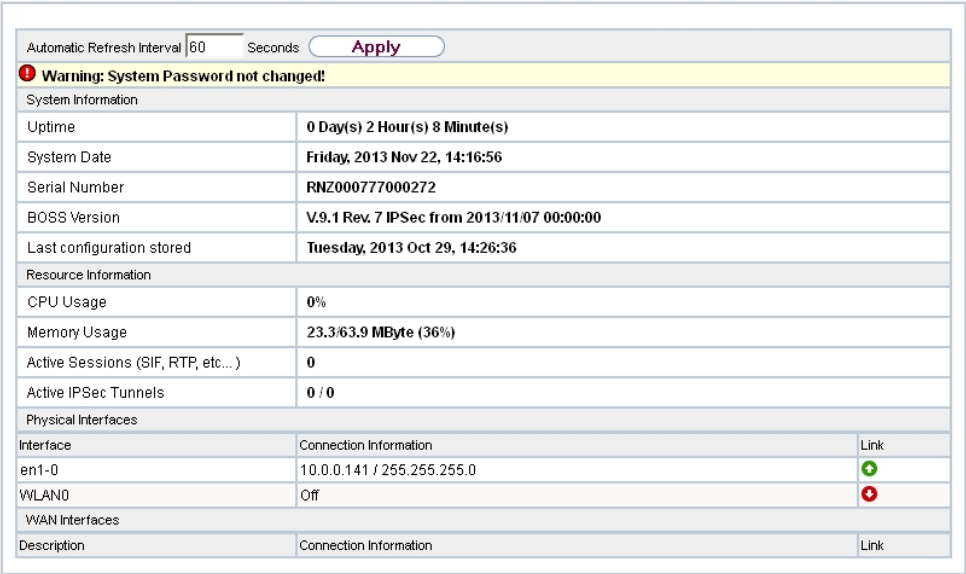


Fig. 15: GUI home page

7.3.1.1 Calling up GUI

- (1) Check whether the device is connected and switched on and that all the necessary cables are correctly connected (see on page).
- (2) Check the settings of the PC from which you want to configure your device (see *Configuring a PC* on page 25).
- (3) Open a web browser.
- (4) Enter `http://192.168.0.254` in the address field of the web browser.
- (5) Enter `admin` in the **User** field and enter `admin` in the **Password** field and click **LOGIN**.

You are not in the status menu of your device's GUI (see *Status* on page 52).

7.3.1.2 Operating elements

GUI window

The GUI window is divided into three areas:

- The header
- The navigation bar
- The main configuration window

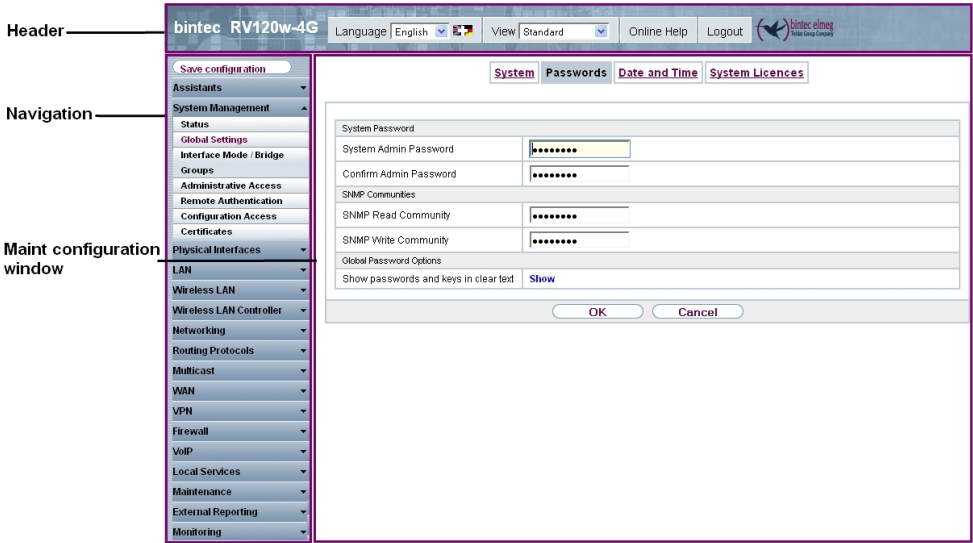


Fig. 16: Areas of the GUI

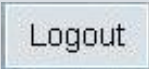
Header



Fig. 17: GUI header

GUI header

Menu	Position
<div>LanguageEnglish</div>	Language: In the dropdown menu, choose the language in which you want to display the GUI . Here you can choose the language in which you perform the configuration. German and English are available.
<div>ViewStandard</div>	View: Select the desired view from the dropdown menu. Stand-ard and SNMP browsers can be selected.
<div>Online Help</div>	Online Help: Click this button if you want help with the menu now active. The description of the sub-menu where you are now is displayed.
	Logout: If you want to end the configuration, click this button to

Menu	Position
	<p>log out of your device. A window is opened offering you the following options:</p> <ul style="list-style-type: none">• Save configuration, save previous boot configuration, then exit.• Save configuration, then exit.• Exit without saving.

Navigation bar



Fig. 18: Save Configuration button

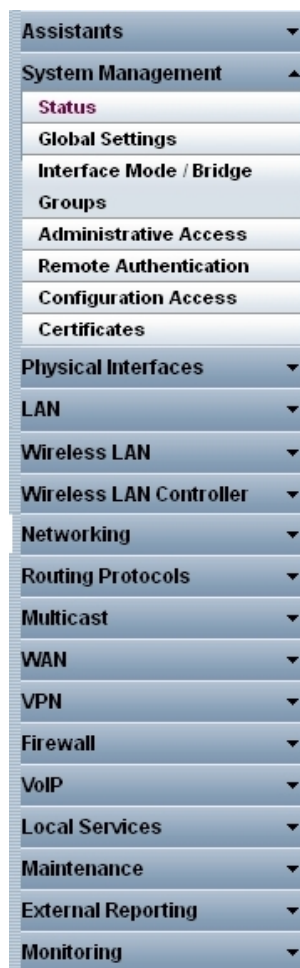


Fig. 19: Menus

The **Save configuration** button is found in the navigation bar.

If you save a current configuration, you can save this as the boot configuration or you can also archive the previous boot configuration as a backup.

If you click the **Save configuration** button in the FCI, you will be asked "Do you really want to save the current configuration as a boot configuration?"

You have the following two options:

- *Save configuration*, i.e. save the current configuration as the boot configuration
- *Save configuration with boot backup* i.e. save current configuration as boot configuration while also archiving previous boot configuration as backup.

If you want to load the archived boot configuration into your device, go to the **Maintenance->Software & Configuration** menu, select **Action = Import configuration** and click on **Go**. The archived backup is used as the current boot configuration.

The navigation bar also contains the main configuration menus and their sub-menus.

Click the main menu you require. The corresponding sub-menu then opens.

If you click the sub-menu you want, the entry selected will be displayed in red. All the other sub-menus will be closed. You can see at a glance the sub-menu you are in.

Status page

If you call the **GUI**, the status page of your device is displayed after you log in. The most important data of your device can be seen on this at a glance.

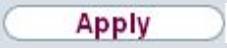

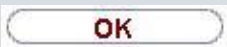



Main configuration window

The sub-menus generally contain several pages. These are called using the buttons at the top of the main window. If you click a button, the window is opened with the basic parameters. You can extend this by clicking the **Advanced Settings** tab, which displays the additional options.


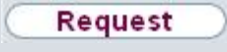


Configuration elements

The various actions that you can perform when configuring your device in the **GUI** are triggered by means of the following buttons:

GUI buttons
















Button	Position
	Updates the view.
	If you do not want to save a newly configured list entry, cancel this and any settings made by pressing Cancel .
	Confirms the settings of a new entry and the parameter changes in a list.
	Immediately starts the configured action.
	Calls the sub-menu to create a new entry.
	Inserts an entry in an internal list.


GUI buttons for special functions

Button	Position
	In the System Management->Certificates->Certificate List menu and the System Management->Certificates->CRLs menu, this button activates the sub-menus for configuration of the certificate or CRL imports.
	In the System Management->Certificates->Certificate List menu, this button activates the sub-menu for the configuration of the certificate request.
	In the Monitoring->ISDN/Modem->Current Calls menu, pressing this button ends the active calls selected in the  column.

Various icons indicate the following possible actions or statuses:

GUI symbols

Symbol	Position
	Deletes the list entry.
	Displays the menu for changing the settings of an entry.
	Displays the details for an entry.
	Moves an entry. A combo box opens in which you can choose the list entry that selected entry is to be placed in front of/after.
	Creates another list entry first and opens the configuration menu.
	Sets the status of the entry to <i>Inactive</i> .
	Sets the status of the entry to <i>Active</i> .
	Indicates "Dormant" status for an interface or connection.
	Indicates "Up" status for an interface or connection.
	Indicates "Down" status for an interface or connection.
	Indicates "Blocked" status for an interface or connection.
	Indicates "Going up" status for an interface or connection.
	Indicates that data traffic is encrypted.
	Triggers a WLAN bandscan.
	Displays the next page in a list.

Symbol	Position
	Displays the previous page in a list.

You can select the following operating functions in the list view:

GUI list options





Menu	Position
Update Interval	Here you can set the interval in which the view is to be updated. To do this, enter a period in seconds in the input field and confirm it with  .
Filter	You can have the list entries filtered and displayed according to certain criteria. You can determine the number of entries displayed per page by entering the required number in View x per page . Use the  and  buttons to scroll one page forward and one page back. You can filter according to certain keywords within the configuration parameters by selecting the filter rule you want under Filter in x <Option> y and entering the search word in the input field.  launches filter operation.
Configuration elements	Some lists contain configuration elements. You can therefore change the configuration of the corresponding list entry directly in the list.



Fig. 20: Configuration of the update interval






Fig. 21: Filter list

Structure of the GUI configuration menu





The menus of the **GUI** contain the following basic structures:


GUI Menu architecture

Menu	Position
Basic configuration menu/list	<p>When you select a menu from the navigation bar, the menu of basic parameters is displayed first. In a sub-menu containing several pages, the menu containing the basic parameters is displayed on the first page.</p> <p>The menu contains either a list of all the configured entries or the basic settings for the function concerned.</p>
Sub-menu 	The New button is available in each menu in which a list of all the configured entries is displayed. Click the button to display the configuration menu for creating a new list entry.
Sub-menu 	Click this button to process the existing list entry. You go to the configuration menu.
Menu 	Click this tab to display extended configuration options.

The following options are available for the configuration:


GUI configuration elements

Menu	Position				
Input fields	<p>e.g. empty text field</p>  <p>Text field with hidden input</p>  <p>Enter the data.</p>				
Radio buttons	<p>e.g.</p>  <p>Select the corresponding option.</p>				
Checkboxes	<p>e.g. activation by selecting checkbox</p>  <p>Selection of several possible options</p> <table><tr><td>Encryption Algorithms</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 Algorithms</td><td><input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD160</td></tr></table>	Encryption Algorithms	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256	Hashing Algorithms	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD160
Encryption Algorithms	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256				
Hashing Algorithms	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD160				
Dropdown menus	e.g.				

Menu	Position
	<div><div>Configured Speed / Mode</div><div><div>Full Autonegotiation</div><div>Full Autonegotiation</div><div>Full Autonegotiation</div><div>Full Autonegotiation</div></div></div> <p>Click the arrow to open the list. Select the required option using the mouse.</p>
Internal lists	<p>e.g.</p> <div><div>Remote IP Address</div><div>Netmask</div><div><div></div><div>255.255.255.0</div><div></div></div><div>Add</div></div> <p>Click Add . A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm with OK. Delete the entries by clicking the  icon.</p>

Display of options that are not available



Options that are not available because they depend on the selection of other options are generally hidden. If the display of these options could be helpful for a configuration decision, they are instead greyed out and cannot be selected.



Important

Please look at the messages displayed in the sub-menus. These provide information on any incorrect configurations.

Warning symbols

Symbol	Meaning
	This symbol appears in messages referring you to settings that were made with the Setup Tool.
	This symbol appears in messages referring you to the fact that values were entered or selected incorrectly.

Pay particular attention to the following message:

"Warning: Changes not supported by the Setup Tool!" If you change them with the **GUI**, this can cause inconsistencies or malfunctions. Therefore, it is recommended that the configuration is continued with the Setup Tool.

7.3.1.3 GUI Menus

The configuration options of your device are contained in the sub-menus, which are displayed in the navigation bar in the left-hand part of the window.



Note

Please note that not all devices have the full range of functions. Check the software of your device on the corresponding product page under www.bintec-elmeg.com.

SNMP Browser

If you select the *SNMP Browser* option under **View** header, you will see an HTML view of all internal system MIB tables and can modify the saved values. This view is only provided for professional configuration and extended monitoring.

SNMP (Simple Network Management Protocol) is a protocol that allows access for configuring your device. All configuration parameters are stored in the MIB (Management Information Base) in the form of MIB tables and MIB variables. You can read and modify these directly via the SNMP browser.



Caution

This configuration method assumes an in-depth system knowledge of bintec devices!

7.3.2 SNMP shell

SNMP (Simple Network Management Protocol) is a protocol that defines how you can access the configuration settings.

All configuration settings are stored in the MIB (Management Information Base) in the form of MIB tables and MIB variables. You can access these directly from the SNMP shell via SNMP commands. This type of configuration requires a detailed knowledge of our devices.

7.4 BOOTmonitor

The BOOTmonitor is only available over a serial connection to the device.

The BOOTmonitor provides the following functions, which you select by entering the corresponding number:

- (1) Boot System (reboot the system):
The device loads the compressed boot file from the flash memory to the working memory. This happens automatically on starting.
- (2) Software Update via TFTP:
The device performs a software update via a TFTP server.
- (3) Software Update via XMODEM:
The device performs a software update via a serial interface with XMODEM.
- (4) Delete configuration:
The device is reset to the ex works state. All configuration files are deleted and the BOOTmonitor settings are set to the default values.
- (5) Default BOOTmonitor Parameters:
You can change the default settings of the BOOTmonitor of the device, e.g. the baud rate for serial connections.
- (6) Show System Information:
Shows useful information about your device, e.g. serial number, MAC address and software versions.

The BOOTmonitor is started as follows.

The device passes through various functional states when starting:

- Start mode
- BOOTmonitor mode
- Normal mode

After some self-tests have been successfully carried out in the start mode, your device reaches the BOOTmonitor mode. The BOOTmonitor prompt is displayed if you are serially connected to your device.

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

```
RV120w-4G Bootmonitor V.7.9 Rev.1 from 2009/10/19 00:00:00
Copyright (c) 1996-2005 by bintec elmeg 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> _
```

After display of the BOOTmonitor prompt, press the space bar within four seconds to use

the functions of the BOOTmonitor. If you do not make an entry within four seconds, the device changes back to normal operating mode.

**Note**

If you change the baudrate (the preset value is 9600 baud), make sure the terminal program used also uses this baudrate. If this is not the case, you will not be able to establish a serial connection to the device.

Chapter 8 Assistants

The **Assistants** menu offers step-by-step instructions for the following basic configuration tasks:

- **First steps**
- **Internet Access**
- **VPN**
- **Wireless LAN**
- **VoIP PBX in LAN**

Choose the corresponding task from the navigation bar and follow the instructions and explanations on the separate pages of the Wizard.

Chapter 9 System Management

The **System Management** menu contains general system information and settings.

You see a system status overview. Global system parameters such as the system name, date/time, passwords and licences are managed and the access and authentication methods are configured.

9.1 Status

If you log into the **GUI**, your device's status page is displayed, which shows the most important system information.

You see an overview of the following data:

- System status
- Your device's activities: Resource utilisation, active sessions and tunnels
- Status and basic configuration of the LAN, WAN, ISDN, and ADSL interfaces
- Information on plugged add-on modules (if any)

You can customise the update interval of the status page by entering the desired period in seconds as **Automatic Refresh Interval** and clicking on the **Apply** button.



Caution

Under **Automatic Refresh Interval** do not enter a value of less than 5 seconds, otherwise the refresh interval of the screen will be too short to make further changes!

Automatic Refresh Interval Seconds Apply

Warning: System Password not changed!

System Information

Uptime	0 Day(s) 2 Hour(s) 8 Minute(s)	
System Date	Friday, 2013 Nov 22, 14:16:56	
Serial Number	RNZ000777000272	
BOSS Version	V.9.1 Rev. 7 IPSec from 2013/11/07 00:00:00	
Last configuration stored	Tuesday, 2013 Oct 29, 14:26:36	

Resource Information

CPU Usage	0%	
Memory Usage	23.3/63.9 MByte (36%)	
Active Sessions (SIF, RTP, etc....)	0	
Active IPSec Tunnels	0 / 0	

Physical Interfaces

Interface	Connection Information	Link
en1-0	10.0.0.141 / 255.255.255.0	<div></div>
WLAN0	Off	<div></div>

WAN Interfaces

Description	Connection Information	Link
-------------	------------------------	------

Fig. 23: System Management->Status

The menu **System Management->Status** consists of the following fields:

Fields in the System Information menu

Field	Value
Uptime	Displays the time past since the device was rebooted.
System Date	Displays the current system date and system time.
Serial Number	Displays the device serial number.
BOSS Version	Displays the currently loaded version of the system software.
Last configuration stored	Displays day, date and time of the last saved configuration (boot configuration in flash).

Fields in the Resource Information menu

Field	Value
CPU Usage	Displays the CPU usage as a percentage.
Memory Usage	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is also displayed in brackets as a percentage.
Active Sessions (SIF, RTP, etc...)	Displays the total of all SIF, TDRC, and IP load balancing sessions.
Active IPSec Tunnels	Displays the number of currently active IPSec tunnels in relation

Field	Value
	to the number of configured IPSec tunnels.

Fields in the Physical Interfaces menu

Field	Value
Interface - Connection Information - Link	<p>The physical interfaces are listed here and their most important settings are shown. The system also displays whether the interface is connected or active.</p> <p>Connection Information for Ethernet interfaces:</p> <ul style="list-style-type: none">• IP address• Netmask <p>Connection Information for ISDN interfaces:</p> <ul style="list-style-type: none">• Configured• Not configured <p>Connection Information for xDSL interfaces:</p> <ul style="list-style-type: none">• Downstream/Upstream Line Speed <p>Connection Information for WLAN interfaces:</p> <p>Access Point Mode:</p> <ul style="list-style-type: none">• Operation Mode: Access Point or Off• The channel used on this wireless module• Number of connected clients• Number of WDS links• Software version of the wireless card <p>Connection Information for UMTS/LTE interfaces:</p> <ul style="list-style-type: none">• <i>SIM insert required</i> appears if no SIM card is inserted.• <i>PIN input required</i> is displayed if the SIM card is inserted, but the PIN has not yet been entered.• <i>Init</i> is displayed while the SIM card is initialized.• If the SIM card is operational, the Network Quality is displayed.

Fields in the WAN Interfaces menu

Field	Value
Description - Connection Information - Link	All the WAN interfaces are listed here and their most important settings are shown. The system also displays whether the interface is active.

9.2 Global Settings

The basic system parameters are managed in the **Global Settings** menu.

9.2.1 System

Your device's basic system data is entered in the **System Management->Global Settings->System** menu.

System

Passwords

Date and Time

System Licences

Basic Settings

System Name

rv120w-4g

Location

Contact

TELDAT

Maximum Number of Syslog Entries

50

Maximum Message Level of Syslog Entries

Information

Maximum Number of Accounting Log Entries

20

Manual WLAN Controller IP Address

LED mode

Status

Power Settings

Power Off Timeout

900

Seconds

OK

Cancel

Fig. 24: **System Management->Global Settings->System**

The **System Management->Global Settings->System** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Value
System Name	Enter the system name of your device. This is also used as the PPP host name.

Field	Value
	<p>A character string with a maximum of 255 characters is possible.</p> <p>The device type is entered as the default value.</p>
Location	Enter the location of your device.
Contact	<p>Enter the relevant contact person. Here you can enter the e-mail address of the system administrator, for example.</p> <p>A character string with a maximum of 255 characters is possible.</p> <p>The default value is <i>bintec elmeg</i>.</p>
Maximum Number of Syslog Entries	<p>Enter the maximum number of syslog messages that are stored internally in the device.</p> <p>Possible values are <i>0</i> to <i>1000</i>.</p> <p>The default value is <i>50</i>.</p> <p>You can display the stored messages in Monitoring->Internal Log.</p>
Maximum Message Level of Syslog Entries	<p>Select the priority of system messages above which a log should be created.</p> <p>System messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level <i>Debug</i>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Emergency</i>: Only messages with emergency priority are recorded. • <i>Alert</i>: Messages with emergency and alert priority are recorded. • <i>Critical</i>: Messages with emergency, alert and critical priority are recorded. • <i>Error</i>: Messages with emergency, alert, critical and error priority are recorded. • <i>Warning</i>: Messages with emergency, alert, critical, error and

Field	Value
	<p>warning priority are recorded.</p> <ul style="list-style-type: none">• <i>Notice</i>: Messages with emergency, alert, critical, error, warning and notice priority are recorded.• <i>Information</i> (default value): Messages with emergency, alert, critical, error, warning, notice and information priority are recorded.• <i>Debug</i>: All messages are recorded.
Maximum Number of Accounting Log Entries	<p>Enter the maximum number of login process entries that are stored internally in the device.</p> <p>Possible values are 0 to 1000.</p> <p>The default value is 20.</p>
Manual WLAN Controller IP Address	<p>This function is only available on devices with a wireless LAN controller.</p> <p>Enter the IP address of the WLAN controller.</p> <p>The value can only be modified if the WLAN controller function is enabled.</p>
LED mode	<p>This function is only available for bintec W1003n, bintec W2003n, bintec W2003n-ext and bintec W2004n.</p> <p>Select the LEDs' lighting behaviour.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>State</i> (default value): Only the status LED flashes once per second.• <i>Flashing</i>: The LEDs display their default behaviour.• <i>Off</i>: All LEDs are disabled.

Fields in the menu Power Settings (for devices with GPS only)

Field	Value
Power Off Timeout	<p>Enter the time, in seconds, for how long the device is to remain switched on after switching the motor off.</p> <p>The default value is 900 seconds.</p>

9.2.2 Passwords

Setting the passwords is another basic system setting.

System

Passwords

Date and Time

System Licences

System Password

System Admin Password

.....

Confirm Admin Password

.....

SNMP Communities

SNMP Read Community

.....

SNMP Write Community

.....

Global Password Options

Show passwords and keys in clear text

Show

OK

Cancel

Fig. 25: **System Management->Global Settings->Passwords**



Note

All bintec elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are not protected against unauthorised use.

Make sure you change the passwords to prevent unauthorised access to the device

If the password is not changed, under **System Management->Status** there appears the warning: "System password not changed!"

The **System Management->Global Settings->Passwords** menu consists of the following fields:

Fields in the System Password menu.

Field	Value
System Admin Password	Enter the password for the user name <code>admin</code> . This password is also used with SNMPv3 for authentication (MD5) and encryption (DES).
Confirm Admin Password	Confirm the password by entering it again.

Fields in the SNMP Communities menu.

Field	Value
SNMP Read Community	Enter the password for the user name <code>read</code> .
SNMP Write Community	Enter the password for the user name <code>write</code> .

Fields in the Global Password Options menu

Field	Value
Show passwords and keys in clear text	<p>Define whether the passwords are to be displayed in clear text (plain text).</p> <p>The function is enabled with <code>Show</code></p> <p>The function is disabled by default.</p> <p>If you activate the function, all passwords and keys in all menus are displayed and can be edited in plain text.</p> <p>One exception is IPSec keys. They can only be entered in plain text. If you press OK or call the menu again, they are displayed as asterisks.</p>

9.2.3 Date and Time

You need the system time for tasks such as correct timestamps for system messages, accounting or IPSec certificates.

System

Passwords

Date and Time

System Licences

Basic Settings

Time Zone

Europe/Berlin

Current Local Time

Thursday, 2013 Oct 24, 17:51:33

Manual Time Settings

Set Date

Day

Month

Year

Set Time

Hour

Minute

Automatic Time Settings (Time Protocol)

First Timeserver

SNTP

Second Timeserver

SNTP

Third Timeserver

SNTP

Time Update Interval

1440

Minute(s)

Time Update Policy

Normal

Internal Time Server

☐ Enabled

Time Settings (GPS)

Time Update Interval

☐ Enabled

OK

Cancel

Fig. 26: System Management->Global Settings->Date and Time

You have the following options for determining the system time (local time):

ISDN/Manual

In devices with an ISDN interface, the system time can be updated via ISDN, i. e. the date and time are taken from the ISDN when the first outgoing call is made. The time can also be set manually on the device.

If the correct location of the device (country/city) is set for the **Time Zone**, switching from summer time to winter time (and back) is automatic. This is independent of the exchange time or the ntp server time. Summer time starts on the last Sunday in March by switching from 2 a.m. to 3 a.m. The calendar-related or schedule-related switches that are scheduled for the missing hour are then carried out. Winter time starts on the last Sunday in October by switching from 3 a.m. to 2 a.m. The calendar-related or schedule-related switches that are scheduled for the additional hour are then carried out.

If a value other than Universal Time Coordinated (UTC), option *UTC+-x*, has been chosen for the **Time Zone**, the switch from summer to winter time must be carried out manually when required.

Time server

60

bintec RV Series

You can obtain the system time automatically, e.g. using various time servers. To ensure that the device uses the desired current time, you should configure one or more time servers. Switching from summer time to winter time (and back) must be carried out manually if the time is derived using this method by changing the value in the **Time Zone** field with an option UTC+ or UTC-.



Note

If a method for automatically deriving the time is defined on the device, the values obtained in this way automatically have higher priority. A manually entered system time is therefore overwritten.

The menu **System Management->Global Settings->Date and Time** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Time Zone	Select the time zone in which your device is installed. You can select Universal Time Coordinated (UTC) plus or minus the deviation in hours or a predefined location, e. g. <i>Europe/Berlin</i> .
Current Local Time	The current date and current system time are shown here. The entry cannot be changed.

Fields in the menu Manual Time Settings

Field	Description
Set Date	Enter a new date. Format: <ul style="list-style-type: none">• Day: dd• Month: mm• Year: yyyy
Set Time	Enter a new time. Format: <ul style="list-style-type: none">• Hour: hh• Minute: mm

Fields in the menu Automatic Time Settings (Time Protocol)

Field	Description
ISDN Timeserver	<p>Only for devices with an ISDN interface.</p> <p>Determine whether the system time is to be updated via ISDN.</p> <p>If a time server is configured, the time is only determined over ISDN until a successful update is received from this time server. Updating over ISDN is deactivated for the period in which the time is determined by means of a time server.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
First Timeserver	<p>Enter the primary time server, by using either a domain name or an IP address.</p> <p>In addition, select the protocol for the time server request.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123. • <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37. • <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37. • <i>None</i>: This time server is not currently used for the time request.
Second Timeserver	<p>Enter the secondary time server, by using either a domain name or an IP address.</p> <p>In addition, select the protocol for the time server request.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123. • <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37. • <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37.

Field	Description
	<ul style="list-style-type: none">• <i>None</i>: This time server is not currently used for the time request.
Third Timeserver	<p>Enter the third time server, by using either a domain name or an IP address.</p> <p>In addition, select the protocol for the time server request.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123.• <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37.• <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37.• <i>None</i>: This time server is not currently used for the time request.
Time Update Interval	<p>Enter the time interval in minutes at which the time is automatically updated.</p> <p>The default value is <i>1440</i>.</p>
Time Update Policy	<p>Enter the time period after which the system attempts to contact the time server again following a failed time update.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Normal</i> (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes.• <i>Aggressive</i>: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds.• <i>Endless</i>: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. <p>If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for Time Update Policy, select the value <i>Endless</i>.</p>

Field	Description
Internal Time Server	<p>Select whether the internal timeserver is to be used.</p> <p>The function is activated by selecting <i>Enabled</i>. Time requests from a client will be answered with the current system time. This is given as GMT, without offset.</p> <p>The function is disabled by default. Time requests from a client are not answered.</p>

Fields in the menu Time Settings (GPS) (for devices with GPS only)

Field	Description
Time Update Interval	<p>Select whether the device is to receive the system time via GPS.</p> <p>If appropriate, enter the time (in seconds) for updating the system time via GPS.</p> <p>The value 0 (default value) means that the system time is updated every time the GPS is fixed.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

9.2.4 System Licences

This chapter describes how to activate the functions of the software licences you have purchased.

The following licence types exist:

- Licences already available in the device's ex works state
- Free extra licences
- Extra licences at additional cost

The data sheet for your device tells you which licences are available in the device's ex works state and which can also be obtained free of charge or at additional cost. You can access this data sheet at www.bintec-elmeg.com.

Entering licence data

You can obtain the licence data for extra licences via the online licensing pages in the sup-

port section at www.bintec-elmeg.com . Please follow the online licensing instructions. (Please also note the information on the licence card for licences at additional cost.) You will then receive an e-mail containing the following data:

- **Licence Key** and
- **Licence Serial Number**.

You enter this data in the **System Management->Global Settings->System Licences->New** menu.

In the **System Management->Global Settings->System Licences->New** menu, a list of all registered licences is displayed (**Description, Licence Type, Licence Serial Number, Status**).

Possible values for Status

Licence	Meaning
OK	Subsystem is activated.
Not OK	Subsystem is not activated.
Not supported	You have entered a licence for a subsystem your device does not support.


In addition, above the list is shown the **System Licence ID** required for online licensing.



Note

To restore the standard licences for a device, click the **Default Licences** button (standard licences).

9.2.4.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter more licences.

System

Passwords

Date and Time

Timer

System Licences

Basic Settings

Licence Serial Number

Licence Key

OK

Cancel

Fig. 27: **System Management->Global Settings->System Licences->New**

Activating extra licences

You activate extra licences by adding the received licence information in the **System Management->Global Settings->System Licences->New** menu.

The menu **System Management->Global Settings->System Licences->New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Value
Licence Serial Number	Enter the licence serial number you received when you bought the licence.
Licence Key	Enter the licence key you received by e-mail.



Note


If *Not OK* is displayed as the status:

- Enter the licence data again.
- Check your hardware serial number.

If *Not Supported* is displayed as the status, you have entered a license for a sub-system that your device does not support. This means you cannot use the functions of this licence.

Deactivating a licence

Proceed as follows to deactivate a licence:

- (1) Go to **System Management->Global Settings->System Licences->New**.
- (2) Press the  icon in the line containing the licence you want to delete.
- (3) Confirm with **OK**.

The licence is deactivated. You can reactivate your additional licence at any time by entering the valid licence key and licence serial number.

9.3 Interface Mode / Bridge Groups

In this menu, you define the operation mode for your device's interfaces.

Routing versus bridging

Bridging connects networks of the same type. In contrast to routing, bridges operate at layer 2 of the OSI model (data link layer), are independent of higher-level protocols and transmit data packets using MAC addresses. Data transmission is transparent, which means the information contained in the data packets is not interpreted.

With routing, different networks are connected at layer 3 (network layer) of the OSI model and information is routed from one network to the other.

Conventions for port/interface names

If your device has a radio port, it receives the interface name WLAN. If there are several radio modules, the names of wireless ports in the user interface of your device are made up of the following parts:

- (a) WLAN
- (b) Number of the physical port (1 or 2)

Example: *WLAN1* The name of the Ethernet port is made up of the following parts:

- (a) ETH
- (b) Number of the port

Example: *ETH1*

The name of the interface connected to an Ethernet port is made up of the following parts:

- (a) Abbreviation for interface type, whereby *en* stands for internet.
- (b) Number of the Ethernet port
- (c) Number of the interface

Example: *en1-0* (first interface on the first Ethernet port)

The name of the bridge group is made up of the following parts:

- (a) Abbreviation for interface type, whereby *br* stands for bridge group.
- (b) Number of the bridge group

Example: *br0* (first bridge group)

The name of the wireless network (VSS) is made up of the following parts:

Abbreviation for interface type, whereby *vss* stands for wireless network.

- (a) Number of the wireless module
- (b) Number of the interface

Example: *vss1-0* (first wireless network on the first wireless module)

The name of the WDS link or bridge link is made up of the following parts:

- (a) Abbreviation for interface type
- (b) Number of the wireless module on which the WDS link or bridge link is configured
- (c) Number of the WDS link or bridge link

Example: *wds1-0* (first WDS link or bridge link on the first wireless module)

The name of the client link is made up of the following parts:

- (a) Abbreviation for interface type
- (b) Number of the wireless module on which the client link is configured
- (c) Number of the client link

Example: *sta1-0* (first client link on the first wireless module)

The name of the virtual interface connected to an Ethernet port is made up of the following parts:

- (a) Abbreviation for interface type
- (b) Number of the Ethernet port
- (c) Number of the interface connected to the Ethernet port
- (d) Number of the virtual interface

Example: *en1-0-1* (first virtual interface based on the first interface on the first Ethernet port)

9.3.1 Interfaces

You define separately whether each interface is to operate in routing or bridging mode.

If you want to set bridging mode, you can either use existing bridge groups or create a new bridge group.

The default setting for all existing interfaces is routing mode. When selecting the option *New Bridge Group* for **Mode / Bridge Group**, a bridge group, i.e. *br0*, *br1* etc. is automatically created and the interface is run in bridging mode.

Interfaces

#	Interface Description	Mode / Bridge Group
1	en1-0	Routing Mode
2	en1-4	Routing Mode

Configuration Interface Select one

OKCancel

Fig. 28: **System Management->Interface Mode / Bridge Groups->Interfaces**

The **System Management->Interface Mode / Bridge Groups->Interfaces** menu consists of the following fields:

Fields in the Interfaces menu.

Field	Description
Interface Description	Displays the name of the interface.
Mode / Bridge Group	Select whether you want to run the interface in <i>Routing Mode</i> or whether you want to assign the interface to an existing (<i>br0</i> , <i>br1</i> etc.) or new bridge group (<i>New Bridge Group</i>). When selecting <i>New Bridge Group</i> , a new bridge group is automatically created after you click the OK button.
Configuration Interface	Select the interface via which the configuration is to be carried out. Possible values: <ul style="list-style-type: none">• <i>Select one</i> (default value): Ex works setting The right configuration interface must be selected from the other options.• <i>Ignore</i>: No interface is defined as configuration interface.• <i><Interface name></i>: Select the interface to be used for configuration. If this interface is in a bridge group, it is assigned the group's IP address when it is taken out of the group.

9.3.1.1 Add or Edit

Add

Choose the **Add** button to edit the mode of PPP interfaces.

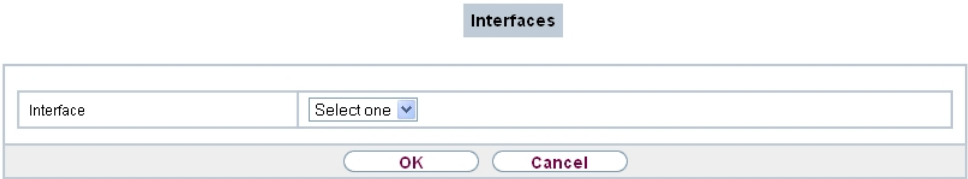



Fig. 29: **System Management->Interface Mode / Bridge Groups->Interfaces->Add**

The **System Management->Interface Mode / Bridge Groups->Interfaces->Add** menu consists of the following fields:

Fields in the Interfaces menu.

Field	Description
Interface	Select the interface whose status should be changed.

Edit for devices the Wlxxxxn and RS series

For WLAN clients in bridge mode (so-called MAC Bridge) you can also edit additional settings via the  icon.

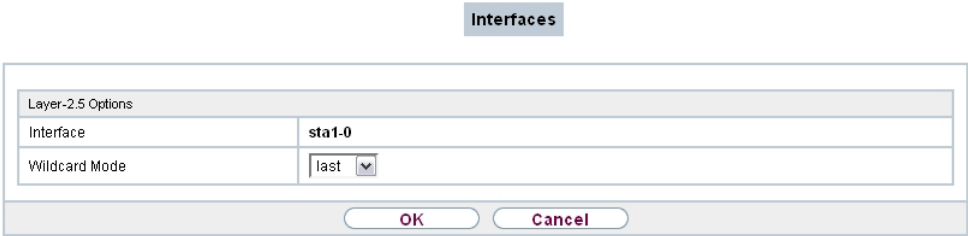



Fig. 30: **System Management->Interface Mode / Bridge Groups->Interfaces->Add**

You can realise bridging for devices behind access clients with the MAC Bridge function. In wildcard mode you cannot define how Unicast non-IP frames or non-ARP frames are processed. To use the MAC bridge function, you must carry out configuration steps in several menus.

- (1) Select **GUI menu Wireless LAN->WLAN->Radio Settings** and click the icon to modify an entry.
- (2) Select **Operation Mode = Access Client** and save the settings with **OK**.
- (3) Select the **System Management->Interface Mode / Bridge Groups->Interfaces** menu. The additional interface **sta1-0** is displayed.
- (4) For interface **sta1-0** select Mode / Bridge Group = *br0 (<IPAddress>)* and **Configuration Interface= en1-0** and save the settings with **OK**.
- (5) Click the **Save configuration** button to save all of the configuration settings. You can

use the MAC Bridge.

The **System Management->Interface Mode / Bridge Groups->Interfaces->** menu consists of the following fields:

Fields in the Layer-2.5 Options menu.

Field	Value
Interface	Shows the interface that is being edited.
Wildcard Mode	<p>Select the Wildcard mode you want to use on the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>none</i> (default value): Wildcard mode is not used.• <i>static</i>: With this setting, you must enter the MAC address of a device that is connected over IP under Wildcard MAC Address. Each packet without IP and without ARP is forwarded to this device. This occurs even when the device is no longer connected.• <i>first</i>: If you choose this setting, the MAC address of the first non-IP unicast frame or non-ARP unicast frame, which occurs on any of the Ethernet interfaces, is used as the wildcard MAC address. This wildcard MAC address can only be reset by rebooting the device or by selecting another wildcard mode.• <i>last</i>: If you choose this setting, the internal WLAN MAC address is used to establish a connection to the access point. As soon as a non-IP unicast frame or non-ARP unicast frame appears, it is forwarded to the MAC address from which the last non-IP unicast frame or non-ARP unicast frame was received on the Ethernet interface of the device. This wildcard MAC address is renewed with each non-IP unicast frame or non-ARP unicast frame.
Wildcard MAC Address	<p>Only for Wildcard Mode = <i>static</i></p> <p>Enter the MAC address of a device that is connected over IP.</p>
Transparent MAC Address	<p>Only for Wildcard Mode = <i>static, first</i></p> <p>Choose whether or not the Wildcard MAC Address are used in addition as WLAN MAC address to establish the connection to the access point.</p>

Field	Value
	The function is enabled with <i>Enabled</i> .
	The function is disabled by default.

9.4 Administrative Access

In this menu, you can configure the administrative access to the device.

9.4.1 Access

In the **System Management->Administrative Access->Access** menu, a list of all IP-capable interfaces is displayed.

AccessSSHSNMP

ⓘ Administrative access is currently unrestricted. The displayed configuration is not yet activated.

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

Advanced Settings

Restore Default Settings

Add

OK

Cancel


Fig. 31: **System Management->Administrative Access->Access**

For an Ethernet interface you can select the access parameters *Telnet*, *SSH*, *HTTP*, *HTTPS*, *Ping*, *SNMP* and for the ISDN interfaces *ISDN Login*.

Only for **hybird** devices: You can also authorise your device for maintenance work from bintec elmeg's Customer Service department. You do this you enable either **Service Login (ISDN Web-Access)** or **Service Call Ticket (SSH Web Access)**, depending on the service you require, and select the **OK** button. Follow the instructions given by Telekom's Customer Service!

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Restore Default Settings	Only when you make changes to the administrative access configuration are relevant access rules set up and activated. You can restore the default settings with the  icon.

9.4.1.1 Add

Select the **Add** button to configure administrative access for additional interfaces.

AccessSSHSNMP

Interface

Select one

OK

Cancel

Fig. 32: **System Management->Administrative Access->Access->Add**

The **System Management->Administrative Access->Access->Add** menu consists of the following fields:

Fields in the menu Access

Field	Description
Interface	Select the interface for which administrative access is to be configured.

9.4.2 SSH

Your devices offers encrypted access to the shell. You can enable or disable this access in the **System Management->Administrative Access->SSH Enabled** menu (standard value). You can also access the options for configuring the SSH login.

AccessSSHSNMP

SSH (Secure Shell) Parameters

SSH service active	<input checked="" type="checkbox"/> Enabled
SSH Port	<input type="text" value="22"/>
Maximum number of concurrent connections	<input type="text" value="1"/>

Authentication and Encryption Parameters

Encryption Algorithms	<input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> Blowfish <input checked="" type="checkbox"/> AES-128 <input type="checkbox"/> AES-256
Hashing Algorithms	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA-1 <input checked="" type="checkbox"/> RipeMD 160

Key Status

RSA Key Status	Generated
DSA Key Status	Not generated [Generate]

Advanced Settings

Login Grace Time	<input type="text" value="600"/> Seconds
Compression	<input type="checkbox"/> Enabled
TCP Keepalives	<input checked="" type="checkbox"/> Enabled
Logging Level	<input type="text" value="Information"/>


OKCancel

Fig. 33: **System Management->Administrative Access->SSH**

You need an SSH client application, e.g. PuTTY, to be able to reach the SSH Daemon.

If you wish to use SSH Login together with the PuTTY client, you may need to comply with some special configuration requirements, for which we have prepared FAQs. You will find these in the Service/Support section at www.bintec-elmeg.com.

To be able to reach the shell of your device via an SSH client, make sure the settings for the SSH Daemon and SSH client are the same.



Note

If configuration of an SSH connection is not possible, restart the device to initialise the SSH Daemon correctly.

The **System Management->Administrative Access->SSH** menu consists of the following fields:

Fields in the menu SSH (Secure Shell) Parameters

Field	Value
SSH service active	Select whether the SSH Daemon is to be enabled for the inter-

Field	Value
	face. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.
SSH Port	Here you can enter the port via which the SSH connection is to be established. The default value is <i>22</i> .
Maximum number of concurrent connections	Enter the maximum number of simultaneously active SSH connections. The default value is <i>1</i> .

Fields in the menu Authentication and Encryption Parameters

Field	Value
Encryption Algorithms	Select the algorithms that are to be used to encrypt the SSH connection. Possible options: <ul style="list-style-type: none">• <i>3DES</i>• <i>Blowfish</i>• <i>AES-128</i>• <i>AES-256</i> By default <i>3DES</i> , <i>Blowfish</i> and <i>AES-128</i> are enabled.
Hashing Algorithms	Select the algorithms that are to be available for message authentication of the SSH connection. Possible options: <ul style="list-style-type: none">• <i>MD5</i>• <i>SHA-1</i>• <i>RipeMD 160</i> By default <i>MD5</i> , <i>SHA-1</i> and <i>RipeMD 160</i> are enabled.

Fields in the menu Key Status

Field	Value
RSA Key Status	<p>Shows the status of the RSA key.</p> <p>If an RSA key has not been generated yet, <i>Not generated</i> is displayed in red and a link, <i>Generate</i>, is provided. If you select the link, the generation process is triggered and the view is updated. The <i>Generating</i> status is displayed in green. When generation has been completed successfully, the status changes from <i>Generating</i> to <i>Generated</i>. If an error occurs during the generation, <i>Not generated</i> and the <i>Generate</i> link are displayed again. You can then repeat generation.</p> <p>If the <i>Unknown</i> status is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.</p>
DSA Key Status	<p>Shows the status of the DSA key.</p> <p>If no DSA key has yet been generated, <i>Not generated</i> is displayed in red and a link, <i>Generate</i>, is provided. If you select the link, the generation process is triggered and the view is updated. The <i>Generating</i> status is displayed in green. When generation has been completed successfully, the status changes from <i>Generating</i> to <i>Generated</i>. If an error occurs during the generation, <i>Not generated</i> and the <i>Generate</i> link are displayed again. You can then repeat generation.</p> <p>If the <i>Unknown</i> status is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Value
Login Grace Time	<p>Enter the time (in seconds) that is available for establishing the connection. If a client cannot be successfully authenticated during this time, the connection is terminated.</p> <p>The default value is <i>600</i> seconds.</p>
Compression	<p>Select whether data compression should be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p>

Field	Value
	The function is disabled by default.
TCP Keepalives	<p>Select whether the device is to send keepalive packets.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Logging Level	<p>Select the syslog level for the syslog messages generated by the SSH Daemon.</p> <p>Possible settings:</p> <ul style="list-style-type: none">• <i>Information</i> (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded.• <i>Fatal</i>: Only fatal errors of the SSH Daemon are recorded.• <i>Error</i>: Fatal and simple errors of the SSH Daemon are recorded.• <i>Debug</i>: All messages are recorded.

9.4.3 SNMP

SNMP (Simple Network Management Protocol) is a network protocol used to monitor and control network elements (e.g. routers, servers, switches, printers, computers etc.) from a central station. SNMP controls communication between the monitored devices and monitoring station. The protocol describes the structure of the data packets that can be transmitted, as well as the communication process.

The data objects queried via SNMP are structured in tables and variables and defined in the MIB (Management Information Base). This contains all the configuration and status variables of the device.

SNMP can be used to perform the following network management tasks:

- Surveillance of network components
- Remote controlling and configuration of network components
- Error detection and notification

You use this menu to configure the use of SNMP.

AccessSSHSNMP

Basic Settings

SNMP Version

☒v1☒v2c☒v3

SNMP Listen UDP Port

161

OK

Cancel

Fig. 34: **System Management->Administrative Access->SNMP**

The menu **System Management->Administrative Access->SNMP** consists of the following fields:

Fields in the Basic Settings menu.

Field	Value
SNMP Version	<div>Select the SNMP version your device is to use to listen for external SNMP access.</div> <div>Possible values:</div> <div><ul style="list-style-type: none">v1: SNMP Version 1v2c: Community-Based SNMP Version 2v3: SNMP Version 3</div> <div>By default, v1, v2c and v3 are enabled.</div> <div>If no option is selected, the function is deactivated.</div>
SNMP Listen UDP Port	<div>Shows the UDP port (161) at which the device receives SNMP requests.</div> <div>The value cannot be changed.</div>



Tip

If your SNMP Manager supports SNMPv3, you should, if possible, use this version as older versions transfer all data unencrypted.

9.5 Remote Authentication

This menu contains the settings for user authentication.

9.5.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) is a service that enables authentication and configuration information to be exchanged between your device and a RADIUS server. The RADIUS server administrates a database with information about user authentication and configuration and for statistical recording of connection data.

RADIUS can be used for:

- Authentication
- Accounting
- Exchange of configuration data

For an incoming connection, your device sends a request with user name and password to the RADIUS server, which then searches its database. If the user is found and can be authenticated, the RADIUS server sends corresponding confirmation to your device. This confirmation also contains parameters (called RADIUS attributes), which your device uses as WAN connection parameters.

If the RADIUS server is used for accounting, your device sends an accounting message at the start of the connection and a message at the end of the connection. These start and end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets

The following types of packets are sent between the RADIUS server and your device (client):


Packet types

Field	Value
ACCESS_REQUEST	Client -> Server If an access request is received by your device, a request is sent to the RADIUS server if no corresponding connection partner has been found on your device.
ACCESS_ACCEPT	Server -> Client If the RADIUS server has authenticated the information contained in the ACCESS_REQUEST, it sends an ACCESS_ACCEPT to your device together with the parameters used for setting up the connection.

Field	Value
ACCESS_REJECT	<p>Server -> Client</p> <p>If the information contained in the ACCESS_REQUEST does not correspond to the information in the user database of the RADIUS server, it sends an ACCESS_REJECT to reject the connection.</p>
ACCOUNTING_START	<p>Client -> Server</p> <p>If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the start of each connection.</p>
ACCOUNTING_STOP	<p>Client -> Server</p> <p>If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the end of each connection.</p>

A list of all entered RADIUS servers is displayed in the **System Management->Remote Authentication->RADIUS** menu.

9.5.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to add RADIUS servers.

RADIUS

TACACS+

Options

Basic Parameters

Authentication Type

PPP Authentication

Server IP Address

RADIUS Secret

••••••••

Default User Password

••••••••

Priority

0

Entry active

☒ Enabled

Group Description

Default Group 0

Advanced Settings

Policy

Authoritative

UDP Port

1812

Server Timeout

1000

Milliseconds

Alive Check

☒ Enabled

Retries

1

RADIUS Dialout

☐ Enabled

Reload Interval

0

Seconds

OK

Cancel

Fig. 35: **System Management->Remote Authentication->RADIUS->New**

The **System Management->Remote Authentication->RADIUS->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Value
Authentication Type	<div>Select what the RADIUS server is to be used for.</div> <div>Possible values:</div> <ul style="list-style-type: none">• <i>PPP Authentication</i> (default value only for PPP connections): The RADIUS server is used for controlling access to a network.• <i>Accounting</i> (for PPP connections only): The RADIUS server is used for recording statistical call data.• <i>Login Authentication</i>: The RADIUS server is used for controlling access to the SNMP shell of your device.• <i>IPSec Authentication</i>: The RADIUS server is used for sending configuration data for IPSec peers to your device.

Field	Value
	<ul style="list-style-type: none"> • <i>WLAN (802.1x)</i>: The RADIUS server is used for controlling access to a wireless network. • <i>XAUTH</i>: The RADIUS server is used for authenticating IPsec peers via XAuth.
Vendor Mode	<p>Only for Authentication Type = <i>Accounting</i></p> <p>In hotspot applications, select the mode define by the provider.</p> <p>In standard applications, leave the value set to <i>Default</i>.</p> <p>Possible values for hotspot applications:</p> <ul style="list-style-type: none"> • <i>France Telecom</i>: For France Telecom hotspot applications. • <i>bintec HotSpot Server</i>: For hotspot applications.
Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Secret	Enter the shared password used for communication between the RADIUS server and your device.
Default User Password	Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server.
Priority	<p>If a number of RADIUS server entries were created, the server with the highest priority is used first. If this server does not answer, the server with the next-highest priority is used.</p> <p>Possible values from <i>0</i> (highest priority) to <i>7</i> (lowest priority).</p> <p>The default value is <i>0</i>.</p> <p>See also Policy in the Advanced Settings.</p>
Entry active	<p>Select whether the RADIUS server configured in this entry is to be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Group Description	Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS

Field	Value
	<p>servers for a group are queried according to Priority and the Policy .</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>New</i> (default value): Enter a new group description in the text field.• <i>Default Group 0</i>: Select this entry for special applications, such as Hotspot Server configuration.• <i><Group Name></i>: Select a predefined group from the list.

The **Advanced Settings** menu consists of the following fields:

Fields in the Advanced Settings menu.

Field	Value
Policy	<p>Select how your device is to react if a negative response to a request is received.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Authoritative</i> (default value): A negative response to a request is accepted.• <i>Non-authoritative</i> : A negative response to a request is not accepted. A request is sent to the next RADIUS server until your device receives a response from a server configured as authoritative.
UDP Port	<p>Enter the UDP port to be used for RADIUS data.</p> <p>RFC 2138 defines the default ports 1812 for authentication (1645 in older RFCs) and 1813 for accounting (1646 in older RFCs). You can obtain the port to be used from the documentation for your RADIUS server.</p> <p>The default value is <i>1812</i>.</p>
Server Timeout	<p>Enter the maximum wait time between ACCESS_REQUEST and response in milliseconds.</p> <p>After timeout, the request is repeated according to Retries or the next configured RADIUS server is requested.</p> <p>Possible values are whole numbers between <i>50</i> and <i>50000</i>.</p>

Field	Value
	The default value is <i>1000</i> (1 second).
Alive Check	<p>Here you can activate a check of the accessibility of a RADIUS server in Status <i>Down</i> .</p> <p>An Alive Check is carried out regularly (every 20 seconds) by sending an ACCESS_REQUEST to the IP address of the RADIUS server. If the server is reachable, Status is set to <i>alive</i> again. If the RADIUS server is only reachable over a switched line (dialup connection), this can cause additional costs if the server is <i>down</i> for a long time.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Retries	<p>Enter the number of retries for cases when there is no response to a request. If an response has still not been received after these attempts, the Status is set to <i>down</i>. In Alive Check = <i>Enabled</i> your device attempts to reach the server every 20 seconds. If the server responds, Status is set back to <i>alive</i> .</p> <p>Possible values are whole numbers between <i>0</i> and <i>10</i>.</p> <p>The default value is <i>1</i>. To prevent Status being set to <i>down</i>, set this value to <i>0</i>.</p>
RADIUS Dialout	<p>Only for Authentication Type = <i>PPP Authentication</i> and <i>IPSec Authentication</i>.</p> <p>Select whether your device receives requests from RADIUS server dialout routes. This enables temporary interfaces to be configured automatically and your device can initiate outgoing connections that are not configured permanently.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If the function is active, you can enter the following options:</p> <ul style="list-style-type: none"> • <i>Reload Interval</i>: Enter the time period in seconds between update intervals. <p>The default entry here is <i>0</i> i.e. an automatic reload is not car-</p>

Field	Value
	ried out.

9.5.2 TACACS+

TACACS+ permits access control for your device, network access servers (NAS) and other network components via one or more central servers.

Like RADIUS, TACACS+ is an AAA protocol and offers authentication, authorisation and accounting services (TACACS+ Accounting is currently not supported by bintec elmeg devices).


The following TACACS+ functions are available on your device:

- Authentication for login shell
- Command authorisation on the shell (e.g. telnet, show)

TACACS+ uses TCP port 49 and establishes a secure and encrypted connection.

A list of all entered TACACS+ servers is displayed in the **System Management->Remote Authentication->TACACS+** menu.

9.5.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to add TACACS+ servers.

RADIUS

TACACS+

Options

Basic Parameters

Authentication Type

Login Authentication

Server IP Address

TACACS+ Secret

••••••••

Priority

0

Entry active

☒ Enabled

Advanced Settings

Policy

Non-authoritative

TCP Port

49

Timeout

3

Seconds

Block Time

60

Seconds

Encryption

☒ Enabled

OK

Cancel

Fig. 36: **System Management->Remote Authentication->TACACS+ ->New**

The **System Management->Remote Authentication->TACACS+ ->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Authentication Type	<p>Displays which TACACS+ function is to be used. The value cannot be changed.</p> <p>Possible values:</p> <ul style="list-style-type: none"><i>Login Authentication</i>: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.
Server IP Address	<p>Enter the IP address of the TACACS+ server that is to be requested for login authentication.</p>
TACACS+ Secret	<p>Enter the password to be used to authenticate and, if applicable, encrypt data exchange between the TACACS+ server and the network access server (your device). The maximum length of the entry is 32 characters.</p>
Priority	<p>Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login</p>

Field	Description
	authentication. If no response is given or access is denied (only if Policy = <i>Non-authoritative</i>), the entry with the next-highest priority is used. The available values are 0 to 9, the default value is 0.
Entry active	Select whether this server is to be used for login authentication. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Policy	Select the interpretation of the TACACS+ response. Possible values: <ul style="list-style-type: none">• <i>Non-authoritative</i> (default value): The TACACS+ servers are queried in order of their priority (see Priority) until a positive response is received or a negative response has been received from an authoritative server.• <i>Authoritative</i>: A negative response to a request is accepted, i.e. a request is not sent to another TACACS+ server. The device's internal user administration is not turned off by TACACS+. It is checked after all TACACS+ servers have been queried.
TCP Port	Shows the default TCP port (49) used for the TACACS+ protocol. The value cannot be changed.
Timeout	Enter time in seconds for which the NAS is to wait for a response from TACACS+. If a response is not received during the wait time, the next configured TACACS+ server is queried (only if Policy = <i>Non-authoritative</i>) and the status of the current server is set to <i>Blocked</i> . The possible values are 1 to 60, the default value is 3.

Field	Description
Block Time	<p>Enter the time in seconds for which the status of the current server shall remain blocked.</p> <p>When the block has ended, the server is set to the status specified in the Entry active field.</p> <p>The possible values are 0 to 3600, the default value is 60. The value 0 means that the server is never set to <i>Blocked</i> status and thus no other servers are queried.</p>
Encryption	<p>Select whether data exchange between the TACACS+ server and the NAS is to be encrypted with MD5.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>If the function is not enabled, the packets and all related information are transferred unencrypted. Unencrypted transfer is not recommended as a default setting and should only be used for debugging.</p>

9.5.3 Options

This setting possible here causes your device to carry out authentication negotiation for incoming calls, if it cannot identify the calling party number (e.g. because the remote terminal does not signal the calling party number). If the data (password, partner PPP ID) obtained by executing the authentication protocol is the same as the data of a listed remote terminal or RADIUS user, your device accepts the incoming call.

RADIUSTACACS+Options

Global RADIUS Options

Authentication for PPP Dialin

☒ Inband
☐ Outband (CLID)

OK

Cancel

Fig. 37: **System Management->Remote Authentication->Options**

The menu **System Management->Remote Authentication->Options** consists of the following fields:

Fields in the Global RADIUS Options menu.


Field	Description
Authentication for PPP Dialin	<p>By default, the following authentication sequence is used for incoming calls with RADIUS: First CLID, then PPP and then PPP with RADIUS.</p> <p>Options:</p> <ul style="list-style-type: none">• <i>Inband</i>: Only inband RADIUS requests (PAP,CHAP, MS-CHAP V1 & V2) (i.e. PPP requests without CLID) are sent to the RADIUS server defined in Server IP Address.• <i>Outband (CLID)</i> : Only outband RADIUS requests (i.e. requests for calling line identification = CLID) are sent to the RADIUS server. <p><i>Inband</i> is enabled by default.</p>



9.6 Configuration Access

In the **Configuration Access** menu you can configure user profiles.

To do so, you create access profiles and users and assign each user at least one access profile. An access profile makes available that part of the GUI that a user requires for their tasks. Parts of the GUI that are not required are blocked.

9.6.1 Access Profiles

The menu **System Management->Configuration Access->Access Profiles** displays a list of all the access profiles that have been configured. You can delete existing entries with the icon .

By default, more than one access profile has already been created for the devices **elmeg hybrid 120/130** and **elmeg hybrid 300/600**. You can change these using the icon  or reset them to the default settings using the icon .

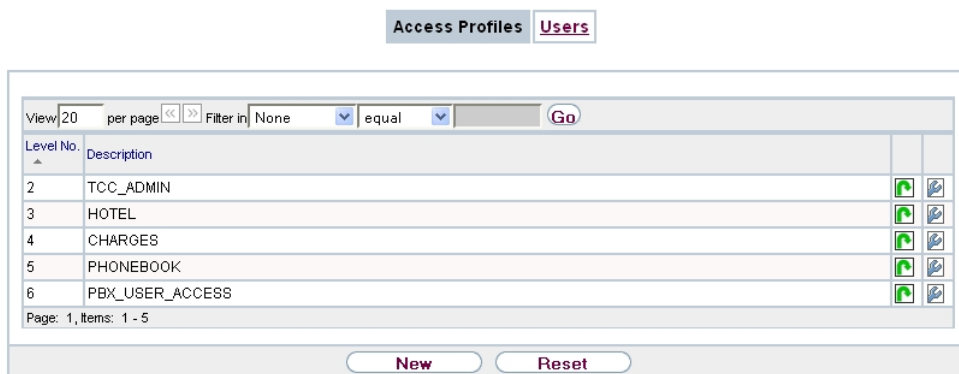


Fig. 38: System Management->Configuration Access->Access Profiles

9.6.1.1 Edit or New

Choose the icon to edit existing entries. Choose the **New** button to create additional access profiles.

To create an access profile you can use all the entries in the navigation bar of the GUI plus **Save configuration** and **Switch to SNMP Browser**. You can create a maximum of 29 access profiles.

Access Profiles

Users

Basic Settings

Description

Level No.

7

Buttons

Save configuration

☐ Enabled

Switch to SNMP Browser

☐ Enabled

Navigation Entries

Assistants

First steps

PBX

System Management

Physical Interfaces

VoIP

Numbering

Terminals

Call Routing

Applications

LAN

Networking

Firewall

VoIP

Local Services

Maintenance

External Reporting

Monitoring

User Access

OK

Cancel



Fig. 39: **System Management->Configuration Access->Access Profiles->New**

The menu **System Management->Configuration Access->Access Profiles->New** consists of the following fields:








Fields in the menu Basic Settings

Field	Description
Description	Enter a unique name for the access profile.
Level No.	The system automatically assigns a sequential number to the access profile. This cannot be edited.


Fields in the menu Buttons

Field	Description
Save configuration	<p>If you activate the button Save configuration the user is permitted to save configurations.</p> <div>Note<p>Note that the passwords in the saved file can be viewed in clear text.</p></div> <p>Enable or disable Save configuration.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Switch to SNMP Browser	<p>If you activate the button Switch to SNMP Browser, the user can switch to the SNMP browser view, access the parameters and modify all the settings displayed there.</p> <div>Caution<p>Note that the permission for Switch to SNMP Browser means that the user can access the entire MIB, because no individual access profile can be created in this view. The user can save the changed MIB with the permission for Save configuration.</p><p>With the permission for Switch to SNMP Browser you remove the configured GUI restrictions at the MIB level once more.</p><p>Enable or disable Switch to SNMP Browser.</p><p>The function is enabled with <i>Enabled</i>.</p><p>The function is disabled by default.</p></div>

Fields in the menu Navigation Entries

Field	Description
Menus	<p>You see all the menus from the GUI's navigation bar. Menus that contain at least one sub-menu are flagged by  and  .</p> <p>The icon  indicates pages.</p> <p>When you create a new access profile, no elements are assigned yet, i.e. all the available menus, sub-menus and pages are flagged with the icon .</p> <p>Each element in the navigation bar can have three values. Click the icon  in the row you want to display these three values.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Deny</i>: The menu and all its lower-level menus are blocked.• <i>Allow</i>: The menu is released. Lower-level menus may need to be specifically released.• <i>Allow all</i>: The menu and all its lower-level menus are released. <p>You can select <i>Allow</i> and <i>Allow all</i> in the corresponding row to assign elements to the current access profile.</p> <p>Elements that are assigned to the current access profile are flagged with the icon .</p> <p> indicates a menu that is blocked, but which has at least one released sub-menu.</p>

9.6.2 Users

The menu **System Management->Configuration Access->Users** displays a list of all the users that have been configured. You can delete existing entries with the icon .

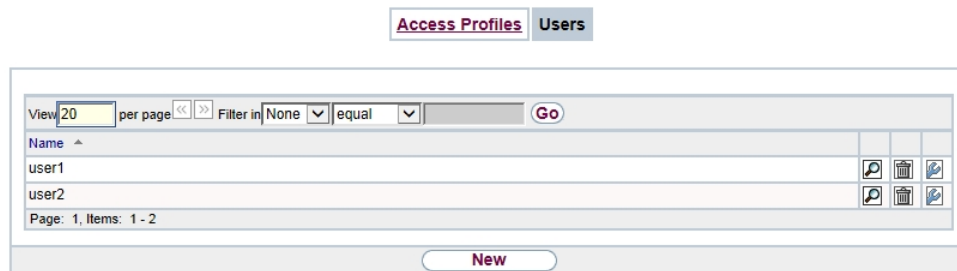


Fig. 40: **System Management->Configuration Access->Users**

You can click the button to display the details of the configured user. You can see which fields and menus are assigned to the user.

Access Profiles

Users

Basic Settings

User	user 1
User must change password	Disabled

Buttons

Save configuration	Disabled
Switch to SNMP Browser	Disabled

Navigation Entries

Assistants

First steps

PBX

System Management

Physical Interfaces

VoIP

Numbering

Terminals

Call Routing

Applications

LAN

Networking

Firewall

VoIP

Local Services

Maintenance







External Reporting

Monitoring


User Access

Cancel

Fig. 41: System Management->Configuration Access->Users->

The icon   means that **Read-only** is permitted. If a row is flagged with the icon   the information is released for reading and writing. The icon   indicates blocked entries.

9.6.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional users.

Access Profiles

Users

Basic Settings

User

Password

.....

User must change password

☐ Enabled

Access Level

Access Level

Read-only

Add

OK

Cancel

Fig. 42: System Management->Configuration Access->Users->New

The menu **System Management->Configuration Access->Users->New** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
User	Enter a unique name for the user.
Password	Enter a password for the user.
User must change password	<p>The administrator can use the option User must change password to specify that the user must select their own password the first time they log in. To do this, the option Save configuration needs to be enabled in the menu Access Profiles. If this option is not enabled, a warning message displays.</p> <p>Enable or disable User must change password.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Access Level	<p>Use Add to assign at least one access profile to the user. Selecting Read-only specifies that the user can view the parameters of the access profile, but not change them. Selecting Read-only is only possible if the option Switch to SNMP Browser in the menu Access Profiles is not enabled.</p> <p>If the option Switch to SNMP Browser is enabled, a warning message displays because the user can switch to the SNMP browser view, access the parameters and make any changes they like. The option Read-only is not available in the SNMP browser view.</p>

Field	Description
	If intersecting access profiles are assigned to a user, read and write have a higher priority than Read-only . Buttons cannot be set to the setting Read-only .

9.7 Certificates

An asymmetric cryptosystem is used to encrypt data to be transported in a network, to generate or check digital signatures and the authenticate users. A key pair consisting of a public key and a private key is used to encrypt and decrypt the data.

For encryption the sender requires the public key of the recipient. The recipient decrypts the data using his private key. To ensure that the public key is the real key of the recipient and is not a forgery, a so-called digital certificate is required.

This confirms the authenticity and the owner of a public key. It is similar to an official passport in that it confirms that the holder of the passport has certain characteristics, such as gender and age, and that the signature on the passport is authentic. As there is more than one certificate issuer, e.g. the passport office for a passport, and as such certificates can be issued by several different issuers and in varying qualities, the trustworthiness of the issuer is extremely important. The quality of a certificate is regulated by the German Signature Act or respective EU Directives.

Certification authorities that issue so-called qualified certificates are organised in a hierarchy with the Federal Network Agency as the higher certifying authority. The structure and content of a certificate are stipulated by the standard used. X.509 is the most important and the most commonly use standard for digital certificates. Qualified certificates are personal and extremely trustworthy.

Digital certificates are part of a so-called Public Key Infrastructure (PKI). PKI refers to a system that can issue, distribute and check digital certificates.

Certificates are issued for a specific period, usually one year, i.e. they have a limited validity period.

Your device is designed to use certificates for VPN connections and for voice connections over Voice over IP.

9.7.1 Certificate List

A list of all existing certificates is displayed in the **System Management->Certificates->Certificate List** menu.

9.7.1.1 Edit

Click the  icon to display the content of the selected object (key, certificate, or request).

Certificate ListCRLsCertificate Servers

Edit parameters

Description	test
Certificate is CA Certificate	<input checked="" type="checkbox"/> True
Certificate Revocation List (CRL) Checking	<div><input type="radio"/> Disabled <input type="radio"/> Always <input checked="" type="radio"/> Only if a CRL Distribution Point is present <input type="radio"/> Use settings from superior certificate</div>
Force certificate to be trusted	<input type="checkbox"/> True

View details

Certificate =
SerialNumber = 11
SubjectName = <CN=r1200_aw, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE>
IssuerName = <CN=linuxCA, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE>
Validity =
NotBefore = 2006 Sep 15th, 07:07:49 GMT
NotAfter = 2008 Sep 14th, 07:07:49 GMT
PublicKeyInfo =
Algorithm name (X.509) : rsaEncryption
Modulus n (1024 bits) :
1657430007353061929971175628985365836058592284552111716307381855989730994
4241959750497426343375890536490502929548450998243446632595011570952551767
7011616656908963216398179133323977323187771274664312501085550617414306630
0411834850766905090689578661769721208181141085359073369329733126120426693
320106097890434357773
Exponent e (17 bits) : 65537
Extensions =
Available = key usage, basic constraints
KeyUsage = DigitalSignature NonRepudiation KeyEncipherment
BasicConstraints =
cA = FALSE


MD5 Fingerprint	EE:AB:21:CB:4A:82:02:44:6C:A2:F6:5E:0D:0C:65:34
SHA1 Fingerprint	77:5A:14:BC:60:17:66:56:8C:F7:CC:90:C0:4E:25:19:3B:D3:7B:F7
Used	

OK

Cancel

Fig. 43: System Management->Certificates->Certificate List->

The certificates and keys themselves cannot be changed, but a few external attributes can be changed, depending on the type of the selected entry.

The **System Management->Certificates->Certificate List->** menu consists of the following fields:

Fields in the Edit parameters menu.

Field	Description
Description	Shows the name of the certificate, key, or request.
Certificate is CA Certificate	<p>Mark the certificate as a certificate from a trustworthy certification authority (CA).</p> <p>Certificates issued by this CA are accepted during authentication.</p> <p>The function is enabled with <i>True</i>.</p> <p>The function is disabled by default.</p>
Certificate Revocation List (CRL) Checking	<p>Only for Certificate is CA Certificate = <i>True</i></p> <p>Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate.</p> <p>Possible settings:</p> <ul style="list-style-type: none">• <i>Disabled</i>: No CRLs check.• <i>Always</i>: CRLs are always checked.• <i>Only if a CRL Distribution Point is present</i> (default value): A check is only carried out if a CRL Distribution Point entry is included in the certificate. This can be determined under "View Details" in the certificate content.• <i>Use settings from superior certificate</i>: The settings of the higher level certificate are used, if one exists. If it does not, the same procedure is used as that described under "Only if a CRL Distribution Point is present".
Force certificate to be trusted	<p>Define that this certificate is to be accepted as the user certificate without further checks during authentication.</p> <p>The function is enabled with <i>True</i>.</p> <p>The function is disabled by default.</p>

**Caution**

It is extremely important for VPN security that the integrity of all certificates manually marked as trustworthy (certification authority and user certificates) is ensured. The displayed "fingerprints" can be used to check this integrity: Compare the displayed values with the fingerprints specified by the issuer of the certificate (e.g. on the Internet). It is sufficient to check one of the two values.

9.7.1.2 Certificate Request

Registration authority certificates in SCEP

If SCEP (Simple Certificate Enrollment Protocol) is used, your device also supports separate registration authority certificates.

Registration authority certificates are used by some Certificate Authorities (CAs) to handle certain tasks (signature and encryption) during SCEP communication with separate keys, and to delegate the operation to separate registration authorities, if applicable.

When a certificate is downloaded automatically, i.e. if **CA Certificate** = -- *Download* -- is selected, all the certificates needed for the operation are loaded automatically.

If all the necessary certificates are already available in the system, these can also be selected manually.

Select the **Certificate Request** button to request or import more certificates.

Certificate ListCRLsCertificate Servers

Certificate Request

Certificate Request Description

Mode

Manual

SCEP

Generate Private Key

RSA

1024

Bits

Subject Name

Custom

Enabled

Common Name

E-mail

Organizational Unit

Organization

Locality

State/Province

Country

Advanced Settings

Subject Alternative Names

#1

None

#2

None

#3

None

Options

Autosave Mode

Enabled


OK

Cancel

Fig. 44: System Management->Certificates->Certificate List->Certificate Request

The menu **System Management->Certificates->Certificate List->Certificate Request** consists of the following fields:

Fields in the Certificate Request menu.

Field	Description
Certificate Request Description	Enter a unique description for the certificate.
Mode	<div>Select the way in which you want to request the certificate.</div> <div>Possible settings:</div> <ul style="list-style-type: none">Manual (default value): Your device generates a PKCS#10 for the key. This file can then be uploaded directly in the browser or copied in the  menu using the View details

bintec RV Series

101

Field	Description
	<p>field. This file must be provided to the CA and the received certificate must then be imported manually to your device.</p> <ul style="list-style-type: none">• <i>SCEP</i>: The key is requested from a CA using the Simple Certificate Enrolment Protocol.
Generate Private Key	<p>Only for Mode = <i>Manual</i></p> <p>Select an algorithm for key creation.</p> <p><i>RSA</i> (default value) and <i>DSA</i> are available.</p> <p>Also select the length of the key to be created.</p> <p>Possible values: <i>512, 768, 1024, 1536, 2048, 4096</i>.</p> <p>Please note that a key with a length of 512 bits could be rated as unsecure, whereas a key of 4096 bits not only needs a lot of time to create, but also occupies a major share of the resources during IPsec processing. A value of 768 or more is, however, recommended and the default value is 1024 bits.</p>
SCEP URL	<p>Only for Mode = <i>SCEP</i></p> <p>Enter the URL of the SCEP server, e.g. <code>http://scep.bintec-elmeg.com:8080/scep/scep.dll</code></p> <p>Your CA administrator can provide you with the necessary data.</p>
CA Certificate	<p>Only for Mode = <i>SCEP</i></p> <p>Select the CA certificate.</p> <ul style="list-style-type: none">• In <code>-- Download --</code>: In CA Name, enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. <i>cawindows</i>. Your CA administrator can provide you with the necessary data. <p>If no CA certificates are available, the device will first download the CA certificate of the relevant CA. It then continues with the enrolment process, provided no more important parameters are missing. In this case, it returns to the Generate Certificate Request menu.</p> <p>If the CA certificate does not contain a CRL distribution point (Certificate Revocation List, CRL), and a certificate server is</p>

Field	Description
	<p>not configured on the device, the validity of certificates from this CA is not checked.</p> <ul style="list-style-type: none">• <name of an existing certificate>: If all the necessary certificates are already available in the system, you select these manually.
RA Sign Certificate	<p>Only for Mode = <i>SCEP</i></p> <p>Only for CA Certificate not = -- <i>Download</i> --</p> <p>Select a certificate for signing SCEP communication.</p> <p>The default value is -- <i>Use CA Certificate</i> --, i.e. the CA certificate is used.</p>
RA Encrypt Certificate	<p>Only for Mode = <i>SCEP</i></p> <p>Only if RA Sign Certificate not = -- <i>Use CA Certificate</i> --</p> <p>If you use one of your own certificates to sign communication with the RA, you can select another one here to encrypt communication.</p> <p>The default value is -- <i>Use RA Sign Certificate</i> --, i.e. the same certificate is used as for signing.</p>
Password	<p>Only for Mode = <i>SCEP</i></p> <p>You may need a password from the certification authority to obtain certificates for your keys. Enter the password you received from the certification authority here.</p>

Fields in the Subject Name menu.

Field	Description
Custom	<p>Select whether you want to enter the name components of the subject name individually as specified by the CA or want to enter a special subject name.</p> <p>If <i>Enabled</i> is selected, a subject name can be given in Summary with attributes not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".</p>

Field	Description
	<p>If the field is not selected, enter the name components in Common Name, E-mail, Organizational Unit, Organization, Locality, State/Province and Country.</p> <p>The function is disabled by default.</p>
Summary	<p>Only for Custom = enabled.</p> <p>Enter a subject name with attributes not offered in the list.</p> <p>Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".</p>
Common Name	<p>Only for Custom = disabled.</p> <p>Enter the name according to CA.</p>
E-mail	<p>Only for Custom = disabled.</p> <p>Enter the e-mail address according to CA.</p>
Organizational Unit	<p>Only for Custom = disabled.</p> <p>Enter the organisational unit according to CA.</p>
Organization	<p>Only for Custom = disabled.</p> <p>Enter the organisation according to CA.</p>
Locality	<p>Only for Custom = disabled.</p> <p>Enter the location according to CA.</p>
State/Province	<p>Only for Custom = disabled.</p> <p>Enter the state/province according to CA.</p>
Country	<p>Only for Custom = disabled.</p> <p>Enter the country according to CA.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Subject Alternative Names menu.

Field	Description
#1, #2, #3	<p>For each entry, define the type of name and enter additional subject names.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): No additional name is entered.• <i>IP</i>: An IP address is entered.• <i>DNS</i>: A DNS name is entered.• <i>E-mail</i>: An e-mail address is entered.• <i>URI</i>: A uniform resource identifier is entered.• <i>DN</i>: A distinguished name (DN) name is entered.• <i>RID</i>: A registered identity (RID) is entered.

Fields in the Options menu

Field	Description
Autosave Mode	<p>Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

9.7.1.3 Import

Choose the **Import** button to import certificates.



Fig. 45: **System Management->Certificates->Certificate List->Import**

The menu **System Management->Certificates->Certificate List->Import** consists of the following fields:

Fields in the Import menu.

Field	Description
External Filename	Enter the file path and name of the certificate to be imported, or use Browse... to select it from the file browser.
Local Certificate Description	Enter a unique description for the certificate.
File Encoding	Select the type of coding so that your device can decode the certificate. Possible values: <ul style="list-style-type: none">• <i>Auto</i> (default value): Activates automatic code recognition. If downloading the certificate in auto mode fails, try with a certain type of encoding.• <i>Base64</i>• <i>Binary</i>
Password	You may need a password to obtain certificates for your keys. Enter the password here.

9.7.2 CRLs

In the **System Management->Certificates->CRLs** menu, a list of all CRLs (Certification Revocation List) is displayed.

If a key is no longer to be used, e.g. because it has fallen into the wrong hands or has been lost, the corresponding certificate is declared invalid. The certification authority revokes the certificate and publishes it on a certificate blacklist, so-called CRL. Certificate users should always check against these lists to ensure that the certificate used is currently valid. This check can be automated via a browser.

The Simple Certificate Enrollment Protocol (SCEP) supports the issue and revocation of certificates in networks.

9.7.2.1 Import

Choose the **Import** button to import CRLs.

Certificate ListCRLsCertificate Servers

CRL Import

External Filename

Browse...

Local Certificate Description

File Encoding

Auto

Password

OK

Cancel

Fig. 46: System Management->Certificates->CRLs->Import

The **System Management->Certificates->CRLs->Import** menu consists of the following fields:

Fields in the CRL Import menu.

Field	Description
External Filename	Enter the file path and name of the CRL to be imported, or use Browse... to select it from the file browser.
Local Certificate Description	Enter a unique description for the CRL.
File Encoding	<div>Select the type of encoding, so that your device can decode the CRL.</div> <div>Possible values:</div> <ul style="list-style-type: none"><i>Auto</i> (default value): Activates automatic code recognition. If downloading the CRL in auto mode fails, try with a certain

Field	Description
	type of encoding. <ul style="list-style-type: none">• <i>Base64</i>• <i>Binary</i>
Password	Enter the password required for the import.

9.7.3 Certificate Servers

A list of certificate servers is displayed in the **System Management->Certificates->Certificate Servers** menu.

A certification authority (certification service provider, Certificate Authority, CA) issues your certificates to clients applying for a certificate via a certificate server. The certificate server also issues the private key and provides certificate revocation lists (CRL) that are accessed by the device via LDAP or HTTP in order to verify certificates.

9.7.3.1 New

Choose the **New** button to set up a certificate server.

Certificate ListCRLsCertificate Servers

Basic Parameters

Description

LDAP URL Path

ldap://

OK

Cancel

Fig. 47: **System Management->Certificates->Certificate Servers->New**

The **System Management->Certificates->Certificate Servers->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a unique description for the certificate server.
LDAP URL Path	Enter the LDAP URL or the HTTP URL of the server.

Chapter 10 Physical Interfaces

In this menu, you configure the physical interfaces that you have used when connecting your gateway. The configuration interface only shows the interfaces that are available on your device. In the **System Management->Status** menu, you can see a list of all physical interfaces and information on whether the interfaces are connected or active and whether they have already been configured.

10.1 AUX

You require a special cable for the console port of your gateway (e.g. AUX Backup cable) to connect an external analogue modem to the AUX port on a bintec elmeg gateway.

10.1.1 AUX

With an analogue/GSM interface, the gateway also supports connections for analogue and GSM modems (e.g. as backup). In principle, you can use any Hayes- or GSM07.07-compatible modem with a serial interface for this purpose. The following modems have been tested successfully for bintec elmeg:

- US Robotics Sportster Flash (analogue modem)
- US Robotics 56K Fax Modem (analogue modem)
- Siemens TC35i (GSM modem)

AUX

Basic Settings	
AUX Port Status	<input checked="" type="checkbox"/> Enabled
Line Speed	9600 bps
Incoming Service Type	<input type="radio"/> Disabled <input checked="" type="radio"/> ISDN Login <input type="radio"/> PPP Dialin
SIM Card Uses PIN	
Modem Escape Character	+
Modem Init Sequence	
APN (Access Point Name)	

OK Cancel

Fig. 48: Physical Interfaces->AUX->AUX

The **Physical Interfaces->AUX->AUX** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
AUX Port Status	<p>Select whether the AUX port should be enabled or disabled.</p> <p>The port is enabled by choosing <i>Enabled</i>. The port is disabled by default.</p>
Line Speed	<p>Only for AUX Port Status = enabled</p> <p>Here you select the speed at which the gateway addresses the modem (in bps).</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Default</i>: The Baud rate of the serial terminal connection is retained. (9600 in ex works state) <p>All other values mean that the modem is addressed at the corresponding speed in bps.</p> <ul style="list-style-type: none">• <i>9600 bps</i>• <i>19200 bps</i>• <i>38400 bps</i>• <i>57600 bps</i> (default value): Recommended for communication with a GSM modem.• <i>115200 bps</i>: Recommended for communication with an analogue modem.
Incoming Service Type	<p>Only for AUX Port Status = enabled</p> <p>Here you select the gateway subsystem to which an incoming call over the modem is to be assigned.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Disabled</i>: No call is accepted.• <i>ISDN Login</i>: The call is assigned to the ISDN Login subsystem.• <i>PPP Dialin</i> (default value): The call is assigned to the PPP subsystem.
SIM Card Uses PIN	<p>Only for AUX Port Status = enabled</p> <p>Here you enter the PIN of your GSM modem, if your modem</p>

Field	Description
	asks for it. Entering a wrong PIN blocks communication with the modem until the entry in the profile is corrected.
Modem Escape Character	Only for AUX Port Status = enabled The value for this field is set by default to <code>+</code> . It should only be changed if the escape character of the modem is different.
Modem Init Sequence	Only for AUX Port Status = enabled Here you can enter an initialization string for your modem. The command <code>ATX3&K3\V1</code> is the default setting (the modem does not wait for a free signal before dialling). You can add other AT commands by separating them with semicolons. The entry is limited to 50 characters. Make sure you enter the command for activating the XON/XOFF software flow control. This is proprietary and cannot be set automatically. The command sequence can be obtained from your modem manual or the manufacturer.
APN (Access Point Name)	Only for AUX Port Status = enabled If GPRS is used, the so-called Access Point Name of the provider must be entered, e.g. <code>internet.eplus.de</code> for eplus and so on. A maximum of 40 characters can be entered. If no APN or an incorrect APN is entered, a configured GPRS connection will not function.

10.2 Ethernet Ports

An Ethernet interface is a physical interface for connection to the local network or external networks.

The Ethernet ports **ETH1** to **ETH4** are assigned to a single logical Ethernet interface in ex works state. The logical Ethernet interface `en1-0` is assigned and is preconfigured with the **IP Address** `192.168.0.254` and **Netmask** `255.255.255.0`.

The port **ETH5** is assigned to the logical Ethernet interface `en1-4` and is not precon-

figured.



Note

To ensure your device can be reached, when splitting ports make sure that Ethernet interface `en1-0` is assigned - with the preconfigured IP address and netmask - to a port that can be reached via Ethernet. If in doubt, carry out the configuration using a serial connection via the **Console** interface.

ETH1 - ETH4

The interfaces can be used separately. They are logically separated from each other, each separated port is assigned the desired logical Ethernet interface in the **Ethernet Interface Selection** field of the **Port Configuration** menu. For each assigned Ethernet interface, another interface is displayed in the list in the **LAN->IP Configuration** menu, and the interface can be configured completely independently.

ETH5

By default, the logical Ethernet interface `en1-4` is assigned to the **ETH5** port. The configuration options are the same as those for the ports **ETH1 - ETH4**.



Note

If you want to operate the port **ETH5** with an SFP module, this must be inserted before the system reboot!

During operation, you cannot switch to operating the **ETH5** without an SFP module. If the **ETH5** port is used after adding an SFP module, the device must be rebooted.

The **ETH5** port can however be used during operation without first inserting the SFP module.

The following SFP modules with SERDES interface are supported for FTTH connections:

- AT-SPBD10-13: 1000LX Single Mode BiDi SFP (1310 Tx, 1490 Rx) 10 km
- AT-SPBD10-14: 1000LX Single Mode BiDi SFP (1490 Tx, 1310 Rx) 10 km
- AT-SPLX40: 1000LX (LC) SFP, 40km

VLANs for Routing Interfaces

Configure VLANs to separate individual network segments from each other, for example (e.g. individual departments of a company) or to reserve bandwidth for individual VLANs when managed switches are used with the QoS function.

10.2.1 Port Configuration

Port Separation

Your device makes it possible to run the switch ports as one interface or to logically separate these from each other and to configure them as independent Ethernet interfaces.

During configuration, please note the following: The splitting of the switch ports into several Ethernet interfaces merely logically separates these from each other. The available total bandwidth of max. 1000 mbps full duplex for all resulting interfaces remains the same. For example, if you split all the switch ports from each other, each of the resulting interfaces only uses a part of the total bandwidth. If you group together several switch ports into one interface, the full bandwidth of max. 1000 mbps full duplex is available for all the ports together.

Port Configuration

Automatic Refresh Interval 60 Seconds Apply

Switch Configuration

Switch Port	Ethernet Interface Selection	Configured Speed / Mode	Current Speed / Mode	Flow Control
1	en1-0	Full Autonegotiation	Down	Disabled
2	en1-0	Full Autonegotiation	100 mbps / Full Duplex	Disabled
3	en1-0	Full Autonegotiation	Down	Disabled
4	en1-0	Full Autonegotiation	Down	Disabled
5	en1-4	Full Autonegotiation	Down	Disabled

OK Cancel

Fig. 49: Physical Interfaces->Ethernet Ports->Port Configuration

The menu **Physical Interfaces->Ethernet Ports->Port Configuration** consists of the following fields:

Fields in the Switch Configuration menu

Field	Description
Switch Port	Shows the respective switch port. The numbering corresponds

Field	Description
	<p>to the numbering of the Ethernet ports on the back of the device.</p> <p>Switch-Port 5: Port ETH5 is configured here.</p>
Ethernet Interface Selection	<p>Assign a logical Ethernet interface to the switch port.</p> <p>You can select from five interfaces, <i>en1-0</i> to <i>en1-4</i>. In the basic setting, switch ports 1-4 are assigned to interface <i>en1-0</i> and switch port 5 is assigned to interface <i>en1-4</i></p>
Configured Speed / Mode	<p>Select the mode in which the interface is to run.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Full Autonegotiation</i> (default value)• <i>Auto 1000 mbps only</i>• <i>Auto 100 mbps only</i>• <i>Auto 10 mbps only</i>• <i>Auto 100 mbps / Full Duplex</i>• <i>Auto 100 mbps / Half Duplex</i>• <i>Auto 10 mbps / Full Duplex</i>• <i>Auto 10 mbps / Half Duplex</i>• <i>Fixed 1000 mbps / Full Duplex</i>• <i>Fixed 100 mbps / Full Duplex</i>• <i>Fixed 100 mbps / Half Duplex</i>• <i>Fixed 10 mbps / Full Duplex</i>• <i>Fixed 10 mbps / Half Duplex</i>• <i>None</i>: The interface is created but remains inactive.
Current Speed / Mode	<p>Shows the actual mode and actual speed of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>1000 mbps / Full Duplex</i>• <i>100 mbps / Full Duplex</i>• <i>100 mbps / Half Duplex</i>• <i>10 mbps / Full Duplex</i>• <i>10 mbps / Half Duplex</i>

Field	Description
	<ul style="list-style-type: none">• <i>Down</i>
Flow Control	<p>Select whether a flow control should be conducted on the corresponding interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Disabled</i> (default value): No flow control is performed.• <i>Enabled</i>: Flow control is performed.• <i>Auto</i>: Automatic flow control is performed.

10.3 Serial Port

The serial interface can be operated as a console or as a data interface. In data interface mode, the data for the serial interface can be transmitted over an IP infrastructure (Serial over IP).

10.3.1 Serial Port

In the **Physical Interfaces->Serial Port->Serial Port** menu, you can perform settings for the serial interface.



Fig. 50: Physical Interfaces->Serial Port->Serial Port

The **Physical Interfaces->Serial Port->Serial Port** menu consists of the following fields:

Fields in the Controller Configuration menu

Field	Description
Port Mode	<p>Select in which mode the serial interface is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Configuration</i> (default value): The serial interface is used as a console.

Field	Description
	<ul style="list-style-type: none"><i>Data Port</i>: The serial interface is operated as a data interface, Serial over IP is used.

If the *Data Port* option is selected for **Port Mode**, an extra configuration section opens.

Serial Port

General

Port Mode

☐ Configuration ☒ Data Port

Serial Settings

Baudrate

9600

Data Bits

8

Parity

None

Stop Bits

1

Handshake:

None

IP

Mode

☒ Server ☐ Client ☐ UDP

Local IP Address

0.0.0.0

Local Port

0

Remote IP

0.0.0.0

Port Number

0

Trigger

Byte Count

128

Timeout

☐ Enabled

Inter-Byte Gap

100 ms ☒ Enabled

Buffer

Clear Serial RX-Buffer

Clear

Clear Serial TX-Buffer

Clear

OK

Cancel

Fig. 51: Physical Interfaces->Serial Port->Serial Port with Port Mode = Data Port

Fields in the Serial Settings menu

Field	Description
Baudrate	<p>Select which baud rate should be used. Make sure that the remote terminal is suitable for the selected baud rate. If this is not the case, you will not be able to establish a serial connection to the device.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• 300• 600• 1200• 2400• 4800• 9600 (default value)• 19200• 57600• 115200
Data Bits	<p>Select how many data bits should be sent in sequence for traffic data.</p> <p>Possible values:</p> <ul style="list-style-type: none">• 8 (default value): Eight Data Bits are sent in sequence.• 7: Seven Data Bits are sent in sequence.
Parity	<p>Select whether or not a parity bit should be used to identify transmission errors.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): No parity bit is used.• <i>Even</i>: An even number of "1" bits is used to identify transmission errors.• <i>Odd</i>: An uneven number of "1" bits is used to identify transmission errors.
Stop Bits	<p>Stop bits terminate the data transmission of a transmission unit.</p> <p>Choose whether a stop bit should be used or whether two stop bits should be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• 1 (default value)• 2
Handshake	<p>Choose how the recipient can continue the data transmission so that no data is lost, if no other data can be processed.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): The recipient is unable to continue the data transmission.• <i>RTS/CTS</i>: The hardware handshake used controls the data flow over the RTS and CTS lines.• <i>XON/XOFF</i>: If the software handshake is used, the recipient sends special signs to the sender to control the data flow.

Fields in the IP menu

Field	Description
Mode	<p>Select the Mode in which the gateway should process IP data packets.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Server</i> (default value): The gateway waits for incoming TCP connections.• <i>Client</i>: The gateway actively sets up a TCP connection.• <i>UDP</i>: The gateway sends and receives UDP packets.
Local IP Address	<p>Enter the IP address of the client logging in. IF Local IP Address = 0.0.0.0, any client can log in.</p>
Local Port	<p>Enter the port for Local IP Address.</p>
Remote IP	<p>Enter the IP address of the server at which your gateway should log in.</p>
Port Number	<p>Enter the port for Remote IP.</p>

Fields in the Trigger menu

Field	Description
Byte Count	<p>Enter the received characters in bytes, which are used as a trigger for data transmission.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>Possible values: 1 .. 1460. Default value: 128.</p>

Field	Description
Timeout	<p>Enter the time in ms since receiving the last character, which is used as a trigger for data transmission.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>Possible values: 0 .. 65535. Default value: 0.</p>
Inter-Byte Gap	<p>Enter the time in ms since receiving the first character, which is used as a trigger for data transmission.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Possible values: 0 .. 65535. Default value: 100.</p>

Fields in the Buffer menu

Field	Description
Clear Serial RX-Buffer	Click the Clear button to clear the receive buffer.
Clear Serial TX-Buffer	Click the Clear button to clear the send buffer.

10.4 UMTS/LTE

10.4.1 UMTS/LTE

In the **UMTS/LTE** menu, configure the connection for the integrated UMTS/HSDPA/LTE modem (depending on the configuration of your device) or an optional pluggable UMTS/LTE SIM card.

A list of compatible UMTS/LTE SIM cards can be found at www.bintec-elmeg.com under **Products**.



Note


If you are connecting to the internet via UMTS and are using the SMS alert service, the connection is briefly interrupted when an SMS is sent.

**Note**

LTE cannot currently be used for incoming connections via ISDN login.

LTE cannot currently be used together with the SMS alert service.

10.4.1.1 Edit

Click the  icon to edit the respective entry for the integrated modem or a plugged UMTS/LTE SIM card.

Select the following entry for the corresponding UMTS/LTE modem:

- *Slot6 Unit 0*: The integrated modem is to be configured.
- *Slot6 Unit 1*: The plug-in UMTS SIM card is to be configured.

**Note**

Please note that the technology used not only depends on availability and the setting in the **Preferred Network Type** field; rather it is also determined by the strength and quality of the signal.

UMTS/LTE

Basic Settings

UMTS/LTE Status	<input checked="" type="checkbox"/> Enabled
Modem Status	Up
Actual Network	LTE
Network Provider	Telekom.de
Network Quality	<div><div></div></div> -77 dBm
Preferred Network Type	Automatic
Incoming Service Type	<input checked="" type="radio"/> Disabled <input type="radio"/> ISDN Login <input type="radio"/> PPP Dialin <input type="radio"/> IPSec
SIM Card Uses PIN	••••••••
Fallback Number	
APN (Access Point Name)	internet.telekom

Advanced Settings

Roaming/PLNM Selection

Roaming Mode	Auto
--------------	------

Closed User Group

Authentication Method	pap-chap
Username	
Password	
Fixed IP Address	

OK Cancel

Fig. 52: Physical Interfaces->UMTS/LTE->UMTS/LTE->



The menu Physical Interfaces->UMTS/LTE->UMTS/LTE-> consists of the following fields:




Fields in the Basic Settings menu.


Field	Description
UMTS/LTE Status	Select whether the chosen UMTS/LTE modem should be enabled or disabled. The function is enabled with <i>Enabled</i> . The function is enabled by default.
Modem Status	Only for UMTS/LTE Status = <i>Enabled</i> Shows the status of the UMTS/LTE modem. Possible values:

Field	Description
	<ul style="list-style-type: none">• <i>Up</i>• <i>Down</i>• <i>Init</i>• <i>Called</i>• <i>Calling</i>• <i>Connect</i>• <i>SIM insert required</i>• <i>PIN input required</i>• <i>Error</i>• <i>Disconnected</i>
Network Provider	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>This is only displayed if the status of the modem is "up".</p> <p>Displays the Network Provider currently connected.</p>
Actual Network	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>Displays the current network, e.g. GSM or UMTS.</p>
Network Quality	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>Displays the current quality of the UMTS/LTE connection. The value cannot be changed.</p>
Preferred Network Type	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>Select which network type should preferably be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Automatic</i> (default value): GPRS, UMTS or LTE is automatically selected for the connection, depending on which network type is locally available.• <i>GPRS only</i>: Only GPRS is used; should GPRS not be available, no connection is established.• <i>UMTS only</i>: Only UMTS is used; should UMTS not be available, no connection is established.• <i>GPRS preferred</i>: GPRS is preferentially used; should GPRS not be available, UMTS is used.

Field	Description
	<ul style="list-style-type: none">• <i>UMTS preferred</i>: UMTS is preferentially used; should UMTS not be available, GPRS is used.• <i>LTE only</i>: Only LTE is used; should LTE be unavailable, no connection is established.• <i>LTE preferred (Priority 4G/3G/2G)</i>: LTE is preferably used; should LTE be unavailable, UMTS is used, and if UMTS is unavailable, GPRS is used.• <i>LTE/UMTS (Priority 4G/3G)</i>: LTE is used. If the strength and quality of the signal are insufficient with LTE then UMTS is used.• <i>LTE/GPRS (Priority 4G/2G)</i>: LTE is used. If the strength and quality of the signal are insufficient with LTE then GPRS is used.• <i>LTE/GPRS/UMTS (Priority 4G/2G/3G)</i>: LTE is used. If the strength and quality of the signal are insufficient with LTE then GPRS is used. If the strength and quality of the signal are insufficient with GPRS then UMTS is used.• <i>UMTS/LTE (Priority 3G/4G)</i>: UMTS is used. If the strength and quality of the signal are insufficient with UMTS then LTE is used.• <i>UMTS/GPRS (Priority 3G/2G)</i>: UMTS is used. If the strength and quality of the signal are insufficient with UMTS then GPRS is used.• <i>UMTS/LTE/GPRS (Priority 3G/4G/2G)</i>: UMTS is used. If the strength and quality of the signal are insufficient with UMTS then LTE is used. If the strength and quality of the signal are insufficient with LTE then GPRS is used.• <i>GPRS/LTE (Priority 2G/4G)</i>: GPRS is used. If the strength and quality of the signal are insufficient with GPRS then LTE is used.• <i>GPRS/UMTS (Priority 2G/3G)</i>: GPRS is used. If the strength and quality of the signal are insufficient with GPRS then UMTS is used.• <i>GPRS/LTE/UMTS (Priority 2G/4G/3G)</i>: GPRS is used. If the strength and quality of the signal are insufficient with GPRS then LTE is used. If the strength and quality of the signal are insufficient with LTE then UMTS is used.

Field	Description
	<div><div></div><div><div>Note</div><div><p>An incoming data call (PPP dialin or ISDN login via V.110) can generally only be set up via GSM. Setup for UMTS/LTE is generally only possible if the provider has activated this functionality on demand.</p><p>When a modem is in the "up" state and Preferred Network Type is not <i>UMTS only</i>, the modem normally logs in to the GSM network, so that incoming data calls can be signalled. If a connection to the Internet is then established, there occurs a switch to the UMTS network, provided that UMTS is currently available.</p></div></div></div>
Incoming Service Type	<div><div><p>Only for UMTS/LTE Status = <i>Enabled</i></p><p>Here you select the gateway subsystem to which an incoming call over the modem is to be assigned.</p><p>Possible values:</p><ul style="list-style-type: none">• <i>Disabled</i>: Call is not accepted (default value for LTE connections).• <i>ISDN Login</i>: The call is assigned to the ISDN Login subsystem (default value for UMTS connections).• <i>PPP Dialin</i>: The call is assigned to the PPP subsystem.• <i>IPSec</i>: The call is made via IPSec.<p>Please note the following for the setting Incoming Service Type <i>IPSec</i>:</p><p>IPSec callback is used to cause an IPSec peer to set up an Internet connection, thus allowing an IPSec tunnel over the Internet. You can make a direct call via the UMTS/LTE wireless network in order to signal to a peer that you are online and waiting for an IPSec tunnel to be set up over the Internet. If the called peer currently has no connection to the Internet, the mobile call causes a connection to be set up.</p><p>In the VPN->IPSec->IPSec Peers->->Advanced Settings menu, you can also choose whether the IP address for IPSec tunnel setup should be transmitted with the UMTS/LTE callback</p></div></div>

Field	Description
	call under Transfer own IP address over ISDN/GSM . This may shorten and simplify tunnel setup.
PUK	<p>This is only displayed if the device has made three failed attempts to establish a connection, e.g. if the PIN for the SIM card (see the SIM Card Uses PIN field) has been entered incorrectly three times.</p> <p>Enter the PUK (personal unblocking key) for your SIM card to unblock the SIM card.</p>
SIM Card Uses PIN	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>Enter the PIN for your UMTS/LTE modem card.</p>
	<div>Note<p>Entering a wrong PIN blocks communication until the entry is corrected.</p></div>
	<div>Note<p>If the device has made three failed attempts to establish a connection, e.g. because the PIN has been entered incorrectly three times, you will need to enter the PUK in order to unblock the SIM card.</p></div>
Fallback Number	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>Enter the call number for the GSM fallback function.</p> <p>When a voice calls goes in on this number, any active connection is immediately disconnected and the operating mode of the modem reset to GSM, where the modem remains until another data call (PPP, ISDN login, IPSec callback) comes in. If flat-rate mode is enabled for the WAN connection (option Always active enabled in WAN->Internet + Dialup->UMTS/LTE-></p>

Field	Description
	<div><div></div><div>Note Please note that the SIM card must support this function, and that not all mobile telephony providers relay voice calls over data SIM cards.</div></div>
APN (Access Point Name)	<p>Only for UMTS/LTE Status = <i>Enabled</i></p> <p>If GPRS/UMTS/LTE is to be used, you must enter the so-called Access Point Name that you received from your provider here. A maximum of 80 characters can be entered.</p> <p>If no APN or an incorrect APN has been entered, a configured GPRS/UMTS/LTE connection will not function.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Roaming/PLMN Selection


Field	Description
Roaming Mode	<p>Select if you intend to use Roaming.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Disabled</i> : Roaming is disabled. The Home PLMN (Public Land Mobile Network) is used, i.e. the provider the SIM card is registered at.• <i>Auto Select</i>(Default setting): Use this mode if neither Roaming Mode = <i>Disabled</i> nor Roaming Mode = <i>Fixed</i> suits your requirements. Note that first a scan across all APNs is carried out in this mode. The system tries to use cost-efficient routing in order to reduce roaming charges.• <i>Unrestricted</i>: This mode is intended for specific requirements. Note that first a scan across all APNs is carried out in this mode.• <i>Fixed Operator</i>: At Roaming Mode = <i>Fixed</i> no scan is performed, and only the manually selected Mobile Network Provider is used. If the selected Mobile Network Provider is unavailable, no connection is made.• <i>Full Auto Select</i>: No scan is performed with this selection. The modem automatically selects the strongest Mobile

Field	Description
	Network Provider . Close to a country border this could also be the network of a foreign roaming partner.
Mobile Network Provider	<p>Only for Roaming Mode = <i>Fixed Operator</i></p> <p>Select a Mobile Network Provider from the list.</p> <p>Possible values</p> <ul style="list-style-type: none">• <Provider>: Select a Mobile Network Provider from the list.• <i>Manual Selection</i>: This allows entering a Provider ID (PLMN) manually.
Mobile Network Provider	<p>Here you can add a PLMN (Public Land Mobile Network).</p> <p>Every mobile network is identified by a globally unique identifier that consists of the MCC (Mobile Country Code) and the MNC (Mobile Network Code). The MCC for Germany, e.g. is 262, and the MNC for T-Mobile in Germany is 01. This results in the PLMN <i>26201</i>.</p>

Fields in the menu **Closed User Group**

Field	Description
Authentication Method	<p>Select an authentication protocol for the Closed User Group. Select only an authentication method that has been specified by your provider.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i>: Some providers do not use authentication. Select this option if your provider is among them.• <i>pap</i>: Execute only PAP (PPP Password Authentication Protocol), the password is sent unencrypted.• <i>chap</i>: Execute only CHAP (PPP Challenge Handshake Authentication Protocol according to RFC 1994) the password is sent encrypted.• <i>pap-chap</i> (Default value): Prefer CHAP, use PAP if not available.
Username	Enter the user name that has been supplied by your provider.
Password	Enter the password that has been supplied by your provider.

Field	Description
Fixed IP Address	Enter the Ip address that has been supplied by your provider.

Clicking the  button opens a page with detailed statistics on the current UMTS/LTE connection.

UMTS/LTE

Automatic Refresh Interval Seconds

Mobile Device Status			
Device	/dev/usbTTY0		
Modem Model	MC7710		
IMEI	355060020096827		
Oper Status	PIN input required		
ICC ID	89490200000473279466		
Subscriber Number			
Service Center Address			
Home PLNM	0 Not configured		
Selected PLNM	0		
Actual Network	Unknown		
Network Quality	-		
Location Area Code			
Cell ID			
Last Command	AT+CPIN?		
Last Reply	SIM PIN		
Mobile Operators			
PLNM	Name	Access Type	State

Fig. 53: Physical Interfaces->UMTS/LTE-> 

Values in the list Mobile Device Status

Field	Description
Device	Displays the description of the internal modem port.
Modem Model	Displays the modem model description.
IMEI	The IMEI (International Mobile Station Equipment Identity) displays the 15 digit serial number of the modem.
Oper Status	Displays the operation mode of the modem.
ICC ID	Displays the card ID stored on the SIM card.
Subscriber Number	Displays the calling number stored on the SIM card.
Service Center Address	Displays the address of the provider's service center stored on the SIM card.
Home PLMN	Displays the Home PLMN (Public Land Mobile Network), i.e. the

Field	Description
	provider the SIM card is registered at.
Selected PLMN	Displays the selected PLMN. If no PLMN is selected, the Home PLNM is displayed.
Actual Network	Displays which kind of network is currently used (e.g., UMTS or GPRS).
Network Quality	Displays the current connection quality.
Location Area Code	Displays the radio cell code of the cell the modem is currently connected to.
Cell ID	Displays the Cell ID of the cell the modem is currently registered in.
Last Command	Displays the last command sent to the modem by the system.
Last Reply	Displays the last reply sent by the modem.

Values in the list Mobile Operators

Field	Description
PLMN	Displays the PLMN of the carrier.
Name	Displays the name of the carrier.
Access Type	Displays the currently available network type (e.g., UMTS oder GSM).
State	Displays the registration status.

10.5 GPS

Your bintec device gives you a Global Positioning System (GPS) with Google Maps integrated, i.e. you can determine your position and display the position found on a map.

10.5.1 GPS Configuration

In the **Physical Interfaces->GPS->GPS Configuration** menu, you can make the settings for the GPS.

GPS Configuration

GEO Zones

Basic Settings

GPS Port Status

☐ Enabled

GPS Data

Last Fix

Map

Show Position on Google Maps

☐ Enabled

OK

Cancel

Fig. 54: Physical Interfaces->GPS->GPS Configuration

The **Physical Interfaces->GPS->GPS Configuration** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
GPS Port Status	Select whether GPS is to be used. GPS is enabled with GPS Port Status = <i>Enabled</i> . By default, GPS is not enabled.
Name	Only for GPS Port Status = <i>Enabled</i> . The system automatically issues and displays a name. It cannot be changed.
NMEA TCP Port	Only for GPS Port Status = <i>Enabled</i> . You can make the NMEA data from your GPS receiver available for communication with other devices. Select whether NMEA data is to be exported via the TCP port. The exporting of NMEA data via the TCP port is disabled with a value of <i>-1</i> . The default value is <i>10110</i> . The function is enabled with <i>Enabled</i> . The function is disabled by default.

Fields in the menu GPS Data


Field	Description
Last Fix	Displays the date and time the position was last fixed.
Latitude	Displays the geographic latitude the last time the position was fixed.
Longitude	Displays the geographic longitude the last time the position was fixed.

Fields in the menu Map


Field	Description
Show Position on Google Maps	<p>You can use Google Maps to display a position that has been found by GPS on a map.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

10.5.2 GEO Zones

The software on your bintec device uses rectangular GEO zones. The coordinates of the diagonally opposed corners in the top left and bottom right are used to define each GEO zone.

The **Physical Interfaces->GPS->GEO Zones** menu displays a list of all the configured **GEO Zones**. You can delete existing entries with the icon .

10.5.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional access **GEO Zones**. After the GPS is used to fix a position for the first time, a GEO zone is created around the position found and displayed on the map. If you have not yet fixed a position, a GEO zone around the company location in Peine is displayed on the map. When you create a new GEO zone, **GEO Zones** that were previously marked display in grey.

To create or change a GEO zone, you can either enter the coordinates or move the cursor position marked on the map displayed. You can "mix" the two methods, i.e. you can enter the coordinates for a point in the GEO zone and use the cursor to specify the other point of the same GEO zone.

The **Zone Parameters** are used to assign the status **True** or **False** to a GEO zone under certain conditions, so that this status can be used to initiate actions via **Scheduling**.

GPS Configuration

GEO Zones

Basic Parameters

Description

GPS Data

Point A

Use

Enabled

Marker Position

Marker Position (Latitude, Longitude)

52° 19,4629 N, 10° 13,4451 E

Point B

Use

Enabled

Marker Position

Marker Position (Latitude, Longitude)

52° 19,2504 N, 10° 13,7455 E

Zone Parameters

Zone Valid

False

Zone Time To True

10

Seconds

Zone Time To False

10

Seconds

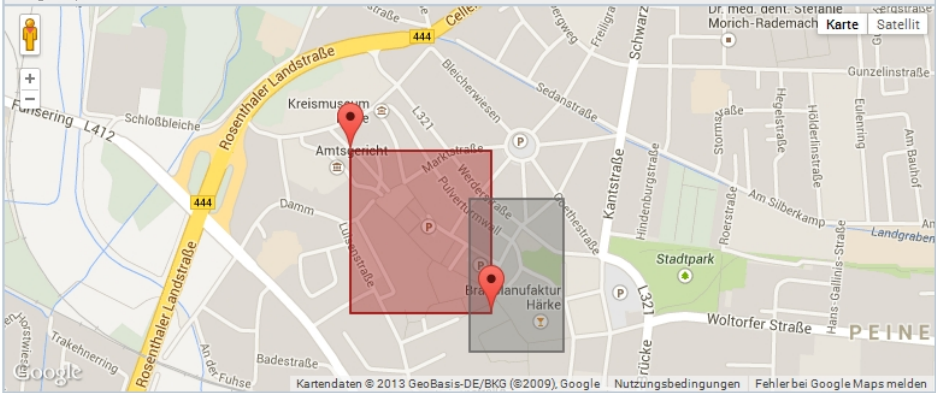
Zone Initial State

False

Zone Coverage Fail State

last-state

Google Maps



Advanced Settings

Horizontal Dilution Of Precision (HDOP)

6

OK

Cancel

Fig. 55: Physical Interfaces->GPS->GEO Zones->New

The Physical Interfaces->GPS->GEO Zones->New menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter a unique name for the GEO zone.

Fields in the menu GPS Data Point A

Field	Description
Use	<p>Select whether the coordinates or the cursor positions are to be used to configure the GEO zone on the map.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Enabled</i>: The coordinates will be used to configure the GEO zone.• <i>Position marked</i> (default value): The cursor will be used to specify the GEO zone on the map.
Marker Position (Latitude, Longitude)	<p>Only for Use = <i>position marked</i></p> <p>Displays the geographic coordinates (latitude and longitude) of the marked position. You can change the position by dragging with the mouse.</p>
Latitude	<p>Only for Use = <i>Enabled</i></p> <p>Enter the required latitude (in degrees) and the orientation (north/south). The latitude can have a value from 0° (at the equator) to ± 90° (at the poles).</p>
Longitude	<p>Only for Use = <i>Enabled</i></p> <p>Enter the required longitude and the orientation (east/west). The longitude can be measured from the zero meridian (0°) to 180° in an easterly direction and to 180° in a westerly direction.</p>

Fields in the menu **GPS Data Point B**

Field	Description
Use	<p>Select whether the coordinates or the cursor positions are to be used to configure the GEO zone on the map.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Enabled</i>: The coordinates will be used to configure the GEO zone.• <i>Position marked</i> (default value): The cursor will be used to specify the GEO zone on the map.
Marker Position (Latitude, Longitude)	<p>Only for Use = <i>position marked</i></p> <p>Displays the geographic coordinates (latitude and longitude) of</p>

Field	Description
	the marked position. You can change the position by dragging with the mouse.
Latitude	<p>Only for Use = <i>Enabled</i></p> <p>Enter a new latitude (in degrees) and the orientation (north/south). The latitude can have a value from 0° (at the equator) to ± 90° (at the poles).</p>
Longitude	<p>Only for Use = <i>Enabled</i></p> <p>Enter a new longitude and the orientation (east/west). The longitude can be measured from the zero meridian (0°) to 180° in an easterly direction and to 180° in a westerly direction.</p>

Fields in the menu **Zone Parameters**

Field	Description
Zone Valid	<p>Displays whether the current position lies within the defined zone.</p> <p>Possible values:</p> <ul style="list-style-type: none">• True: The current position lies within the defined zone.• False: The current position lies outside the defined zone.
Zone Time To True	<p>Enter the time in seconds that will elapse, when GPS reception is good, before the status changes from False to True. This transition is enabled if the GPS receiver enters the zone.</p> <p>The default value is <i>10</i> seconds.</p>
Zone Time To False	<p>Enter the time in seconds that will elapse, when GPS reception is good, before the status changes from True to False. This transition is enabled if the GPS receiver leaves the zone.</p> <p>The default value is <i>10</i> seconds.</p>
Zone Initial State	<p>Define the zone's status if GPS is switched on but no signal is being received.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>True</i>: The zone's status is True.

Field	Description
	<ul style="list-style-type: none">• <i>False</i> (default setting): The zone's status is False.• <i>true-time-false</i>: The zone's status is True. It changes to False if no GPS signal is received in the time specified under Zone Initial State Time.• <i>false-time-true</i>: The zone's status is False. It changes to True if no GPS signal is received in the time specified under Zone Initial State Time.
Zone Initial State Time	<p>Only for Zone Initial State = <i>true-time-false</i> or <i>false-time-true</i></p> <p>Define the time for the device status after being switched on.</p> <p>Enter the time in seconds during which no GPS signal is available after the device is switched on. If no GPS signal is available after this time has elapsed, the zone's status will change if the Zone Initial State parameter is set accordingly.</p> <p>You can set a value from <i>0</i> to <i>255</i> seconds.</p> <p>The default value is <i>120</i> seconds.</p>
Zone Coverage Fail State	<p>Define the zone's status if the receiver loses the GPS signal or if the signal is not strong enough to fix a position.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>True</i>: The zone's status is True.• <i>False</i>: The zone's status is False.• <i>true-time-false</i>: The zone's status is True. It changes to False if a GPS signal of adequate strength is not received in the time specified under Zone Coverage Fail State Time.• <i>false-time-true</i>: The zone's status is False. It changes to True if a GPS signal of adequate strength is not received in the time specified under Zone Coverage Fail State Time.• <i>last-state</i> (default setting): The zone's status remains unchanged.• <i>last-time-false</i>: The zone's status remains unchanged. It changes to False if a GPS signal of adequate strength is not received in the time specified under Zone Coverage Fail State Time.

Field	Description
	<ul style="list-style-type: none"><i>last-time-true</i>: The zone's status remains unchanged. It changes to True if a GPS signal of adequate strength is not received in the time specified under Zone Coverage Fail State Time.
Zone Coverage Fail State Time	<p>Only for Zone Coverage Fail State = <i>true-time-false</i>, <i>false-time-true</i>, <i>last-time-false</i> or <i>last-time-true</i></p> <p>Define the time for the device status where there is no GPS signal or it is too weak.</p> <p>Enter the time in seconds during which the device has lost the GPS signal or the signal is too weak to fix a position. If no GPS signal of adequate strength is available after this time has elapsed, the zone's status will change if the Zone Coverage Fail State parameter is set accordingly.</p> <p>You can set a value from <i>0</i> to <i>255</i> seconds.</p> <p>The default value is <i>120</i> seconds.</p>

Fields in the menu Google Maps

Field	Description
Google Maps	Displays the GEO zone on the map. You can change the two marked cursor positions by dragging with the mouse. All the GEO zones that have been created are displayed. The active GEO zone displays in red, while all the other GEO zones have a grey background.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Horizontal Dilution Of Precision (HDOP)	<p>The parameter is a measure for the distribution of the measurement values when fixing the position.</p> <p>If the value defined here is exceeded, no position is fixed.</p> <p>You can set a value from <i>2</i> to <i>20</i>.</p> <p>The default value is <i>6</i>.</p>

Chapter 11 LAN


In this menu, you configure the addresses in your LAN and can structure your local network using VLANs.

11.1 IP Configuration

In this menu, you can edit the IP configuration of the LAN and Ethernet interfaces of your device.

11.1.1 Interfaces

The existing IP interfaces are listed in the **LAN->IP Configuration->Interfaces** menu. You can edit the IP configuration of the interfaces or create virtual interfaces for special applications. Here is a list of all of the interfaces (logical Ethernet interfaces and others created in the subsystems) configured in the **System Management->Interface Mode / Bridge Groups->Interfaces** menu.

Use the  to edit the settings of an existing interface (bridge groups, Ethernet interfaces in routing mode).

You can use the **New** button to create virtual interfaces. However, this is only needed in special applications (e.g. BRRP).

Depending on the option selected, different fields and options are available. All the configuration options are listed below.



Note

Please note:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the fallback IP address is deleted automatically and your device will no longer function over this address.


However, if you have set up a connection to the device over the fallback IP address or have assigned an IP address with the **Dime Manager** in the basic configuration, you will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

Example of subnets

If your device is connected to a LAN that consists of two subnets, you should enter a second **IP Address / Netmask**.

The first subnet has two hosts with the IP addresses 192.168.42.1 and 192.168.42.2, for example, and the second subnet has two hosts with the IP addresses 192.168.46.1 and 192.168.46.2. To be able to exchange data packets with the first subnet, your device uses the IP address 192.168.42.3, for example, and 192.168.46.3 for the second subnet. The netmasks for both subnets must also be indicated.

11.1.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create virtual interfaces.

Interfaces

Basic Parameters

Based on Ethernet Interface

Select one

Address Mode

Static

DHCP

IP Address / Netmask

IP Address

Netmask

Add

Interface Mode

Untagged

Tagged (VLAN)

MAC Address

00:a0:f9

Use built-in

VLAN ID

1

Advanced Settings

Proxy ARP

Enabled

TCP-MSS Clamping

Enabled

OK

Cancel

Fig. 56: LAN->IP Configuration->Interfaces->/New

The LAN->IP Configuration->Interfaces->/New menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Based on Ethernet Interface	This field is only displayed if you are editing a virtual routing interface.

Field	Description
	Select the Ethernet interface for which the virtual interface is to be configured.
Address Mode	<p>Select how an IP address is assigned to the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Static</i> (default value): The interface is assigned a static IP address in IP Address / Netmask.• <i>DHCP</i>: An IP address is assigned to the interface dynamically via DHCP.
IP Address / Netmask	<p>Only for Address Mode = <i>Static</i></p> <p>With Add, add a new address entry, enter the IP Address and the corresponding Netmask of the virtual interface.</p>
Interface Mode	<p>Only for physical interfaces in routing mode and for virtual interfaces.</p> <p>Select the configuration mode of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Untagged</i> (default value): The interface is not assigned for a specific purpose.• <i>Tagged (VLAN)</i>: This option only applies for routing interfaces. <p>You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. The definition of a MAC address in MAC Address is optional in this mode.</p>
MAC Address	Enter the MAC address associated with the interface. For virtual interfaces, you can use the MAC address of the physical interface under which the virtual interface was created by activating Use built-in , but VLAN IDs must be different. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed).
VLAN ID	<p>Only for Interface Mode = <i>Tagged (VLAN)</i></p> <p>This option only applies for routing interfaces. Assign the inter-</p>

Field	Description
	face to a VLAN by entering the VLAN ID of the relevant VLAN. Possible values are <i>1</i> (default value) to <i>4094</i> .

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
DHCP MAC Address	<p>Only for Address Mode = <i>DHCP</i></p> <p>If Use built-in is activated (default setting), the hardware MAC address of the Ethernet interface is used. In the case of physical interfaces, the current MAC address is entered by default.</p> <p>If you disable Use built-in, you enter an MAC address for the virtual interface, e.g. <i>00:e1:f9:06:bf:03</i>.</p> <p>Some providers use hardware-independent MAC addresses to allocate their clients IP addresses dynamically. If your provider has assigned you a MAC address, enter this here.</p>
DHCP Hostname	<p>Only for Address Mode = <i>DHCP</i></p> <p>Enter the host name requested by the provider. The maximum length of the entry is 45 characters.</p>
DHCP Broadcast Flag	<p>Only for Address Mode = <i>DHCP</i></p> <p>Choose whether or not the BROADCAST bit is set in the DHCP requests for your device. Some DHCP servers that assign IP addresses by UNICAST do not respond to DHCP requests with the set BROADCAST bit. In this case, it is necessary to send DHCP requests in which this bit is not set. In this case, disable this option.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Proxy ARP	<p>Select whether your device is to respond to ARP requests from its own LAN on behalf of defined remote terminals.</p> <p>The function is activated by selecting <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.
TCP-MSS Clamping	<p>Select whether your device is to apply MSS Clamping. To prevent IP packets fragmenting, the MSS (Maximum Segment Size) is automatically decreased by the device to the value set here.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default. Once enabled, the default value <i>1350</i> is entered in the input field.</p>

11.2 VLAN

By implementing VLAN segmentation in accordance with 802.1Q, you can configure VLANs on your device. The wireless ports of an access point, in particular, are able to remove the VLAN tag of a frame sent to the clients and to tag received frames with a pre-defined VLAN ID. This functionality makes an access point nothing less than a VLAN-compliant switch with the enhancement of grouping clients into VLAN groups. In general, VLAN segmenting can be configured with all interfaces.

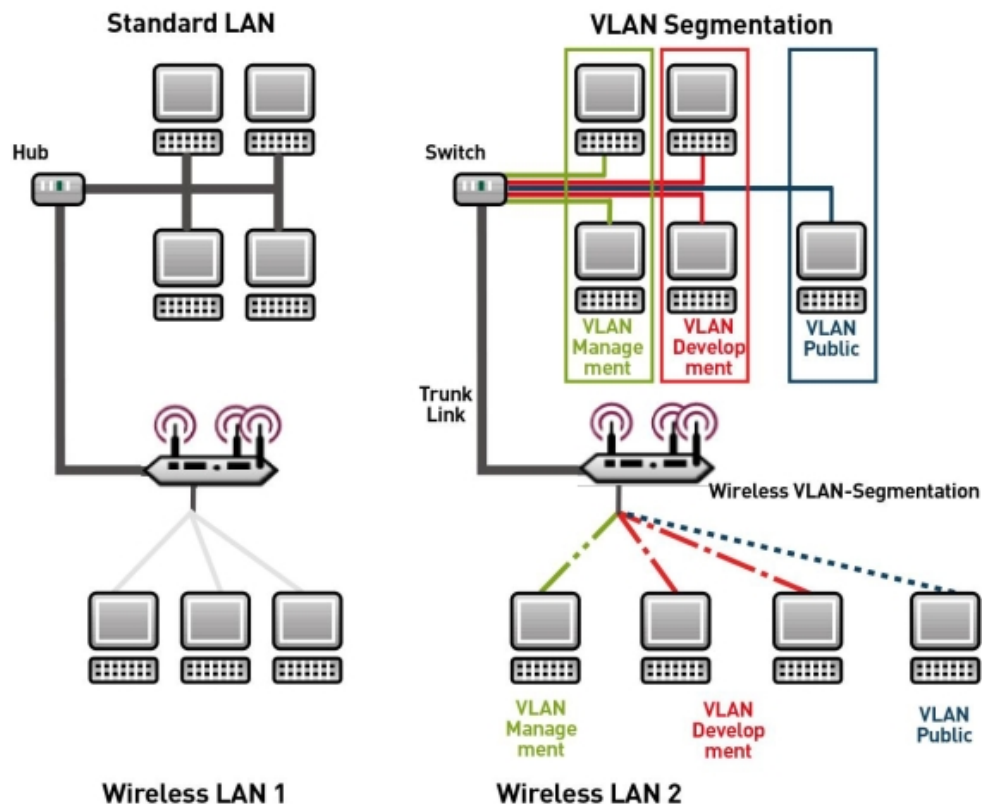


Fig. 57: VLAN segmenting

VLAN for Bridging and VLAN for Routing

In the **LAN->VLAN** menu, VLANs (virtual LANs) are configured with interfaces that operate in Bridging mode. Using the **VLAN** menu, you can make all the settings needed for this and query their status.




Caution

For interfaces that operate in Routing mode, you only assign a VLAN ID to the interface. You define this via the parameters **Interface Mode** = *Tagged (VLAN)* and field **VLAN ID** in menu **LAN->IP Configuration->Interfaces->New**.

11.2.1 VLANs

In this menu, you can display all the VLANs already configured, edit your settings and create new VLANs. By default, the *Management* VLAN is available, to which all interfaces are assigned.

11.2.1.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button in order to create new VLANs.

VLANsPort ConfigurationAdministration

Configure VLAN

VLAN Identifier

1

VLAN Name

Management

VLAN Members

Interface

en1-4

Egress Rule

Untagged

Delete


OK

Cancel

Fig. 58: LAN->VLAN->VLANs->New

The **LAN->VLAN->VLANs->New** menu consists of the following fields:

Fields in the Configure VLAN menu.

Field	Description
VLAN Identifier	Enter the number that identifies the VLAN. In the  menu, you can no longer change this value. Possible values are 1 to 4094.
VLAN Name	Enter a unique name for the VLAN. A character string of up to 32 characters is possible.
VLAN Members	Select the ports that are to belong to this VLAN. You can use the Add button to add members. For each entry, also select whether the frames to be transmitted from this port are to be transmitted <i>Tagged</i> (i.e. with VLAN information) or <i>Untagged</i> (i.e. without VLAN information).

11.2.2 Port Configuration

In this menu, you can define and view the rules for receiving frames at the VLAN ports.

VLANsPort ConfigurationAdministration

View 20 per page<<>>Filter in NoneequalGo

Interface	PVID	Drop untagged frames	Drop non-members
en1-4	1 - Management	<input type="checkbox"/>	<input type="checkbox"/>

Page: 1, Items: 1 - 1

OK

Cancel

Fig. 59: LAN->VLANs->Port Configuration

The LAN->VLANs->Port Configuration menu consists of the following fields:

Fields in the Port Configuration menu.

Field	Description
Interface	Shows the port for which you define the PVID and processing rules.
PVID	Assign the selected port the required PVID (Port VLAN Identifier). If a packet without a VLAN tag reaches this port, it is assigned this PVID.
Drop untagged frames	If this option is enabled, untagged frames are discarded. If the option is disabled, untagged frames are tagged with the PVID defined in this menu.
Drop non-members	If this option is enabled, all tagged frames that are tagged with a VLAN ID to which the selected port does not belong are discarded.

11.2.3 Administration

In this menu, you make general settings for a VLAN. The options must be configured separately for each bridge group.

VLANs

Port Configuration

Administration

Bridge Group br0 VLAN Options

Enable VLAN

☐ Enabled

Management VID

1 - Management

OK

Cancel

Fig. 60: LAN->VLANs->Administration

The LAN->VLANs->Administration menu consists of the following fields:

Fields in the Bridge Group br<ID> VLAN Options menu

Field	Description
Enable VLAN	Enable or disable the specified bridge group for VLAN. The function is enabled with <i>Enabled</i> . The function is not activated by default.
Management VID	Select the VLAN ID of the VLAN in which your device is to operate.

Chapter 12 Wireless LAN

In the case of wireless LAN or **Wireless LAN** (WLAN = Wireless Local Area Network), this relates to the creation of a network using wireless technology.

Network functions

Like a wired network, a WLAN offers all the main network functions. Access to servers, files, printers, and the e-mail system is just as reliable as company-wide Internet access. Because the devices do not require any cables, the great advantage of WLAN is that there are no building-related restrictions (i.e. the device location does not depend on the position and number of connections).

Currently applicable standard: IEEE 802.11

In the case of 802.11-WLANs, all the functions of a wired network are possible. WLAN transmits inside and outside buildings with a maximum of 100 mW.

IEEE 802.11g is currently the most widespread standard for wireless LANs and offers a maximum data transmission rate of 54 mbps. This procedure operates in the radio frequency range of 2.4 GHz, which ensures that parts of the building are penetrated as effectively as possible with a low transmission power that poses no health risks.

A 802.11g-compatible standard is 802.11b, which operates in the 2.4 GHz range (2400 MHz - 2485 MHz) and offers a maximum data transmission rate of 11 mbps. 802.11b and 802.11g WLAN systems involve no charge or login.

With 802.11a, bandwidths of up to 54 mbps can be used in the 5150 GHz to 5725 MHz range. With the higher frequency range, 19 non-overlapping frequencies are available (in Germany). This frequency range can also be used without a licence in Germany. In Europe, transmission power of not just 30 mW but 1000 mW can be used with 802.11h, but only if TPC (TX Power Control, method for controlling transmission power in wireless systems to reduce interferences) and DFS (Dynamic Frequency Selection) are used. The purpose of TPC and DFS is to ensure that satellite connections and radar devices are not interfered with.

The standard 802.11n (Draft 2.0) uses MIMO technology (Multiple Input Multiple Output) for data transmission that allows data transfer via WLAN over longer distances or with higher data rates. With a bandwidth of 20 or 40 MHz, a gross data rate of 150 Mbps or 300 Mbps is achieved.

An amendment to the Telecommunications Act (TKG) allowed the 5.8 GHz band (5755 MHz - 5875 MHz) to be used for so-called BFWA applications (Broadband Fixed Wireless Access). This simply requires registration with the Federal Network Agency. However, the use of TPC and DFS is mandatory in this case.

12.1 WLAN

In the **Wireless LAN->WLAN** menu, you can configure all WLAN modules of your device.

Depending on the model, one or two WLAN modules, **WLAN 1** and, where applicable, **WLAN 2**, are available.

12.1.1 Radio Settings

In the **Wireless LAN->WLAN->Radio Settings** menu, an overview of all the configuration options for the WLAN module is displayed.

Radio Settings

Radio Settings							
MAC Address	Operation Mode	Operation Band	Channel In Use	Maximum Bitrate	Transmit Power	Status	
00:00:00:00:00:00	Off	2.4 GHz	6	Auto	Max.		

Fig. 61: **Wireless LAN->WLAN->Radio Settings**

12.1.1.1 Radio Settings->

In this menu, you change the settings for the wireless module.

Select the icon to edit the configuration.

Radio Settings

Wireless Settings	
Operation Mode	Access-Point / Bridge Link Master
Operation Band	2.4 GHz In/Outdoor
Channel	Auto
Selected Channel	0
Transmit Power	Max.
Performance Settings	
Wireless Mode	802.11g
Airtime fairness	<input type="checkbox"/> Enabled

Advanced Settings

Channel Plan	All
RTS Threshold	Always off
Short Guard Interval	<input checked="" type="checkbox"/> Enabled
Fragmentation Threshold	2346 Bytes

OKCancel

Fig. 62: **Wireless LAN->WLAN->Radio Settings->**  for **Operation Mode** *Access-Point / Bridge Link Master*


Radio Settings

Wireless Settings	
Operation Mode	Access Client
Operation Band	2.4 GHz
Channel	0
Selected Channel	0
Used Secondary Channel	0
Bandwidth	20 MHz
Number of Spatial Streams	2
Transmit Power	Max.
Performance Settings	
Wireless Mode	802.11b/g/n

Advanced Settings

OKCancel

Fig. 63: **Wireless LAN WLAN Radio Settings**  for **Operation Mode** *Access Client*

The **Wireless LAN->WLAN->Radio Settings->**  menu consists of the following fields:

Fields in the menu Wireless Settings

Field	Description
Operation Mode	<p>Define the mode in which the wireless module of your device is to operate.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Off</i> (default value): The wireless module is not active.• <i>Access-Point / Bridge Link Master</i>: Your device is used as an access point in your network.• <i>Access Client</i>: Your device serves as an Access Client in your network.• <i>Bridge Link Client</i>: Your device is used as a wireless bridge link in your network (available only for the devices of the bintec W1003n, W2003n, W2003n-ext und W2004n series) .
Operation Band	<p>Select the operation band and, where applicable, the usage area of the wireless module.</p> <p>For Operation Mode = <i>Access-Point / Bridge Link Master</i> or <i>Bridge Link Client</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>2.4 GHz In/Outdoor</i> (default value): Your device is operated at 2.4 GHz (mode 802.11b and mode 802.11g), inside or outside buildings.• <i>5 GHz Indoor</i>: Your device runs in 5 GHz (Mode 802.11a/h) inside buildings.• <i>5 GHz Outdoor</i>: Your device runs in 5 GHz (Mode 802.11a/h) outside buildings.• <i>5 GHz In/Outdoor</i>: Your device is run with 5 GHz (Mode 802.11a/h) inside or outside buildings.
Usage Area	<p>Only for Operation Mode = <i>Access Client</i> and Operation Band = <i>2.4 and 5 GHz</i> or <i>5 GHz</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Indoor-Outdoor</i> (default value)• <i>Indoor</i>

Field	Description
	<ul style="list-style-type: none"><i>Outdoor</i>
Channel	<p>The number of channels you can select depends on the country setting. Please consult the data sheet for your device.</p> <p>Access Point Mode / Bridge Mode:</p> <p>Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels.</p> <p>In the case of manual channel selection, please make sure first that the clients actually support these channels.</p> <p>Possible values:</p> <ul style="list-style-type: none">For Operation Band = <i>2.4 GHz In/Outdoor</i> <p>Possible values are <i>1</i> to <i>13</i> and <i>Auto</i> (default value). <i>Auto</i> is not possible in bridge mode.</p> <ul style="list-style-type: none">For Operation Band = <i>5 GHz Indoor</i> <p>Possible values are <i>36</i>, <i>40</i>, <i>44</i>, <i>48</i> and <i>Auto</i> (standard value)</p> <ul style="list-style-type: none">For Operation Band = <i>5 GHz In/Outdoor</i> and <i>5 GHz Outdoor</i> <p>Only the <i>Auto</i> option is possible here.</p> <p>Access Client Mode:</p> <p>In the Access Client Mode no channel you can select. The used channel is shown.</p>
Selected Channel	Displays the channel used.
Used Secondary Channel	Not for Operation Mode = <i>Access-Point / Bridge Link Master</i>

Field	Description
	Displays the second channel used.
Bandwidth	<p>For Operation Mode = <i>Access-Point / Bridge Link Master</i> or <i>Bridge Link Client</i></p> <p>Not for Operation Band = <i>2.4 GHz In/Outdoor</i></p> <p>Select how many channels are to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>20 MHz</i> (default value): One channel with 20 MHz bandwidth is used.• <i>40 MHz</i>: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channels and the other as an expansion channel.
Number of Spatial Streams	<p>Not for Wireless Mode = <i>802.11a</i></p> <p>Select how many traffic flows are to be used in parallel.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>2</i>: Two traffic flows are used.• <i>1</i>: One traffic flow is used.
Transmit Power	<p>Select the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. The maximum value for Transmit Power is country-dependent.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Max.</i> (default value): The maximum antenna power is used.• <i>5 dBm</i>• <i>8 dBm</i>• <i>11 dBm</i>• <i>14 dBm</i>• <i>16 dBm</i>• <i>17 dBm</i>

Fields in the menu Performance Settings


Field	Description
Wireless Mode	<p>Select the wireless technology that the access point is to use.</p> <p>Only for Operation Mode = <i>Access Point / Bridge Link Master</i> and Operation Band = <i>2.4 GHz In/Outdoor</i> or for Operation Mode = <i>Access Client</i> and Operation Band = <i>2.4 GHz</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>802.11g</i>: The device operates only in accordance with 802.11g. 802.11b clients have no access.• <i>802.11b</i>: Your device operates only in accordance with 802.11b and forces all clients to adapt to it.• <i>802.11 mixed (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g.• <i>802.11 mixed long (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur.• <i>802.11 mixed short (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates).• <i>802.11b/g/n</i>: Your device operates according to either 802.11b, 802.11g or 802.11n.• <i>802.11g/n</i>: Your device operates according to either 802.11g or 802.11n.• <i>802.11n</i>: Your device operates only according to 802.11n. <p>For Operation Band = <i>5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor, 5.8 GHz Outdoor</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>802.11a</i>: The device operates only in accordance with 802.11a.• <i>802.11n</i>: Your device operates only according to 802.11n.• <i>802.11a/n</i>: Your device operates according to either

Field	Description
	802.11a or 802.11n.
Airtime fairness	<p>This function is not available for all devices.</p> <p>The Airtime fairness function ensures that the access point's send resources are distributed intelligently to the connected clients. This means that a powerful client (e. g. a 802.11n client) cannot achieve only a poor flow level, because a less powerful client (e. g. a 802.11a client) is treated in the same way when apportioning.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>This fuction is only applied to unprioritized frames of the WMM Classe "Background".</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu for operating mode = Access Point / Bridge Link Master

Field	Description
Channel Plan	<p>Only for Operation Mode = <i>Access-Point / Bridge Link Master</i> and Channel = <i>Auto</i></p> <p>Select the desired channel plan.</p> <p>The channel plan makes a preselection when a channel is selected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>All</i>: All channels can be dialled when a channel is selected.• <i>Auto</i>: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided.• <i>User defined</i>: Select the desired channels.
Selected Channels	Only for Channel Plan = <i>User defined</i>

Field	Description
	<p>The currently selected channels are displayed here.</p> <p>With Add you can add channels. If all available channels are displayed, you cannot add any more entries.</p> <p>You can delete entries with the  icon.</p>
RTS Threshold	<p>Here, you select how the RTS/CTS mechanism is to be switched on/off.</p> <p>If you choose <i>User-defined</i>, you can specify in the input field the data packet length threshold in bytes (1 - 2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point. The mechanism can also be switched on/off independently of the data packet length by selecting the value <i>Always on</i> or <i>Always off</i>(default value).</p>
Short Guard Interval	<p>Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.</p>
Fragmentation Threshold	<p>Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). Low values are recommended for this field in areas with poor reception and in the event of radio interference.</p> <p>Possible values are <i>256</i> to <i>2346</i>.</p> <p>The default value is <i>2346</i> bytes.</p>

If *Access Client* is selected for **Operation Mode**, the following parameters are additionally available under **Advanced Settings**:

Advanced Settings

Scan channels	All
Roaming Profile	Normal Roaming
Scan Threshold	-70 dBm
Scan Interval	10000 ms
Min. Period Active Scan	105 ms
Max. Period Active Scan	500 ms
Min. Period Passive Scan	130 ms
Max. Period Passive Scan	500 ms
Max. Scan Duration	50000 ms

OK

Cancel

Fig. 64: Wireless LAN->WLAN->Radio Settings->



Fields in the menu Advanced Settings for Access Client Mode.

Field	Description
Scan channels	<p>Choose the channels which the WLAN client automatically scans for available wireless networks.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>All</i> (default value): All channels are scanned.• <i>Auto</i>: The channel is automatically selected.• <i>User defined</i>: The desired channels can therefore be defined.
User Defined Channel Plan	<p>Only for Scan channels = <i>User defined</i></p> <p>Define the channels which the WLAN client automatically scans for available wireless networks.</p>
Roaming Profile	<p>Select the roaming profile. The options available include typical roaming functions.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Fast Roaming</i>: The WLAN client searches for available wireless networks as soon as the radio signal of the existing radio connection becomes unsuitable for higher data rates.• <i>Normal Roaming</i> (default value): Standard roaming.• <i>Slow Roaming</i>: The WLAN client searches for available wireless networks as soon as the radio signal of the existing

Field	Description
	<p>radio connection becomes weaker.</p> <ul style="list-style-type: none">• <i>No Roaming</i>: The WLAN client searches for available wireless networks if it is no longer connected to a wireless network.• <i>Custom Roaming</i>: Specify the individual roaming parameters.
Scan Threshold	<p>Indicates the value in dBm above which the system scans for available wireless networks in the background.</p> <p>The value can only be modified for Roaming Profile = <i>Custom Roaming</i>. The default value is <i>-70 dBm</i>.</p>
Scan Interval	<p>Indicates the interval in milliseconds after which the system scans for available wireless networks.</p> <p>The value can only be modified for Roaming Profile = <i>Custom Roaming</i>. The default value is <i>5000 ms</i>.</p>
Min. Period Active Scan	<p>Displays the minimum active scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for Roaming Profile = <i>Custom Roaming</i>. The default value is <i>10 ms</i>.</p>
Max. Period Active Scan	<p>Displays the maximum active scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for Roaming Profile = <i>Custom Roaming</i>. The default value is <i>40 ms</i>.</p>
Min. Period Passive Scan	<p>Displays the minimum passive scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for Roaming Profile = <i>Custom Roaming</i>. The default value is <i>20 ms</i>.</p>
Max. Period Passive Scan	<p>Displays the maximum passive scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for Roaming Profile = <i>Custom Roaming</i>. The default value is <i>120 ms</i>.</p>
Max. Scan Duration	<p>Displays the maximum scanning duration for a frequency in mil-</p>

Field	Description
	liseconds. The value can only be modified for Roaming Profile = <i>Custom Roaming</i> . The default value is <i>50000 ms</i> .

12.1.2 Wireless Networks (VSS)

If you are operating your device in Access Point Mode (**Wireless LAN->WLAN->Radio Settings->****->Operation Mode** = *Access-Point / Bridge Link Master*), in the menu **Wireless LAN->WLAN->Wireless Networks (VSS)->** **/ New** you can edit the wireless networks required or set new ones up.



Note

The preset wireless network default has the following security settings in the ex works state:

- **Security Mode** = *WPA-PSK*
- **WPA Mode** = *WPA and WPA 2*
- **WPA Cipher** as well as **WPA2 Cipher** = *AES and TKIP*
- The **Preshared Key** is filled with an internal system value, which you must change during configuration.

Setting network names

In contrast to a LAN set up over Ethernet, a wireless LAN does not have any cables for setting up a permanent connection between the server and clients. Access violations or faults may therefore occur with directly adjacent radio networks. To prevent this, every radio network has a parameter that uniquely identifies the network and is comparable with a domain name. Only clients with a network configuration that matches that of your device can communicate in this WLAN. The corresponding parameter is called the network name. In the network environment, it is sometimes also referred to as the SSID.

Protection of wireless networks

As data can be transmitted over the air in the WLAN, this data can in theory be intercepted and read by any attacker with the appropriate resources. Particular attention must therefore be paid to protecting the wireless connection.

There are three security modes, WEP, WPA-PSK and WPA Enterprise. WPA Enterprise of-

fers the highest level of security, but this security mode is only really suitable for companies, because it requires a central authentication server. Private users should choose WEP or preferably WPA-PSK with higher security as their security mode.

WEP

802.11 defines the security standard **WEP** (Wired Equivalent Privacy = encryption of data with 40 bit (**Security Mode** = *WEP 40*) or 104 bit (**Security Mode** = *WEP 104*)). However, this widely used **WEP** has proven susceptible to failure. However, a higher degree of security can only be achieved through hardware-based encryption which required additional configuration (for example 3DES or AES). This permits even sensitive data from being transferred via a radio path without fear of it being stolen.

IEEE 802.11i

Standard IEEE 802.11i for wireless systems contains basic security specifications for wireless networks, in particular with regard to encryption. It replaces the insecure **WEP** (Wired Equivalent Privacy) with **WPA** (Wi-Fi Protected Access). It also includes the use of the advanced encryption standard (AES) to encrypt data.

WPA

WPA (Wi-Fi Protected Access) offers additional privacy by means of dynamic keys based on the Temporal Key Integrity Protocol (TKIP), and offers PSK (preshared keys) or Extensible Authentication Protocol (EAP) via 802.1x (e.g. RADIUS) for user authentication.

Authentication using EAP is usually used in large wireless LAN installations, as an authentication instance in the form of a server (e.g. a RADIUS server) is used in these cases. PSK (preshared keys) are usually used in smaller networks, such as those seen in SoHo (Small office, Home office). Therefore, all the wireless LAN subscribers must know the PSK, because it is used to generate the session key.

WPA 2

The enhancement of **WPA** is **WPA 2**. In **WPA 2**, the 802.11i standard is not only implemented for the first time in full, but another encryption algorithm AES (Advanced Encryption Standard) is also used.

Access control

You can control which clients can access your wireless LAN via your device by creating an Access Control List (**Access Control** oder **MAC-Filter**). In the Access Control List, you enter the MAC addresses of the clients that may access your wireless LAN. All other clients have no access.


Security measures

To protect the data transferred over the WLAN, the following configuration steps should be carried out in the **Wireless LAN->WLAN->Wireless Networks (VSS)->New** menu, where necessary:

- Change the access passwords for your device.
- Change the default SSID, **Network Name (SSID)** = *default*, of your access point. Set **Visible** = *Enabled*. This will exclude all WLAN clients that attempt to establish a connection with the general value for **Network Name (SSID)** *Any* and do not know the SSID settings.
- Use the available encryption methods. To do this, select **Security Mode** = *WEP 40*, *WEP 104*, *WPA-PSK* or *WPA Enterprise* and enter the relevant key in the access point under **WEP Key 1 - 4** or **Preshared Key** and in the WLAN clients.
- The WEP key should be changed regularly. To do this, change the **Transmit Key**. Select the longer 104 Bit WEP key.
- For transmission of information with very high security relevance, configure **Security Mode** = *WPA Enterprise* with **WPA Mode** = *WPA 2*. This method contains hardware-based encryption and RADIUS authentication of the client. In special cases, combination with IPSec is possible.
- Restrict WLAN access to permitted clients. Enter the MAC addresses of the wireless network cards for these clients in the **Allowed Addresses** list in the **MAC-Filter** menu (see [Fields in the menu MAC-Filter](#) on page 164).

A list of all WLAN networks is displayed in the **Wireless LAN->WLAN->Wireless Networks (VSS)** menu.

12.1.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure additional wireless networks.

Radio Settings

Wireless Networks (VSS)

Service Set Parameters

Network Name (SSID)

default

☒ Visible

Intra-cell Repeating

☒ Enabled

U-APSD

☒ Enabled

Security Settings

Security Mode

Inactive

Client load balancing

Max. number of clients - hard limit

32

Max. number of clients - soft limit

24

Client Band select

Disabled - optimized for fast roaming

MAC-Filter

Access Control

☐ Enabled

Advanced Settings

Beacon Period

100

ms

DTIM Period

2

OK

Cancel

Fig. 65: Wireless LAN->WLAN->Wireless Networks (VSS)->

The **Wireless LAN->WLAN->Wireless Networks (VSS)-> menu consists of the following fields:**


Fields in the menu **Service Set Parameters**

Field	Description
Network Name (SSID)	<div>Enter the name of the wireless network (SSID).</div> <div>Enter an ASCII string with a maximum of 32 characters.</div> <div>Also select whether the Network Name (SSID) is to be transmitted.</div> <div>The network name is displayed by selecting <i>Visible</i>.</div> <div>It is visible by default.</div>
Intra-cell Repeating	<div>Select whether communication between the WLAN clients is to be permitted within a radio cell.</div> <div>The function is activated by selecting <i>Enabled</i>.</div>

Field	Description
	The function is enabled by default.
U-APSD	Select whether the Unscheduled Automatic Power Save Delivery (U-APSD) mode is to be enabled. The function is activated by selecting <i>Enabled</i> . The function is enabled by default.

Fields in the menu Security Settings

Field	Description
Security Mode	Select the Security Mode (encryption and authentication) for the wireless network. Possible values: <ul style="list-style-type: none">• <i>Inactive</i> (default value): Neither encryption nor authentication• <i>WEP 40</i>: WEP 40 bits• <i>WEP 104</i>: WEP 104 bits• <i>WPA-PSK</i>: WPA Preshared Key• <i>WPA Enterprise</i>: 802.11i/TKIP
Transmit Key	Only for Security Mode = <i>WEP 40</i> or <i>WEP 104</i> Select one of the keys configured in WEP Key <1 - 4> as a default key. The default value is <i>Key 1</i> .
WEP Key 1-4	Only for Security Mode = <i>WEP 40</i> , <i>WEP 104</i> Enter the WEP key. Enter a character string with the right number of characters for the selected WEP mode. For <i>WEP 40</i> you need a character string with 5 characters, for <i>WEP 104</i> with 13 characters, e. g. <i>hello</i> for <i>WEP 40</i> , <i>wep1</i> for <i>WEP 104</i> .
WPA Mode	Only for Security Mode = <i>WPA-PSK</i> and <i>WPA Enterprise</i> Select whether you want to use WPA (with TKIP encryption) or

Field	Description
	<p>WPA 2 (with AES encryption), or both.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>WPA and WPA 2</i> (default value): WPA and WPA 2 can be applied.• <i>WPA</i>: Only WPA is applied.• <i>WPA 2</i>: Only WPA 2 is applied.
WPA Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for WPA Mode = <i>WPA</i> and <i>WPA and WPA 2</i></p> <p>Select the type of encryption with which to apply WPA.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>AES</i>: AES is used.• <i>TKIP</i>: TKIP is used.• <i>AES and TKIP</i> (default value): AES or TKIP is used.
WPA2 Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for WPA Mode = <i>WPA 2</i> and <i>WPA and WPA 2</i></p> <p>Select the type of encryption with which to apply WPA 2.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>AES</i>: AES is used.• <i>AES and TKIP</i> (default value): AES or TKIP is used.
Preshared Key	<p>Only for Security Mode = <i>WPA-PSK</i></p> <p>Enter the WPA password.</p> <p>Enter an ASCII string with 8 - 63 characters.</p> <div>Note<p>Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!</p></div>

Field	Description
EAP Preauthentication	<p>Only for Security Mode = <i>WPA Enterprise</i></p> <p>Select whether the EAP preauthentication function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the menu **Client load balancing**

Field	Description
Max. number of clients - hard limit	<p>Enter the maximum number of clients that can be connected to this wireless network (SSID)</p> <p>The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This maximum is distributed across all wireless networks configured for this radio module. No more new wireless networks can be created and a warning message will appear if the maximum number of clients is reached.</p> <p>Possible values are whole numbers between <i>1</i> and <i>254</i>.</p> <p>The default value is <i>32</i>.</p>
Max. number of clients - soft limit	<p>Not all devices support this function.</p> <p>To avoid a radio module being fully utilised, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the Max. number of clients - hard limit is reached.</p> <p>The value of the Max. number of clients - soft limit must be the same as or less than that of the Max. number of clients - hard limit.</p> <p>The default value is <i>28</i>.</p>

Field	Description
	You can disable this function if you set Max. number of clients - soft limit and Max. number of clients - hard limit to identical values.
Client Band select	<p>Not all devices support this function.</p> <p>This function requires a dual radio setup where the same wireless network is configured on both radio modules, but in different frequency bands.</p> <p>The Client Band select option enables clients to be moved from the frequency band originally selected to a less busy one, providing the client supports this. To achieve a changeover, the connection attempt of a client is initially refused so that the client repeats the attempt in a different frequency band.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Disabled - optimized for fast roaming</i>(default value): The function is not used for this VSS. This is useful if clients are to switch between different radio cells with as little delay as possible, e. g. with Voice over WLAN.• <i>2,4 GHz band preferred</i>: Preference is given to accepting clients in the 2.4 GHz band.• <i>5 GHz band preferred</i>: Preference is given to accepting clients in the 5 GHz band.



Fields in the menu MAC-Filter

Field	Description
Access Control	<p>Select whether only certain clients are to be permitted for this wireless network.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Allowed Addresses	Use Add to make entries and enter the MAC addresses (MAC Address) of the clients to be permitted.

Fields in the menu Advanced Settings

Field	Description
Beacon Period	<p>Enter the time in milliseconds between the sending of two beacons.</p> <p>This value is transmitted in Beacon and Probe Response Frames.</p> <p>Possible values are 1 to 65535.</p> <p>The default value is 100 ms.</p>
DTIM Period	<p>Enter the interval for the Delivery Traffic Indication Message (DTIM).</p> <p>The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data.</p> <p>Possible values are 1 to 255.</p> <p>The default value is 2.</p>

12.1.3 Client Link


If you're operating your device in Access Point mode, (**Wireless LAN->WLAN->Radio Settings->****->Operation Mode = Access Client**), you can edit the existing client links in the **Wireless LAN->WLAN->Client Link->** menu.

The **Client Mode** can be operated in infrastructure mode or in ad-hoc mode.

In a network in infrastructure mode, all clients communicate with each other via access points only. There is no direct communication between the individual clients.

In ad-hoc mode, an access client can be used as central interface between a number of terminals. In this way, devices such as computers and printers can be wirelessly interconnected.

12.1.3.1 Edit

Choose the  icon to edit existing entries.

Radio Settings

Client Link

Basic Parameters

Network Name (SSID)


Security Settings

Security Mode

Inactive

OK

Cancel

Fig. 66: Wireless LAN->WLAN->Client Link->

The **Wireless LAN->WLAN->Client Link->** menu consists of the following fields:

Fields in the Basic Parameters menu.


Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters.

Fields in the Security Settings menu.

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values: <ul style="list-style-type: none">• <i>Inactive</i> (default value): Neither encryption nor authentication• <i>WEP 40</i>: WEP 40 bits• <i>WEP 104</i>: WEP 104 bits• <i>WPA-PSK</i>: WPA Preshared Key
Transmit Key	Only for Security Mode = <i>WEP 104</i> Select one of the keys configured in WEP Key <1 - 4> as a default key. The default value is <i>Key 1</i> .
WEP Key 1 - 4	Only for Security Mode = <i>WEP 40</i> , <i>WEP 104</i> Enter the WEP key.

Field	Description
	Enter a character string with the right number of characters for the selected WEP mode. For <i>WEP 40</i> you need a character string with 5 characters, for <i>WEP 104</i> with 13 characters, e.g. <i>hello</i> for <i>WEP 40</i> , <i>wep1</i> for <i>WEP 104</i> .
WPA Mode	<p>Only for Security Mode = <i>WPA-PSK</i></p> <p>Select whether you want to use WPA or WPA 2.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>WPA</i> (default value): Only WPA is used.• <i>WPA 2</i>: Only WPA2 is used.
Preshared Key	<p>Only for Security Mode = <i>WPA-PSK</i></p> <p>Enter the WPA password.</p> <p>Enter an ASCII string with 8 - 63 characters.</p>
WPA Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and WPA Mode = <i>WPA</i></p> <p>Select which encryption method should be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>TKIP</i> (default value): Temporal Key Integrity Protocol• <i>AES</i>: Advanced Encryption Standard. <p>Both encryption methods are rated as secure, with AES offering better performance.</p>
WPA2 Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and WPA Mode = <i>WPA 2</i></p> <p>Select which encryption method is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>AES</i> (default value): Advanced Encryption Standard.• <i>TKIP</i> : Temporal Key Integrity Protocol <p>Both encryption methods are rated as secure, with AES offering better performance.</p>

12.1.3.2 Client Link Scan

After the desired Client Links have been configured, the  icon is shown in the list.

You use this icon to open the **Scan** menu.

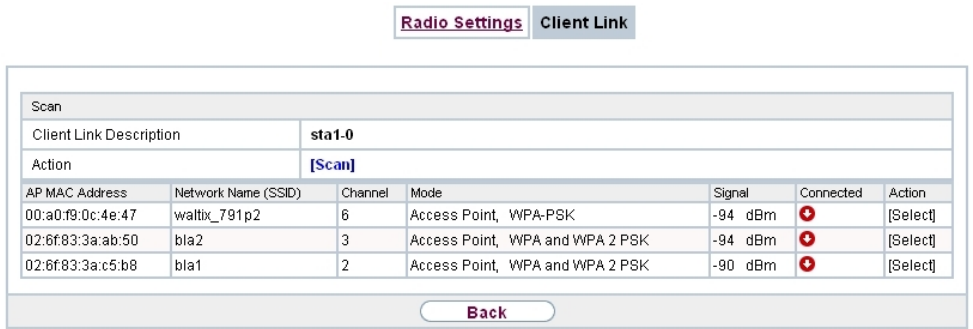




Fig. 67: Wireless LAN->WLAN->Client Link->Scan

After successful scanning, a selection of potential scan partners is displayed in the scan list. In the **Action** column, click **Select** to connect the local clients with this client. If the partners are connected with one another, the  icon appears in the **Connected** column. The  icon appears in the **Connected** column if the connection is active.

The **Wireless LAN->WLAN->Client Link->Scan** menu consists of the following fields:

Fields in the Scan menu.

Field	Description
Client Link Description	Displays the name of the client link you configured.
Action	<p>Start the scan by clicking on Scan.</p> <p>If the antennas are installed correctly on both sides and LOS is free, the client finds available clients and displays them in the following list.</p> <p>If the partner client cannot be found, check the line of sight and the antenna installation. Then carry out the Scan. The partner should then be found.</p>
AP MAC Address	Shows the MAC address of the remote client.
Network Name (SSID)	Displays the name of the remote client.
Channel	Shows the Channel used.


Field	Description
Mode	Shows the security mode (encryption and authentication) for the wireless network.
Signal	Displays the signal strength of the detected client link in dBm.
Connected	Displays the status of the link on your client.
Action	You can change the status of the client link. The available actions are displayed in this field.

12.1.4 Bridge Links

Available only for the devices of the **bintec W1003n, W2003n, W2003n-ext** und **W2004n** series.

Bridge Links allow you to create a dedicated connection between WLAN devices. A radio module operating as a slave exclusively connects to the bridge link master and does not establish or accept any other WLAN connections. A bridge link usually serves to reliably connect two networks via a WLAN connection.

12.1.4.1 Edit oder New

Select the  symbol in order to edit an existing entry. Select the **New** button in order to create a new bridge link.

Radio Settings

Wireless Networks (VSS)

Bridge Links

Basic Settings

Bridge Link Name (ID)

Preshared Key

OK

Cancel

Fig. 68: **Wireless LAN->WLAN->Bridge Links->->New**

The menu **Wireless LAN->WLAN->Bridge Links->->New** contains the following fields:

Fields in the Basic Parameters menu

Field	Description
Bridge Link Name (ID)	Depending on whether you operate the radio module as access point or as wireless bridge link, you create a bridge link in master or in slave mode.

Field	Description
	<p>If the radio module operates in Access Point mode, the bridge link is in master mode. Enter a name for the bridge link. This name also serves as the ID other devices use to connect to this bridge link.</p> <p>If the radio module is in Bridge Link Client mode, the bridge link is in slave mode. Enter the ID of the bridge link the device is supposed to connect to.</p>
Preshared Key	Enter a password for this bridge link. In master mode, this is the password other devices use to connect to this bridge link. In slave mode, it is the password of that bridge link the device is to connect to.

12.2 Administration

The **Wireless LAN->Administration** menu contains basic settings for operating your gateway as an access point (AP).

12.2.1 Basic Settings



Fig. 69: **Wireless LAN->Administration->Basic Settings**

The **Wireless LAN->Administration->Basic Settings** menu consists of the following fields:

Fields in the WLAN Administration menu.

Field	Description
Region	<p>Select the country in which the access point is to be run.</p> <p>Possible values are all the countries configured on the device's wireless module.</p>

Field	Description
	<p>The range of channels available for selection (Channel in the Wireless LAN->WLAN->Radio Settings menu) changes depending on the country setting.</p> <p>The default value is <i>Germany</i>.</p>

Chapter 13 Wireless LAN Controller

By using the wireless LAN controller, you can set up and manage a WLAN infrastructure with multiple access points (APs). The WLAN controller has a Wizard which assists you in the configuration of your access points. The system uses the CAPWAP protocol (Control and Provisioning of Wireless Access Points Protocol) for any communication between masters and slaves.

In smaller WLAN infrastructures with up to six APs, one of the AP's assumes the master function and manages the other AP's as well as itself. In larger WLAN networks a gateway, e.g. such as a **bintec R1202**, assumes the master function and manages the AP's.

Provided the controller has "located" all of the APs in its system, each of these shall receive a new passport and configuration in succession, i.e. they are managed via the WLAN controller and can no longer be amended "externally".

With the **WLAN controller** you can

- automatically detect individual access points (APs) and connect to a WLAN network
- Load the system software into the APs
- Load the configuration into the APs
- Monitor and manage APs

Please refer to your gateway's data sheet to find out the number of APs that you can manage with your gateway's wireless LAN controller and details of the licenses required.

13.1 Wizard

The **Wizard** menu offers step-by-step instructions for the set up of a WLAN infrastructure. The Wizard guides you through the configuration.

When you select the Wizard you will receive instructions and explanations on the separate pages of the Wizard.



Note

We highly recommended that you use the Wizard when initially configuring your WLAN infrastructure.

13.1.1 Basic Settings

Here you can configure all of the various settings that you require for the actual wireless LAN controller.

The wireless LAN controller uses the following settings:

Region

Select the country in which the wireless controller is to be operated.

Please note: The range of channels that can be used varies depending on the country setting.

Interface

Select the interface to be used for the wireless controller.

DHCP Server

Select whether an external DHCP server shall assign IP addresses to the APs or if you wish to assign fixed IP addresses yourself. Alternatively, you can use your device as a DHCP server. For this internal DHCP server, CAPWAP option 138 is active in order to allow communication between the master and slaves.

If you use static IP addresses in your network, you must enter these to all APs manually. The IP addresses of the wireless LAN controller must be entered for each AP in the **System Management->Global Settings->System** menu in the **Manual WLAN Controller IP Address** field.

Please note: Make sure that option 138 is active when using an external DHCP server.

If you wish to use a bintec elmeg Gateway for example as a DHCP server, click on the **GUI** menu for this device under **Local Services->DHCP Server->DHCP Pool->New->Advanced Settings** in the **DHCP Options** field on the **Add** button. Select as **Option** *CAPWAP Controller* and in the **Value** field enter the IP address of the WLAN controller.

IP Address Range

If the IP addresses are to be assigned internally, you must enter the start and end IP address of the desired range.

Please note: If you click on **Next**, a warning appears which informs you that continuing will overwrite the wireless LAN controller configuration. By clicking on **OK** you signal that you agree with this and wish to continue with the configuration.

13.1.2 Radio Profile

Select which frequency band your WLAN controller shall use.

If the *2.4 GHz Radio Profile* is set then the 2.4 GHz frequency band is used.

If the *5 GHz Radio Profile* is set then the 5 GHz frequency band is used.


If the corresponding device contains two wireless modules, you can **Use two independent radio profiles**. This assigns *2.4 GHz Radio Profile* to module 1 and *5 GHz Radio Profile* to module 2.


The function is activated by selecting *Enabled*.

The function is disabled by default.

13.1.3 Wireless Network

All of the configured wireless networks (VSS) are displayed in the list. At least one wireless network (VSS) is set up. This entry cannot be deleted.

Click on  to edit an existing entry.

You can also delete entries using the  icon.


With **Add**, you can create new entries. You can create up to eight wireless networks (VSS) for a wireless module.



Note

If you wish to use the default wireless network that is set up, you must at least change the **Preshared Key** parameters. Otherwise you will be prompted.

13.1.3.1 Change or add wireless networks

Click on  to edit an existing entry.

With **Add**, you can create new entries.

The following parameters are available

Network Name (SSID)

Enter the name of the wireless network (SSID).

Enter an ASCII string with a maximum of 32 characters.

Also select whether the **Network Name (SSID)** *Visible* is to be transmitted.

Security Mode

Select the security mode (encryption and authentication) for the wireless network.

Please note: *WPA Enterprise* means 802.11x.

WPA Mode

Select for **Security Mode** = *WPA-PSK* or *WPA Enterprise*, whether you wish to use WPA oder WPA 2 or both.

Preshared Key

Enter the WPA password for **Security Mode** = *WPA-PSK*.

Enter an ASCII string with 8 - 63 characters.



Important

Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!

Radius Server

You can control access to a wireless network via a RADIUS server.

With **Add**, you can create new entries.

Enter the IP address and the password of the desired RADIUS server.

EAP Preauthentication

For **Security Mode** = *WPA Enterprise*, select whether the EAP preauthentication function is to be *Enabled*. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device.

VLAN

Select whether the VLAN segmentation is to be used for this wireless network.


If you wish to use VLAN segmentation, enter a value between 2 and 4094 in the input field in order to identify the VLAN. (VLAN ID 1 is not possible!).

**Note**

Before you continue, please ensure that all access points that the WLAN controller shall manage are correctly wired and switched on.

13.1.4 Start automatic installation

You will see a list of all detected access points.

If you wish to change the settings of a detected AP, click on  in the corresponding entry.

You will see the settings for all selected access points. You can change these settings.

The following parameters are available in the **Access Point Settings** menu:

Location

Displays the stated locality of the AP. You can enter another locality.

Assigned Wireless Network (VSS)

Displays the wireless networks that are currently assigned.

The following parameters are available in the wireless module 1 menu:

(The parts wireless module 1 and wireless module 2 are displayed if the AP has two wireless modules.)

Operation Mode

Select the mode in which the wireless module is to be operated.

Possible values:

- *On* (default value): The wireless module is used as an access point in your network.
- *Off*: The wireless module is not active.

Active Radio Profile

Displays the wireless module profile that is currently selected. You can select another wireless module profile from the list if more than one wireless module profile are being set up.

Channel

Displays the channel that is assigned. You can select an alternative channel.

The number of channels you can select depends on the country setting. Please consult the data sheet for your device.

**Note**

Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels.

In the case of manual channel selection, please make sure first that the APs actually support these channels.

Transmit Power

Displays the transmission power in dBm. You can select another transmission power.

With **OK** you apply the settings.

Select the access points that your WLAN controller shall manage. In the **Manage** column, click on the desired entries or click on **Select all** in order to select all entries. Click the **Deselect all** button to disable all entries and to then select individual entries if required (e.g. for large lists).

Click on **Start** in order to install the WLAN and automatically assign the frequencies.

**Note**

If there are not enough licences available, the message "The maximum number of slave access points that can be supported has been exceeded". Please check your licences. If this message is displayed then you should obtain additional licences if appropriate.

During the installation of the WLAN and the allocation of frequencies, on the messages displayed you will see how far the installation has progressed. The display is continuously updated.

Provided that non-overlapping wireless channels are located for all access points, the configuration that is set in the Wizard is transferred to the access points.

When the installation is complete, you will see a list of the **Managed** access points.

Under **Configure the Alert Service for WLAN surveillance**, click **Start** to monitor your managed APs. You are taken to the **External Reporting->Alert Service->Alert Recipient** menu with the default setting **Event** = *Managed AP offline*. You can specify that you wish to be notified by e-mail if the *Managed AP offline* event occurs.

Click under **New Neighborscan** on **Start**, to rescan adjacent AP's. You will receive a warning that the wireless modules of the access points must also be disabled for a certain period of time. When you start the process with **OK**, a progress bar is displayed. The located AP display is updated every ten seconds.

13.2 Controller Configuration

In this menu, you make the basic settings for the wireless LAN controller.

13.2.1 General

General

Basic Settings

Region	Germany
Interface	LAN_EN1-0
DHCP Server	DHCP Server with enabled CAPWAP option (138): <input checked="" type="radio"/> External or static <input type="radio"/> Internal
Slave AP location	<input checked="" type="radio"/> Local (LAN) <input type="radio"/> Remote (WAN)
Slave AP LED mode	Status

OKCancel

Fig. 70: Wireless LAN Controller->Controller Configuration->General

The **Wireless LAN Controller->Controller Configuration->General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Region	Select the country in which the wireless LAN controller is to be operated. Possible values are all the countries configured on the device's wireless module.

Field	Description
	<p>The range of channels that can be used varies depending on the country setting.</p> <p>The default value is <i>Germany</i>.</p>
Interface	Select the interface to be used for the wireless controller.
DHCP Server	<p>Select whether an external DHCP server shall assign IP addresses to the APs or if you wish to assign fixed IP addresses yourself. Alternatively, you can use your device as a DHCP server. For this internal DHCP server, CAPWAP option 138 is active in order to allow communication between the master and slaves.</p> <p>Please note: Make sure that option 138 is active when using an external DHCP server.</p> <p>If you wish to use a bintec elmeg Gateway for example as a DHCP server, click on the GUI menu for this device under Local Services->DHCP Server->DHCP Pool->New->Advanced Settings in the DHCP Options field on the Add button. Select as Option <i>CAPWAP Controller</i> and in the Value field enter the IP address of the WLAN controller.</p> <p>If you use static IP addresses in your network, you must enter these to all APs manually. The IP addresses of the wireless LAN controller must be entered for each AP in the System Management->Global Settings->System menu in the Manual WLAN Controller IP Address field.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>External or static</i> (default value): An external DHCP server with an CAPWAP option 138 enabled assigns the IP addresses to the APs or you can give static IP addresses to the APs.• <i>Internal</i>: Your device, on which the CAPWAP option 138 is active, assigns the IP addresses to the APs.
IP Address Range	<p>Only for DHCP Server = <i>Internal</i></p> <p>Enter the start and end IP address of the range. These IP addresses and your device must originate from the same network.</p>

Field	Description
Slave AP location	<p>Select whether the APs that the wireless LAN controller is to manage are located in the LAN or the WAN.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Local (LAN)</i> (default value)• <i>Remote (WAN)</i> <p>The <i>Remote (WAN)</i> setting is useful if, for example, there is a wireless LAN controller installed at head office and its APs are distributed to different branches. If the APs are linked via VPN, it may be that a connection is terminated. If this happens, the relevant AP with the setting <i>Remote (WAN)</i> maintains its configuration until the connection is reestablished. It then boots up and the controller and the AP then resynchronize.</p>
Slave AP LED mode	<p>Select the lighting scheme of the slave AP LEDs.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>State</i> (default value): Only the status LED flashes once per second.• <i>Flashing</i>: All LEDs show their standard behavior.• <i>Off</i>: All LEDs are deactivated.

13.3 Slave AP configuration

In this menu, you will find all of the settings that are required to manage the slave access points.

13.3.1 Slave Access Points

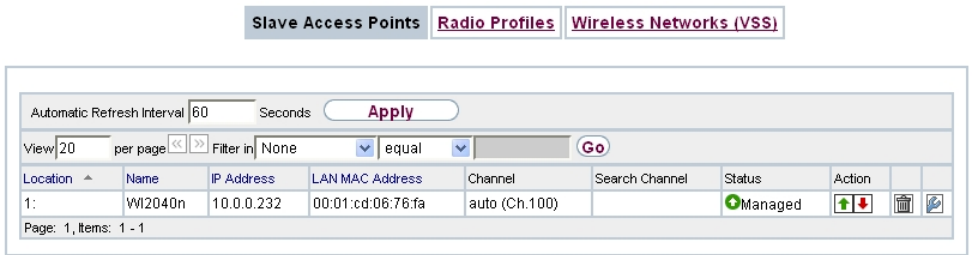


Fig. 71: Wireless LAN Controller->Slave AP configuration->Slave Access Points

In the **Wireless LAN Controller->Slave AP configuration->Slave Access Points** menu a list of all APs found with the wizard is displayed.

You will see an entry with a parameter set for each access point (**Location**, **Name**, **IP Address**, **LAN MAC Address**, **Channel**, **Search Channel**, **Status**, **Action**). Choose whether the selected Access Pont is to be managed by the WLAN Controller by clicking the button or the button in the **Action** column.


You can disconnect the Access Point from the WLAN Controller and therefore remove it from your WLAN infrastructure by click on the button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.


Click on the **START** button under **Channel reallocation** in order to reassign any assigned channels, e.g. when a new access point has been added.

Possible values for Status

Status	Meaning
Discovered	The AP has registered at the wireless LAN controller. The controller has prompted the required parameters from the AP.
Initialising	The WLAN controller and the APs "communicate" via CAPWAP. The configuration is transferred and enabled to the APs.
Managed	The AP is set to "Managed" status. The controller has sent a configuration to the AP and has enabled this. The AP is managed centrally from the controller and cannot be configured via the GUI.
No License Available	The AP does not have an unassigned licence for this AP.
Offline	The AP is either administratively disabled or switched off or has its power supply cut off etc.

13.3.1.1 Edit

Choose the  icon to edit existing entries.

You can also delete entries using the  icon. If you have deleted APs, these will be located again but shall not be configured.

Slave Access Points

Radio Profiles

Wireless Networks (VSS)


Access Point Settings

Device	WI2040n
Location	
Name	WI2040n
Description	
CAPWAP Encryption	<input checked="" type="checkbox"/> Enabled
Radio Module1	
Operation Mode	<input checked="" type="radio"/> On <input type="radio"/> Off
Active Radio Profile	Select one
Channel	No Profile Selected!
Used Channel	0
Transmit Power	Max.
Assigned Wireless Network (VSS)	<div><div>Profile</div><div>MAC Address</div><div>Add</div></div>

OK

Cancel

Fig. 72: Wireless LAN Controller->Slave AP configuration->Slave Access Points->

The data for wireless module 1 and wireless module 2 are displayed in the **Wireless LAN Controller->Slave AP configuration->Slave Access Points->** menu if the corresponding device has two wireless modules. With devices featuring a single wireless module, the data for wireless module 1 are displayed.

The menu consists of the following fields:

Fields in the Access Point Settings menu.

Field	Description
Device	Displays the type of device for the AP.
Location	Displays the locality of the AP. The locations are given numbers if no location has been entered. You can enter another locality.

Field	Description
Name	Displays the name of the AP. You can change the name.
Description	Enter a unique description for the AP.
CAPWAP Encryption	<p>Select whether communication between the master and slaves is to be encrypted.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>You can override the encryption in order to view the communication for debugging purposes.</p>

Fields in the Wireless module1 or in the Wireless module 2 menu.

Field	Description
Operation Mode	<p>Displays the mode in which the wireless module is to be operated. You can change the mode.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>On</i> (default value): The wireless module is used as an access point in your network.• <i>Off</i>: The wireless module is not active.
Active Radio Profile	<p>Displays the wireless module profile that is currently selected. You can select another wireless module profile from the list if more than one wireless module profile are being set up.</p>
Channel	<p>Displays the channel that is assigned. You can select another channel.</p> <p>The number of channels you can select depends on the country setting. Please consult the data sheet for your device.</p> <p>Access Point mode</p> <p>Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to</p>

Field	Description
	<p>different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels.</p> <p>In the case of manual channel selection, please make sure first that the APs actually support these channels.</p> <p>Possible values (according to the selected wireless module profile):</p> <ul style="list-style-type: none">• For Active Radio Profile = 2.4 GHz Radio Profile Possible values are <i>1</i> to <i>13</i> and <i>Auto</i> (default value).• For Active Radio Profile = 5 GHz Radio Profile Possible values are <i>36</i>, <i>40</i>, <i>44</i>, <i>48</i> and <i>Auto</i> (default value)
Used Channel	<p>Only for managed APs.</p> <p>Displays the channel that is currently in use.</p>
Transmit Power	<p>Displays the transmission power. You can select another transmission power.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Max.</i> (default value): The maximum antenna power is used.• <i>5 dBm</i>• <i>8 dBm</i>• <i>11 dBm</i>• <i>14 dBm</i>• <i>16 dBm</i>• <i>17 dBm</i>
Assigned Wireless Network (VSS)	<p>Displays the wireless networks that are currently assigned.</p>

13.3.2 Radio Profiles



Fig. 73: Wireless LAN Controller->Slave AP configuration->Radio Profiles

An overview of all created wireless module profiles is displayed in the **Wireless LAN Controller->Slave AP configuration->Radio Profiles** menu. A profile with 2.4 GHz and a profile with 5 GHz are created by default; the 2.4 GHz profile cannot be deleted.

For each wireless module profile you will see an entry with a parameter set (**Radio Profiles, Configured Radio Modules, Operation Band, Wireless Mode**).

13.3.2.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button in order to create new wireless module profiles.

Slave Access Points

Radio Profiles

Wireless Networks (VSS)

Radio Profile Definition

Description

Operation Mode

Operation Band

Number of Spatial Streams

Performance Settings

Wireless Mode

Max. Transmission Rate

Burst Mode

Airtime fairness

Advanced Settings

Channel Plan

Beacon Period

DTIM Period

RTS Threshold

Short Guard Interval

Short Retry Limit

Long Retry Limit

Fragmentation Threshold

Cyclic Background Scanning

OK

Cancel

Fig. 74: Wireless LAN Controller->Slave AP configuration->Radio Profiles-> / New

The **Wireless LAN Controller->Slave AP configuration->Radio Profiles-> / New** menu consists of the following fields:

Fields in the menu Radio Profile Definition

Field	Description
Description	Enter the desired description of the wireless module profile.
Operation Mode	<div>Define the mode in which the wireless module profile is to be operated.</div> <div>Possible values:</div> <ul style="list-style-type: none">• <i>Off</i> (default value): The wireless module profile is not active.• <i>Access Point</i>: Your device is used as an access point in

Field	Description
	your network.
Operation Band	<p>Select the frequency band of the wireless module profile.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>2.4 GHz In/Outdoor</i> (default value): Your device is operated at 2.4 GHz (mode 802.11b, mode 802.11g and mode 802.11n), inside or outside buildings.• <i>5 GHz Indoor</i>: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside buildings.• <i>5 GHz Outdoor</i>: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) outside buildings.• <i>5 GHz In/Outdoor</i>: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside or outside buildings.• <i>5.8 GHz Outdoor</i>: Only for so-called Broadband Fixed Wireless Access (BFWA) applications. The frequencies in the frequency range from 5755 MHz to 5875 MHz may only be used in conjunction with commercial offers for public network accesses and requires registration with the Federal Network Agency.
Bandwidth	<p>Not for Operation Band = <i>2.4 GHz In/Outdoor</i></p> <p>Select how many channels are to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>20 MHz</i> (default value): One channel with 20 MHz bandwidth is used.• <i>40 MHz</i>: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channel and the other as an expansion channel.
Number of Spatial Streams	<p>Select how many traffic flows are to be used in parallel.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>3</i>: Three traffic flows are used.• <i>2</i>: Two traffic flows are used.• <i>1</i>: One traffic flow is used.

Fields in the menu Performance Settings


Field	Description
Wireless Mode	<p>Select the wireless technology that the access point is to use.</p> <p>For Operation Band = <i>2.4 GHz In/Outdoor</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>802.11g</i>: The device operates only in accordance with 802.11g. 802.11b clients have no access.• <i>802.11b</i>: Your device operates only in accordance with 802.11b and forces all clients to adapt to it.• <i>802.11 mixed (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g.• <i>802.11 mixed long (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur.• <i>802.11 mixed short (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates).• <i>802.11b/g/n</i>: Your device operates according to either 802.11b, 802.11g or 802.11n.• <i>802.11g/n</i>: Your device operates according to either 802.11g or 802.11n.• <i>802.11n</i>: Your device operates only according to 802.11n. <p>For Operation Band = <i>5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor or 5.8 GHz Outdoor</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>802.11a</i>: The device operates only in accordance with 802.11a.• <i>802.11n</i>: Your device operates only according to 802.11n.• <i>802.11a/n</i>: Your device operates according to either 802.11a or 802.11n.

Field	Description
Max. Transmission Rate	<p>Select the transmission speed.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Auto</i> (default value): The transmission speed is determined automatically.• <i><Value></i>: According to setting for Operation Band, Bandwidth, Number of Spatial Streams and Wireless Mode various fixed values in mbps are available.
Burst Mode	<p>Activate this function to increase the transmission speed for 802.11g through frame bursting. As a result, several packets are sent one after the other without a waiting period. This is particularly effective in 11b/g mixed operation.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If problems occur with older WLAN hardware, this function should not be active.</p>
Airtime fairness	<p>This function is not available for all devices.</p> <p>The Airtime fairness function ensures that the access point's send resources are distributed intelligently to the connected clients. This means that a powerful client (e. g. a 802.11n client) cannot achieve only a poor flow level, because a less powerful client (e. g. a 802.11a client) is treated in the same way when apportioning.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>This fuction is only applied to unprioritized frames of the WMM Classe "Background".</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Advanced Settings

Field	Description
Channel Plan	<p>Select the desired channel plan.</p> <p>The channel plan makes a preselection when a channel is se-</p>

Field	Description
	<p>lected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>All</i>: All channels can be dialled when a channel is selected.• <i>Auto</i>: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided.• <i>User defined</i>: You can select the desired channels yourself.
User Defined Channel Plan	<p>Only for Channel Plan = <i>User defined</i></p> <p>The currently selected channels are displayed here.</p> <p>With Add you can add channels. If all available channels are displayed, you cannot add any more entries.</p> <p>You can also delete entries using the  icon.</p>
Beacon Period	<p>Enter the time in milliseconds between the sending of two beacons.</p> <p>This value is transmitted in Beacon and Probe Response Frames.</p> <p>Possible values are <i>1</i> to <i>65535</i>.</p> <p>The default value is <i>100</i>.</p>
DTIM Period	<p>Enter the interval for the Delivery Traffic Indication Message (DTIM).</p> <p>The DTIM field is a data field in transmitted beacons that informs clients about the window to the next broadcast or multicast transmission. If clients operate in power save mode, they come alive at the right time and receive the data.</p> <p>Possible values are <i>1</i> to <i>255</i>.</p> <p>The default value is <i>2</i>.</p>

Field	Description
RTS Threshold	<p>Here you can specify the data packet length threshold in bytes (1..2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point.</p>
Short Guard Interval	<p>Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.</p>
Short Retry Limit	<p>Enter the maximum number of attempts to send a frame with length less than or equal to the value defined in RTS Threshold. After this many failed attempts, the packet is discarded.</p> <p>Possible values are 1 to 255.</p> <p>The default value is 7.</p>
Long Retry Limit	<p>Enter the maximum number of attempts to send a data packet of length greater than the value defined in RTS Threshold. After this many failed attempts, the packet is discarded.</p> <p>Possible values are 1 to 255.</p> <p>The default value is 4.</p>
Fragmentation Threshold	<p>Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). Low values are recommended for this field in areas with poor reception and in the event of radio interference.</p> <p>Possible values are 256 to 2346.</p> <p>The default value is 2346.</p>
Cyclic Background Scanning	<p>Not all devices support this function.</p> <p>You can enable the Cyclic Background Scanning function so that a search is run at regular intervals for neighbouring or rogue access points in the network. This search is run without negatively impacting the function as an access point.</p> <p>Enable or disable the function Cyclic Background Scanning.</p>

Field	Description
	The function is enabled with <i>Enabled</i> .
	The function is not activated by default.

13.3.3 Wireless Networks (VSS)

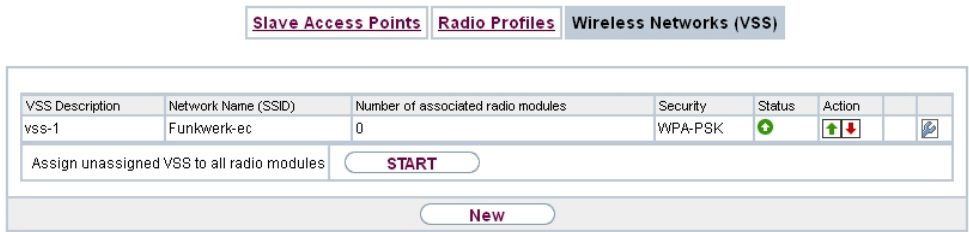



Fig. 75: Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)

An overview of all created wireless networks is displayed in the **Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)** menu. A wireless network is created by default.

For every wireless network (VSS), you see an entry with a parameter set (**VSS Description**, **Network Name (SSID)**, **Number of associated radio modules**, **Security**, **Status**, **Action**).

Under **Assign unassigned VSS to all radio modules** click on the **Start** button to assign a newly-created VSS to all wireless modules.

13.3.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure additional wireless networks.

Slave Access PointsRadio ProfilesWireless Networks (VSS)

Service Set Parameters

Network Name (SSID)

Visible

Intra-cell Repeating

Enabled

ARP Processing

Enabled

WMM

Enabled

Security Settings

Security Mode

Inactive

Client load balancing

Max. number of clients - hard limit

32

Max. number of clients - soft limit

28

Client Band select

Disabled - optimized for fast roaming

MAC-Filter

Access Control

Enabled

Dynamic blacklisting

Enabled

Failed attempts per Time

10

/ 60

Seconds

Blacklist blocktime

500

Seconds

VLAN

VLAN

Enabled

OK

Cancel

Fig. 76: Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)->New

The Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)->New menu consists of the following fields:

Fields in the menu Service Set Parameters

Field	Description
Network Name (SSID)	<p>Enter the name of the wireless network (SSID).</p> <p>Enter an ASCII string with a maximum of 32 characters.</p> <p>Also select whether the Network Name (SSID) is to be transmitted.</p> <p>The network name is displayed by selecting <i>Visible</i>.</p> <p>It is visible by default.</p>
Intra-cell Repeating	<p>Select whether communication between the WLAN clients is to be permitted within a radio cell.</p>

Field	Description
	<p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
ARP Processing	<p>Select whether the ARP processing function should be enabled. The ARP data traffic is reduced in the network by the fact that ARP broadcasts that have been converted to ARP unicasts are forwarded to IP addresses that are known internally. Unicasts are quicker and clients with an enabled power save function are not addressed.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Make sure that ARP processing cannot be applied together with the MAC bridge function.</p>
WMM	<p>Select whether voice or video prioritisation via WMM (Wireless Multimedia) is to be activated for the wireless network so that optimum transmission quality is always achieved for time-critical applications. Data prioritisation is supported in accordance with DSCP (Differentiated Services Code Point) or IEEE802.1d.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the menu Security Settings

Field	Description
Security Mode	<p>Select the security mode (encryption and authentication) for the wireless network.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Inactive</i> (default value): Neither encryption nor authentication• <i>WEP 40</i>: WEP 40 bits• <i>WEP 104</i>: WEP 104 bits• <i>WPA-PSK</i>: WPA Preshared Key• <i>WPA Enterprise</i>: 802.11x

Field	Description
Transmit Key	<p>Only for Security Mode = <i>WEP 40</i> or <i>WEP 104</i></p> <p>Select one of the keys configured in WEP Key as a standard key.</p> <p>The default value is <i>Key 1</i>.</p>
WEP Key 1-4	<p>Only for Security Mode = <i>WEP 40</i>, <i>WEP 104</i></p> <p>Enter the WEP key.</p> <p>Enter a character string with the right number of characters for the selected WEP mode. For <i>WEP 40</i> you need a character string with 5 characters, for <i>WEP 104</i> with 13 characters, e. g. <i>hello</i> for <i>WEP 40</i>, <i>wep1</i> for <i>WEP 104</i>.</p>
WPA Mode	<p>Only for Security Mode = <i>WPA-PSK</i> and <i>WPA Enterprise</i></p> <p>Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>WPA and WPA 2</i> (default value): WPA and WPA 2 can be used.• <i>WPA</i>: Only WPA is used.• <i>WPA 2</i>: Only WPA2 is used.
WPA Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for WPA Mode = <i>WPA</i> and <i>WPA and WPA 2</i></p> <p>Select the type of encryption you want to apply to WPA.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>TKIP</i> (default value): TKIP is used.• <i>AES</i>: AES is used.• <i>AES and TKIP</i>: AES or TKIP is used.
WPA2 Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for WPA Mode = <i>WPA 2</i> and <i>WPA and WPA 2</i></p> <p>Select the type of encryption you want to apply to WPA2.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>AES</i> (default value): AES is used.• <i>TKIP</i>: TKIP is used.• <i>AES and TKIP</i>: AES or TKIP is used.
Preshared Key	<p>Only for Security Mode = <i>WPA-PSK</i></p> <p>Enter the WPA password.</p> <p>Enter an ASCII string with 8 - 63 characters.</p> <p>Note: Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!</p>
Radius Server	<p>You can control access to a wireless network via a RADIUS server.</p> <p>With Add, you can create new entries. Enter the IP address and the password of the RADIUS server.</p>
EAP Preauthentication	<p>Only for Security Mode = <i>WPA Enterprise</i></p> <p>Select whether the EAP preauthentication function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	<p>Enter the maximum number of clients that can be connected to this wireless network (SSID)</p> <p>The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This maximum is distributed across all wireless</p>

Field	Description
	<p>networks configured for this radio module. No more new wireless networks can be created and a warning message will appear if the maximum number of clients is reached.</p> <p>Possible values are whole numbers between <i>1</i> and <i>254</i>.</p> <p>The default value is <i>32</i>.</p>
Max. number of clients - soft limit	<p>Not all devices support this function.</p> <p>To avoid a radio module being fully utilised, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the Max. number of clients - hard limit is reached.</p> <p>The value of the Max. number of clients - soft limit must be the same as or less than that of the Max. number of clients - hard limit.</p> <p>The default value is <i>28</i>.</p> <p>You can disable this function if you set Max. number of clients - soft limit and Max. number of clients - hard limit to identical values.</p>
Client Band select	<p>Not all devices support this function.</p> <p>This function requires a dual radio setup where the same wireless network is configured on both radio modules, but in different frequency bands.</p> <p>The Client Band select option enables clients to be moved from the frequency band originally selected to a less busy one, providing the client supports this. To achieve a changeover, the connection attempt of a client is initially refused so that the client repeats the attempt in a different frequency band.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Disabled - optimized for fast roaming</i> (default value): The function is not used for this VSS. This is useful if clients are to switch between different radio cells with as little

Field	Description
	<p>delay as possible, e. g. with Voice over WLAN.</p> <ul style="list-style-type: none">• <i>2,4 GHz band preferred</i>: Preference is given to accepting clients in the 2.4 GHz band.• <i>5 GHz band preferred</i>: Preference is given to accepting clients in the 5 GHz band.

Fields in the menu MAC-Filter

Field	Description
Access Control	<p>Select whether only certain clients are to be permitted for this wireless network.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Allowed Addresses	<p>Use Add to make entries and enter the MAC addresses (MAC Address) of the clients to be permitted.</p>
Dynamic blacklisting	<p>You can use the Dynamic blacklisting function to identify clients that want to gain possibly unauthorised access to the network and block them for a certain length of time. A client is blocked if the number of unsuccessful login attempts with a specified time exceeds a certain number. This threshold value and the duration of the block can be configured. A blocked client is blocked at all the APs that are managed by the wireless LAN controller for the VSS concerned, so neither are they able to log into a different radio cell in that VSS. If a client needs to be blocked permanently, this can be done in the Wireless LAN Controller->Monitoring->Rogue Clients menu.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is activated by default.</p>
Failed attempts per Time	<p>Enter the number of failed attempts that have to originate from a specific MAC address during a certain time for a blacklist entry to be created.</p> <p>Default values are <i>10</i> failed attempts during <i>60</i> seconds.</p>
Blacklist blocktime	<p>Enter the time for which an entry in the dynamic blacklist remains valid.</p>

Field	Description
	Default value is <i>500</i> seconds.

Fields in the menu VLAN

Field	Description
VLAN	Select whether the VLAN segmentation is to be used for this wireless network. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
VLAN ID	Enter the number that identifies the VLAN. Possible values are <i>2</i> to <i>4094</i> . VLAN ID <i>1</i> is not possible as it is already in use.

13.4 Monitoring

This menu is used to monitor your WLAN infrastructure.

13.4.1 Active Clients

Active Clients

Wireless Networks (VSS)

Client Management

Neighbor APs

Rogue APs

Rogue Clients

Automatic Refresh Interval: 60 Seconds

Apply

View: 20 per page << >> Filter in: None equal

Go

Location	Slave AP Name	VSS	Client MAC	Client IP Address	Signal : Noise (dBm)	Status	Uptime
Page: 1							

Fig. 77: Wireless LAN Controller->Monitoring->Active Clients

In the **Wireless LAN Controller->Monitoring->Active Clients** menu, current values of all active clients are displayed.

For each client you will see an entry with the following parameter set: **Location, Name, VSS, Client MAC, Client IP Address, Signal : Noise (dBm) , Status, Uptime.**

Possible values for Status

Status	Meaning
None	The client is no longer in a valid status.
Logon	The client is currently logging on with the WLAN.
Associated	The client is logged on with the WLAN.
Authenticate	The client is in the process of being authenticated.
Authenticated	The client is authenticated.

13.4.2 Wireless Networks (VSS)

Active Clients

Wireless Networks (VSS)

Client Management

Neighbor APs

Rogue APs

Rogue Clients

View20per page<>Filter inNoneequalGo

Location	Slave AP Name	VSS	MAC Address (VSS)	Channel	Status
Page: 1					

Fig. 78: Wireless LAN Controller->Monitoring->Wireless Networks (VSS)

In menu **Wireless LAN Controller->Monitoring->Wireless Networks (VSS)** an overview of the currently used AP is displayed. You see which wireless module is assigned to which wireless network. For each wireless a parameter set is displayed (**Location**, **Slave AP Name**, **VSS**, **MAC Address (VSS)**, **Channel**, **Status**).

13.4.3 Client Management

Active Clients

Wireless Networks (VSS)

Client Management

Neighbor APs

Rogue APs

Rogue Clients


View20per page<>Filter inNoneequalGo

Location	Slave AP Name	VSS	MAC Address (VSS)	Active Clients	2,4/5 GHz changeover	Denied Clients soft/hard
Page: 1						

Apply

Fig. 79: Wireless LAN Controller->Monitoring->Client Management

The **Wireless LAN Controller->Monitoring->Client Management** menu displays an overview of the **Client Management**. For each VSS you can see such information as the number of clients connected, the number of clients that are affected by the **2,4/5 GHz changeover**, and the number of rejected clients.

You can delete the values of an entry using the  symbol.

13.4.4 Neighbor APs

Active Clients

Wireless Networks (VSS)

Client Management

Neighbor APs

Rogue APs

Rogue Clients

View 20 per page<<>>Filter in NoneequalGo

SSID

MAC Address

Signal dBm

Channel

Security

Last seen

Strongest signal received by

Total detections

Page: 1

Actions

New Neighborscan

START

Fig. 80: Wireless LAN Controller->Monitoring->Neighbor APs

In the **Wireless LAN Controller->Monitoring->Neighbor APs** menu, the adjacent AP's found during the scan are displayed. **Rogue APs**, i.e. APs which are not managed by the WLAN controller but are using an SSID managed by the WLAN controller are highlighted in red.



Note

Check the rogue APs shown carefully, as an attacker could attempt to spy on data in your network using a rogue AP.

Although each AP is found more than once, it is only displayed once with the strongest signal. You see the following parameters for each AP: **SSID**, **MAC Address**, **Signal dBm**, **Channel**, **Security**, **Last seen**, **Strongest signal received by** , **Total detections**.

The entries are displayed in alphabetical order by **SSID**. **Security** shows the security settings of the AP. Under **Strongest signal received by** , you will see the parameters **Location** and **Name** of the APs in which the displayed AP was found. **Total detections** shows how often the corresponding AP was found during the scan.

Click under **New Neighborscan** on **Start**, to rescan adjacent AP's. You will receive a warning that the wireless modules of the access points must also be disabled for a certain period of time. When you start the process with **OK**, a progress bar is displayed. The located AP display is updated every ten seconds.

13.4.5 Rogue APs

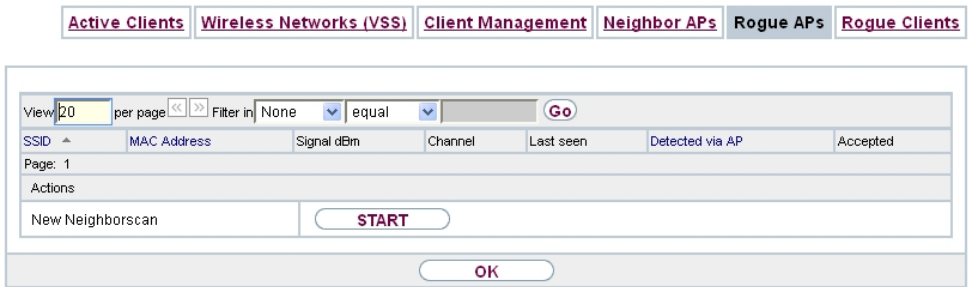


Fig. 81: Wireless LAN Controller->Monitoring->Rogue APs

APs which are using an SSID from their own network but are not managed by **Wireless LAN Controller** are displayed in the **Wireless LAN Controller->Monitoring->Rogue APs** menu. **Rogue APs** which have been found for the first time are displayed with a red background.

For each rogue AP you will see an entry with the following parameter set: **SSID, MAC Address, Signal dBm, Channel, Last seen, Detected via AP, Accepted.**



Note

Check the rogue APs shown carefully, as an attacker could attempt to spy on data in your network using a rogue AP.

You can class a rogue AP as trustworthy by enabling the **Accepted** checkbox. If an alarm has been configured, this is then removed and no longer sent. The red background disappears.

Click under **New Neighborscan** on **Start**, to rescan adjacent AP's. You will receive a warning that the wireless modules of the access points must also be disabled for a certain period of time. When you start the process with **OK**, a progress bar is displayed. The located AP display is updated every ten seconds.

13.4.6 Rogue Clients

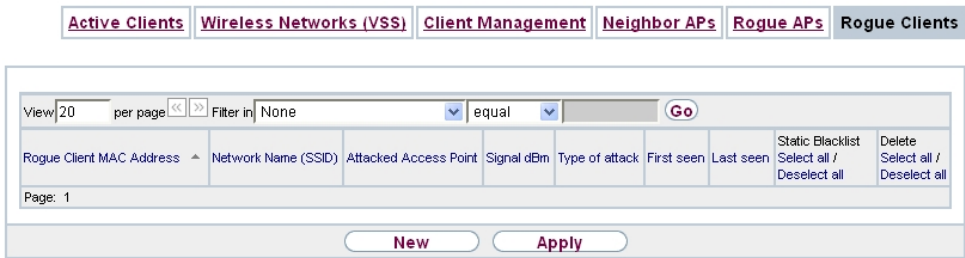



Fig. 82: Wireless LAN Controller->Monitoring->Rogue Clients

The **Wireless LAN Controller->Monitoring->Rogue Clients** menu displays the clients which have attempted to gain unauthorised access to the network and which are therefore on the blacklist. The blacklist is configured for each VSS in the **Wireless LAN Controller->Slave AP configuration->Wireless Networks (VSS)** menu. You can also add a new entry to the static blacklist.

Possible values for Rogue Clients

Status	Meaning
Rogue Client MAC Address	Displays the MAC address of the client on the blacklist.
SSID	Displays the SSID involved.
Attacked Access Point	Displays the AP concerned.
Signal dBm	Displays the signal strength of the client during the attempted access.
Type of attack	This displays the type of potential attack, e. g. an incorrect authentication.
First seen	Displays the time of the first registered attempted access.
Last seen	Displays the time of the last registered attempted access.
Static Blacklist	You can categorise a rogue client as untrustworthy by selecting the checkbox in the Static Blacklist column. The block on the client does not then end automatically, rather you need to lift it manually.
Delete	You can delete entries with the  symbol.

13.4.6.1 New

Choose the **New** button to configure additional blacklist entries.

Active Clients

Wireless Networks (VSS)

Client Management

Neighbor APs

Rogue APs

Rogue Clients

New Blacklist Entry

Rogue Client MAC Address

Network Name (SSID)

Select one ▾

OK

Cancel

Fig. 83: Wireless LAN Controller->Monitoring->Rogue Clients->New

The menu consists of the following fields:

Fields in the New Blacklist Entry menu.

Field	Description
Rogue Client MAC Address	Enter the MAC address of the client you intend to include in the static blacklist.
Network Name (SSID)	Pick the wireless network you want to exclude the rogue client from.

13.5 Maintenance

This menu is used for the maintenance of your managed APs.

13.5.1 Firmware Maintenance

Firmware Maintenance

Managed Access Points

Update firmware
Select all /
Deselect all

Location ▴

Device

IP Address

LAN MAC Address

Firmware Version

Status

Action

Update system software ▾

Source Location

HTTP server ▾

URL

OK

Cancel

Fig. 84: Wireless LAN Controller->Maintenance->Firmware Maintenance

In the **Wireless LAN Controller->Maintenance->Firmware Maintenance** menu, a list of

all **Managed Access Points** is displayed.

For each managed AP you will see an entry with the following parameter set: **Update firmware**, **Location**, **Device**, **IP Address**, **LAN MAC Address**, **Firmware Version** , **Status**.

Click the **Select all** button to select all of the entries for a firmware update. Click the **Deselect all** button to disable all entries and to then select individual entries if required (e.g. if there is a large number of entries and only individual APs are to be given software updates).

Possible values for Status

Status	Meaning
Image already exists.	The software image already exists; no update is required.
Error	An error has occurred.
Running	The operation is currently in progress.
Done	The update is complete.

The **Wireless LAN Controller->Maintenance->Firmware Maintenance** menu consists of the following fields:

Fields in the Firmware Maintenance menu.

Field	Description
Action	<p>Select the action you wish to execute.</p> <p>After each task, a window is displayed showing the other steps that are required.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Update system software</i>: You can also start an update of the system software.• <i>Save configuration with state information</i>: You can save a configuration which contains the AP status information.
Source Location	<p>Select the source for the action.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>HTTP server</i> (default value): The file is stored respectively on a remote server specified in the URL.• <i>Current Software from Update Server</i>: The file is on the official update server. (Only for Action= Update system software)

Field	Description
	<ul style="list-style-type: none">• <i>TFTP server</i>: The file is stored respectively on a TFTP server specified in the URL.
URL	Only for Source Location = <i>HTTP server</i> or <i>TFTP server</i> Enter the URL of the update server from which the system software file is loaded or on which the configuration file is saved.

Chapter 14 Networking

14.1 Routes


Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. If you set up access to the Internet, you must configure the route to your Internet Service Provider (ISP) as a default route. If, for example, you configure a corporate network connection, only enter the route to the head office or branch office as a default route if you do not configure Internet access over your device. If, for example, you configure both Internet access and a corporate network connection, enter a default route to the ISP and a network route to the head office. You can enter several default routes on your device, but only one default route can be active at any one time. If you enter several default routes, you should thus note differing values for **Metric**.

14.1.1 IPv4 Route Configuration

A list of all configured routes is displayed in the **Network->Routes->IPv4 Route Configuration** menu.

14.1.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional routes.

IPv4 Route Configuration

IPv4 Routing Table

Options

Basic Parameters

Route Type

Network Route via Interface

Interface

None

Route Class

☒ Standard ☐ Extended

Route Parameters

Destination IP Address/Netmask

Local IP Address

0.0.0.0

Metric

1

OK

Cancel

Fig. 85: Network->Routes->IPv4 Route Configuration->New with **Extended Route = Standard**.

If the *Extended* option is selected for the **Route Class**, an extra configuration section opens.

IPv4 Route Configuration

IPv4 Routing Table

Options

Basic Parameters

Route Type

Network Route via Interface

Interface

None

Route Class

☐ Standard ☒ Extended

Route Parameters

Destination IP Address/Netmask

Local IP Address

0.0.0.0

Metric

1

Extended Route Parameters

Description

Source Interface

Any

Source IP Address/Netmask

0.0.0.0 / 0.0.0.0

Layer 4 Protocol

Any

Source Port

Any

 Port to Port

Destination Port

Any

 Port to Port

DSCP / TOS Value

Ignore

Mode

Dialup and wait

OK

Cancel


Fig. 86: Network->Routes->IPv4 Route Configuration->New with **Extended = Enabled**

The **Network->Routes->IPv4 Route Configuration->New** menu consists of the following

fields:

Fields in the menu Basic Parameters

Field	Description
Route Type	<p>Select the type of route.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Default Route via Interface</i>: Route via a specific interface which is to be used if no other suitable route is available.• <i>Default Route via Gateway</i>: Route via a specific gateway which is to be used if no other suitable route is available.• <i>Host Route via Interface</i>: Route to an individual host via a specific interface.• <i>Host Route via Gateway</i>: Route to an individual host via a specific gateway.• <i>Network Route via Interface</i> (default value): Route to a network via a specific interface.• <i>Network Route via Gateway</i>: Route to a network via a specific gateway. <p>Only for interfaces that are operated in DHCP client mode:</p> <p>Even if an interface is configured for DHCP client mode, routes can still be configured for data traffic via that interface. The settings received from the DHCP server are then copied, along with those configured here, to the active routing table. This enables, e. g., in the case of dynamically changing gateway addresses, particular routes to be maintained, or routes with different metrics (i. e. of differing priority) to be specified. However, if the DHCP server sends static routes, the settings configured here are not copied to the routing.</p> <ul style="list-style-type: none">• <i>Default Route Template per DHCP</i>: The routing information is taken entirely from the DHCP server. Only advanced parameters can be additionally configured. This route remains unchanged by other routes created for this interface and is copied to the routing table in parallel with them.• <i>Host Route Template per DHCP</i>: The settings received by DHCP are supplemented by routing information about a particular host.• <i>Network Route Template per DHCP</i>: The settings re-

Field	Description
	ceived by DHCP are supplemented by routing information about a particular network.
	<div>Note<p>When the DHCP lease expires or when the device is re-started, the routes that consist from the combination of DHCP settings and those made here are initially deleted once more from the active routing. If the DHCP is reconfigured they are re-generated and re-activated.</p></div>
Interface	Select the interface to be used for this route.
Route Class	<p>Select the type of Route Class.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Standard</i>: Defines a route with the default parameters.• <i>Extended</i>: Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface.

Fields in the menu Route Parameters

Field	Description
Local IP Address	<p>Only for Route Type = <i>Default Route via Interface</i>, <i>Host Route via Interface</i> or <i>Network Route via Interface</i></p> <p>Enter the IP address of the host to which your device is to forward the IP packets.</p>
Destination IP Address/Netmask	<p>Only for Route Type <i>Host Route via Interface</i> or <i>Network Route via Interface</i></p> <p>Enter the IP address of the destination host or destination network.</p>

Field	Description
	When Route Type = <i>Network Route via Interface</i> Also enter the relevant netmask in the second field.
Gateway IP Address	Only for Route Type = <i>Default Route via Gateway, Host Route via Gateway</i> or <i>Network Route via Gateway</i> Enter the IP address of the gateway to which your device is to forward the IP packets.
Metric	Select the priority of the route. The lower the value, the higher the priority of the route. Value range from 0 to 15. The default value is 1.

Fields in the menu **Extended Route Parameters**

Field	Description
Description	Enter a description for the IP route.
Source Interface	Select the interface over which the data packets are to reach the device. The default value is <i>None</i> .
Source IP Address/ Netmask	Enter the IP address and netmask of the source host or source network.
Layer 4 Protocol	Select a protocol. Possible values: <i>ICMP, IGMP, TCP, UDP, GRE, ESP, AH, OSPF, PIM, L2TP, Any</i> . The default value is <i>Any</i> .
Source Port	Only for Layer 4 Protocol = <i>TCP</i> or <i>UDP</i> Enter the source port. First select the port number range. Possible values: <ul style="list-style-type: none">• <i>Any</i> (default value): The route is valid for all port numbers.

Field	Description
	<ul style="list-style-type: none"> • <i>Single</i>: Enables the entry of a port number. • <i>Range</i>: Enables the entry of a range of port numbers. • <i>Privileged</i>: Entry of privileged port numbers: 0 ... 1023. • <i>Server</i>: Entry of server port numbers: 5000 ... 32767. • <i>Clients 1</i>: Entry of client port numbers: 1024 ... 4999. • <i>Clients 2</i>: Entry of client port numbers: 32768 ... 65535. • <i>Not privileged</i>: Entry of unprivileged port numbers: 1024 ... 65535. <p>Enter the appropriate values for the individual port or start port of a range in Port and, for a range, the end port in to Port.</p>
Destination Port	<p>Only for Layer 4 Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter the destination port.</p> <p>First select the port number range.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Any</i> (default value): The route is valid for all port numbers. • <i>Single</i>: Enables the entry of a port number. • <i>Range</i>: Enables the entry of a range of port numbers. • <i>Privileged</i>: Entry of privileged port numbers: 0 ... 1023. • <i>Server</i>: Entry of server port numbers: 5000 ... 32767. • <i>Clients 1</i>: Entry of client port numbers: 1024 ... 4999. • <i>Clients 2</i>: Entry of client port numbers: 32768 ... 65535. • <i>Not privileged</i>: Entry of unprivileged port numbers: 1024 ... 65535. <p>Enter the appropriate values for the individual port or start port of a range in Port and, for a range, the end port in to Port.</p>
DSCP / TOS Value	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ignore</i> (default value): The type of service is ignored. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format).

Field	Description
	<ul style="list-style-type: none">• <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).• <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format).• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F. <p>Enter the relevant value for <i>DSCP Binary Value</i>, <i>DSCP Decimal Value</i>, <i>DSCP Hexadecimal Value</i>, <i>TOS Binary Value</i>, <i>TOS Decimal Value</i> and <i>TOS Hexadecimal Value</i>.</p>
Mode	<p>Select when the interface defined in Route Parameters -> Interface is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Dialup and wait</i> (default value): The route can be used if the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up".• <i>Authoritative</i>: The route can always be used.• <i>Dialup and continue</i>: The route can be used when the interface is "up". If the interface is "dormant", then select and use the alternative route (rerouting) until the interface is "up".• <i>Never dialup</i>: The route can be used when the interface is "up".• <i>Always dialup</i>: The route can be used when the interface is "up". If the interface is "dormant", then dial and wait until the interface is "up". In this case, an alternative interface with a poorer metric is used for routing until the interface is "up".

14.1.2 IPv4 Routing Table

A list of all IPv4 routes is displayed in the **Network->Routes->IPv4 Routing Table** menu. The routes do not all need to be active, but can be activated at any time by relevant data traffic.

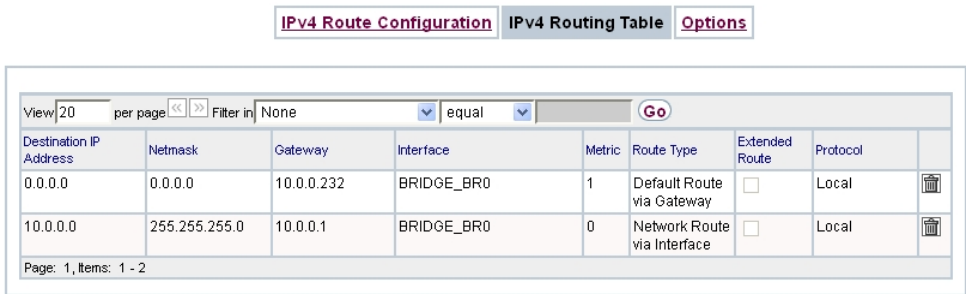


Fig. 87: Network->Routes->IPv4 Routing Table

Fields in the menu IPv4 Routing Table

Field	Description
Destination IP Address	Displays the IP address of the destination host or destination network.
Netmask	Displays the netmask of the destination host or destination network.
Gateway	Displays the gateway IP address. Nothing is displayed here when routes are received by DHCP.
Interface	Displays the interface used for this route.
Metric	Displays the route's priority. The lower the value, the higher the priority of the route
Route Type	Displays the route type.
Extended Route	Displays whether a route has been configured with advanced parameters.
Protocol	Displays how the entry has been created , e.g. manually (<i>Local</i>) or via one of the available protocols.
Delete	You can delete entries with the symbol.

14.1.3 Options

Back Route Verify

The term Back Route Verify describes a very simple but powerful function. If a check is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface. You can therefore prevent the acceptance of packets with false IP addresses - even without using filters.

IPv4 Route Configuration

IPv4 Routing Table

Options

Back Route Verify

Mode

☐ Enable for all interfaces

☒ Enable for specific interfaces

☐ Disable for all interfaces

View20per page<<>>Filter inNoneequalGo

No.	Interface	Back Route Verify
1	br0	<input type="checkbox"/> Enabled

Page: 1, Items: 1 - 1

OK

Cancel

Fig. 88: Networking->Routes->Options

The **Networking->Routes->Options** menu consists of the following fields:

Fields in the Back Route Verify menu.

Field	Description
Mode	<p>Select how the interfaces to be activated for Back Route Verify are to be specified.</p> <p>Possible values:</p> <ul style="list-style-type: none"><i>Enable for all interfaces</i>: Back Route Verify is activated for all interfaces.<i>Enable for specific interfaces</i> (default value): A list of all interfaces is displayed in which Back Route Verify is only enabled for specific interfaces.<i>Disable for all interfaces</i>: Back route verify is disabled for all interfaces.
No.	Only for Mode = <i>Enable for specific interfaces</i>

Field	Description
	Displays the serial number of the list entry.
Interface	Only for Mode = <i>Enable for specific interfaces</i> Displays the name of the interface.
Back Route Verify	Only for Mode = <i>Enable for specific interfaces</i> Select whether <i>Back Route Verify</i> is to be activated for the interface. The function is enabled with <i>Enabled</i> . By default, the function is deactivated for all interfaces.

14.2 NAT

Network Address Translation (NAT) is a function on your device for defined conversion of source and destination addresses of IP packets. If NAT is activated, IP connections are still only allowed by default in one direction, outgoing (forward) (= protective function). Exceptions to the rule can be configured (in [NAT Configuration](#) on page 217).

14.2.1 NAT Interfaces

A list of all NAT interfaces is displayed in the **Networking->NAT->NAT Interfaces** menu.

NAT Interfaces

NAT Configuration

View20per page<<>>Filter inNoneequalGo

Interface	NAT active	Loopback active	Silent Deny	PPTP Passthrough	Portforwardings
LAN_EN1-0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
LAN_EN1-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Page: 1, Items: 1 - 2

OK

Cancel

Fig. 89: **Networking->NAT->NAT Interfaces**

For every NAT interface, the *NAT active*, *Loopback active*, *Silent Deny* and *PPTP Passthrough* can be selected.

In addition, *Portforwardings* displays how many port forwarding rules were configured

for this interface.

Options in the menu NAT Interfaces

Field	Description
NAT active	Select whether NAT is to be activated for the interface. The function is disabled by default.
Loopback active	The NAT loopback function also enables network address translation for connectors whereby NAT is not activated. This is often used in order to interpret queries from the LAN as if they were coming from the WAN. You can use this to test the server services. The function is disabled by default.
Silent Deny	Select whether IP packets are to be silently denied by NAT. If this function is deactivated, the sender of the denied IP packet is informed by means of an appropriate ICMP or TCP RST message. The function is disabled by default.
PPTP Passthrough	Select whether the setup and operation of several simultaneous, outgoing PPTP connections from hosts in the network are also to be permitted if NAT is activated. The function is disabled by default. If PPTP Passthrough is enabled, the device itself cannot be configured as a tunnel endpoint.
Portforwardings	Shows the number of portforwarding rules configured in Networking->NAT->NAT Configuration .

14.2.2 NAT Configuration

In the **Networking->NAT->NAT Configuration** menu you can exclude data from NAT simply and conveniently as well as translate addresses and ports. For outgoing data traffic you can configure various NAT methods, i.e. you can determine how an external host establishes a connection to an internal host.

14.2.2.1 New

Choose the **New** button to set up NAT.

NAT Interfaces

NAT Configuration

Basic Parameters

Description

Interface

Any

Type of traffic

incoming (Destination NAT)

Specify original traffic

Service

User-defined

Protocol

Any

Source IP Address/Netmask

Any

Original Destination IP Address/Netmask

Any

Replacement Values

New Destination IP Address/Netmask

Host

0.0.0.0

OK

Cancel

Fig. 90: Networking->NAT->NAT Configuration->New

The **Networking->NAT->NAT Configuration->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the NAT configuration.
Interface	Select the interface for which NAT is to be configured. Possible values: <ul style="list-style-type: none">Any (default value): NAT is configured for all interfaces.<Interface name>: Select one of the interfaces from the list.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: <ul style="list-style-type: none">incoming (Destination NAT) (default value): The data traffic that comes from outside.outgoing (Source NAT): Outgoing data traffic.

Field	Description
	<ul style="list-style-type: none">• <i>excluding (Without NAT)</i>: Data traffic excluded from NAT.
NAT method	<p>Only for Type of traffic = <i>outgoing (Source NAT)</i></p> <p>Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario in which an "internal" source host has initiated an IP connection to an "external" destination host over the NAT interface, and in which an internally valid source address and internally valid source port are translated to an externally valid source address and an externally valid source port.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>full-cone</i> (UDP only): Any given external host may send IP packets via the external address and the external port to the initiating source address and the initial source port.• <i>restricted-cone</i> (UDP only): Like full-cone NAT; as external host, however, only the initial "external" destination host is allowed.• <i>port-restricted-cone</i> (UDP only): Like restricted-cone NAT; however, exclusively data from the initial destination port are allowed.• <i>symmetric</i> (standard value) any protocol: Outbound, an externally valid source address and an externally valid source port are administratively set. Inbound, only response packets within the existing connection are allowed.

In the **NAT Configuration** -> **Specify original traffic** menu, you can configure for which data traffic NAT is to be used.

Fields in the menu Specify original traffic

Field	Description
Service	<p>Not for Type of traffic = <i>outgoing (Source NAT)</i> and NAT method = <i>full-cone, restricted-cone or port-restricted-cone</i>.</p> <p>Select one of the preconfigured services.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>User-defined</i> (default value)

Field	Description
	<ul style="list-style-type: none">• <i><service name></i>
Action	<p>Only for Type of traffic = <i>excluding (Without NAT)</i></p> <p>Select which data packets are to be excluded by NAT.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Exclude</i> (default value): All the data packets that match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/net-mask, etc.) are excluded by NAT.• <i>Do not exclude</i>: All the data packets that do not match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/net-mask, etc.) are excluded by NAT.
Protocol	<p>Only for certain services.</p> <p>Not for Type of traffic = <i>outgoing (Source NAT)</i> and NAT method = <i>full-cone, restricted-cone</i> or <i>port-restricted-cone</i>. In this case UDP is automatically defined.</p> <p>Select a protocol. According to the selected Service, different protocols are available.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <i>AH</i>• <i>Chaos</i>• <i>EGP</i>• <i>ESP</i>• <i>GGP</i>• <i>GRE</i>• <i>HMP</i>• <i>ICMP</i>• <i>IGMP</i>• <i>IGP</i>• <i>IGRP</i>• <i>IP</i>

Field	Description
	<ul style="list-style-type: none">• <i>IPinIP</i>• <i>IPv6</i>• <i>IPX in IP</i>• <i>ISO-IP</i>• <i>Kryptolan</i>• <i>L2TP</i>• <i>OSPF</i>• <i>PUP</i>• <i>RDP</i>• <i>RSVP</i>• <i>SKIP</i>• <i>TCP</i>• <i>TLSP</i>• <i>UDP</i>• <i>RRP</i>• <i>XNS-IDP</i>
Source IP Address/ Netmask	<p>Only for Type of traffic = <i>incoming (Destination NAT)</i> or <i>excluding (Without NAT)</i></p> <p>Enter the source IP address and corresponding netmask of the original data packets, as the case arises.</p>
Original Destination IP Address/Netmask	<p>Only for Type of traffic = <i>incoming (Destination NAT)</i></p> <p>Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.</p>
Original Destination Port/Range	<p>Only for Type of traffic = <i>incoming (Destination NAT)</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the destination port or the destination port range of the original data packets. The default setting <i>-All-</i> means that the port is not specified.</p>
Original Source IP Ad- dress/Netmask	<p>Only for Type of traffic = <i>outgoing (Source NAT)</i></p> <p>Enter the source IP address and corresponding netmask of the original data packets, as the case arises.</p>

Field	Description
Original Source Port/Range	<p>Only for Type of traffic = <i>outgoing (Source NAT)</i>, NAT method = <i>symmetric</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the source port of the original data packets. The default setting <i>-All-</i> means that the port remains unspecified.</p> <p>If you select <i>Specify port</i> you can specify a single port, if you select <i>Specify port range</i> you can specify a continuous range of ports which will be applied for filtering the outgoing data traffic</p>
Source Port/Range	<p>Only for Type of traffic = <i>excluding (Without NAT)</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the source port or the source port range of the original data packets. The default setting <i>-All-</i> means that the port remains unspecified.</p>
Destination IP Address/Netmask	<p>Only for Type of traffic = <i>excluding (Without NAT)</i> or <i>outgoing (Source NAT)</i> and NAT method = <i>symmetric</i></p> <p>Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.</p>
Destination Port/Range	<p>Only for Type of traffic = <i>outgoing (Source NAT)</i>, NAT method = <i>symmetric</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i> or Type of traffic = <i>excluding (Without NAT)</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Enter the destination port or the destination port range of the original data packets. The default setting <i>-All-</i> means that the port remains unspecified.</p>

In the **NAT Configuration ->Replacement Values** menu you can define, depending on whether you're dealing with inbound or outbound data traffic, new addresses and ports, to which specific addresses and ports from the **NAT Configuration ->Specify original traffic** menu can be translated.

Fields in the menu Replacement Values

Field	Description
New Destination IP Ad-	Only for Type of traffic = <i>incoming (Destination NAT)</i>

Field	Description
dress/Netmask	Enter the destination IP address and corresponding netmask to which the original destination IP address is to be translated.
New Destination Port	<p>Only for Type of traffic = <i>incoming</i> (<i>Destination NAT</i>), Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated.</p> <p>Select <i>Original</i> to leave the original destination port. If you disable <i>Original</i>, an input field appears and you can enter a new destination port.</p> <p><i>Original</i> is active by default.</p>
New Source IP Address/Netmask	<p>Only for Type of traffic = <i>outgoing</i> (<i>Source NAT</i>) and NAT method = <i>symmetric</i></p> <p>Enter the source IP address to which the original source IP address is to be translated, with corresponding netmask, as the case arises.</p>
New Source Port	<p>Only for Type of traffic = <i>outgoing</i> (<i>Source NAT</i>), NAT method = <i>symmetric</i>, Service = <i>user-defined</i> and Protocol = <i>TCP, UDP, TCP/UDP</i></p> <p>Leave the source port as it appears or enter a new source port to which the original source port is to be translated.</p> <p><i>Original</i> leaves the original source port. If you disable <i>Original</i>, an input field appears in which you can enter a new source port. <i>Original</i> is active by default.</p> <p>If you select <i>Specify port range</i> for Original Source Port/Range, you can choose from the following options:</p> <ul style="list-style-type: none">• <i>Use Original Source Port/Range</i>: The range specified for Original Source Port/Range is not changed, all port numbers are retained.• <i>Verwende Port/Bereich beginnend bei</i>: There is an input field for you to specify the port number with which to start the port range that replaces the original port range. The count of ports is retained.


14.3 Load Balancing

The increasing amount of data traffic over the Internet means it is necessary to send data over different interfaces to increase the total bandwidth available. IP load balancing enables the distribution of data traffic within a certain group of interfaces to be controlled.

14.3.1 Load Balancing Groups

If interfaces are combined to form groups, the data traffic within a group is divided according to the following principles:

- In contrast to Multilink PPP-based solutions, load balancing also functions with accounts with different providers.
- Session-based load balancing is achieved.
- Related (dependent) sessions are always routed over the same interface.
- A decision on distribution is only made for outgoing sessions.

A list of all configured load balancing groups is displayed in the **Networking->Load Balancing->Load Balancing Groups** menu. You can click the  icon next to any list entry to go to an overview of the basic parameters that affect this group.



Note

Note that the interfaces that are combined into a load balancing group must have routes with the same metric. If necessary, go to the **Networking->Routes** menu and check the entries there.

14.3.1.1 New

Choose the **New** button to create additional groups.

Load Balancing Groups

Special Session Handling

Basic Parameters

Group Description

Distribution Policy

Session-Round-Robin

Distribution Mode

☒ Always ☐ Only use active interfaces

Interface Selection for Distribution

Interface	Distribution Ratio	Route Selector	Tracking IP Address
<div>Add</div>			

OK

Cancel

Fig. 91: **Networking->Load Balancing->Load Balancing Groups->New**

The menu **Networking->Load Balancing->Load Balancing Groups->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Group Description	Enter the desired description of the interface group.
Distribution Policy	<p>Select the way the data traffic is to be distributed to the interfaces configured for the group.</p> <p>Possible values:</p> <ul style="list-style-type: none"><i>Session-Round-Robin</i> (default value): A newly added session is assigned to one of the group interfaces according to the percentage assignment of sessions to the interfaces. The number of sessions is decisive.<i>Load-dependent Bandwidth</i>: A newly added session is assigned to one of the group interfaces according to the share of the total data rate handled by the interfaces. The current data rate based on the data traffic is decisive in both the send and receive direction.
Consider	<p>Only for Distribution Policy = <i>Load-dependent Bandwidth</i></p> <p>Choose the direction in which the current data rate is to be considered.</p> <p>Options:</p> <ul style="list-style-type: none"><i>Download</i>: Only the data rate in the receive direction is considered.

Field	Description
	<ul style="list-style-type: none">• <i>Upload</i>: Only the data rate in the send direction is considered. <p>By default, the <i>Download</i> and <i>Upload</i> options are disabled.</p>
Distribution Mode	<p>Select the state the interfaces in the group may have if they are to be included in load balancing.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Always</i> (default value): Also includes idle interfaces.• <i>Only use active interfaces</i>: Only interfaces in the up state are included.

In the **Interface** area, you add interfaces that match the current group context and configure these. You can also delete interfaces.

Use **Add** to create more entries.

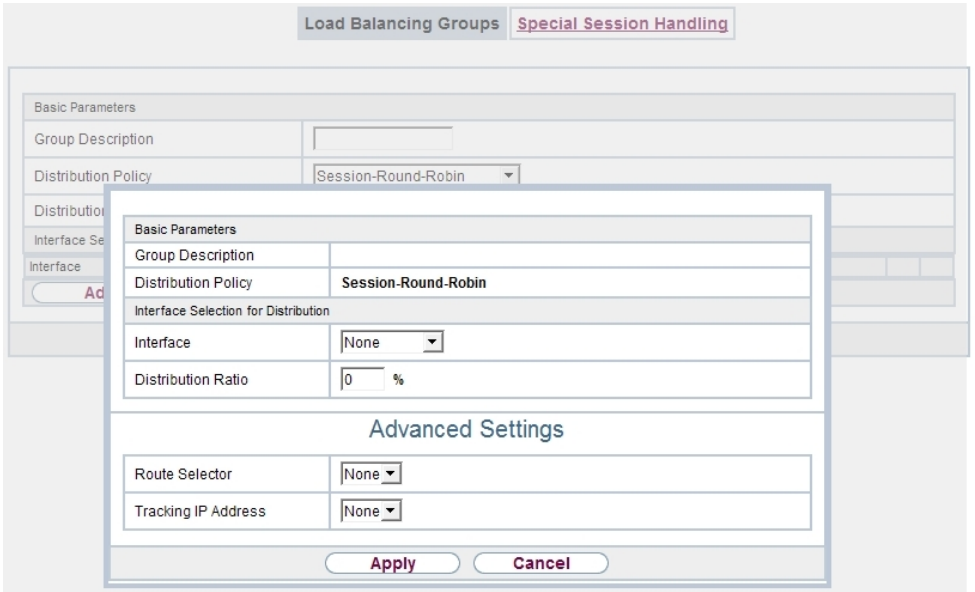


Fig. 92: Networking->Load Balancing->Load Balancing Groups->Add

Fields in the Basic Parameters menu.

Field	Description
Group Description	Shows the description of the interface group.

Field	Description
Distribution Policy	Displays the type of data traffic selected.

Fields in the Interface Selection for Distribution menu.

Field	Description
Interface	Select the interfaces that are to belong to the group from the available interfaces.
Distribution Ratio	<p>Enter the percentage of the data traffic to be assigned to an interface.</p> <p>The meaning differs according to the Distribution Ratio employed:</p> <ul style="list-style-type: none">• For <i>Session-Round-Robin</i> is based on the number of distributed sessions.• For <i>Load-dependent Bandwidth</i>, the data rate is the decisive factor.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Route Selector	<p>The Route Selector parameter is an additional criterion to help define a load balancing group more precisely. Here, routing information is added to the "interface" entry within a load balancing group. The route selector is required in certain scenarios to enable the IP sessions managed by the router to be balanced uniquely for each load balancing group. The following rules apply when using the parameter:</p> <ul style="list-style-type: none">• If an interface is only assigned to one load balancing group, it is not necessary to configure the route selector.• If an interface is assigned to multiple load balancing groups, configuration of the route selector is essential.• The route selector must be configured identically for all interface entries within a load balancing group. <p>Select the Destination IP Address of the desired route.</p>

Field	Description
	You can choose between all routes and all extended routes.
Tracking IP Address	<p>You can use the Tracking IP Address parameter to have a particular route monitored.</p> <p>The load balancing status of the interface and the status of the routes connected to the interface can be influenced using this parameter. This means that routes can be enabled or disabled irrespective of the interface's operation status. The connection is monitored using the gateway's host surveillance function here. Host surveillance entries must be configured in order to use this function. These can be configured in the Local Services->Surveillance->Hosts menu. Here, it is important that only the host surveillance entries with the the action Surveillance are taken into account in the context of load balancing. Links between the load balancing function and the host surveillance function are made through the configuration of the Tracking IP Address in the Load Balancing->Load Balancing Groups->Advanced Settings menu. The interface's load balancing status now varies according to the status of the assigned host surveillance entry.</p> <p>Select the IP address for the route to be monitored.</p> <p>You can choose from the IP addresses you have entered in the Local Services->Surveillance->Hosts->New menu under Monitored IP Address and which are monitored with the aid of the Action to be executed field (Action = <i>Monitor</i>).</p>

14.3.2 Special Session Handling

Special Session Handling enables you to route part of the data traffic to your device via a particular interface. This data traffic is excluded from the **Load Balancing** function.

You can use the **Special Session Handling** function with online banking, for example, to ensure that the HTTPS data traffic is sent to a particular link. Since a check is run in online banking to see whether all the data traffic comes from the same source, data transmission using **Load Balancing** might be terminated at times without **Special Session Handling**.

The **Networking->Load Balancing->Special Session Handling** menu displays a list of entries. If you have not configured any entries, the list is empty.

Every entry contains parameters which describe the properties of a data packet in more or


less detail. The first data packet which the properties configured here match specifies the route for particular subsequent data packets.

Which data packets are subsequently routed via this route is configured in the **Networking->Load Balancing->Special Session Handling->New->Advanced Settings** menu.

If in the **Networking->Load Balancing->Special Session Handling->New** menu, for example, you select the parameter **Service** = *http (SSL)* (and leave the default value for all the other parameters), the first HTTPS packet specifies the **Destination Address** and the **Destination Port** (i. e. Port 443 with HTTPS) for data packets sent subsequently.

If, under **Frozen Parameters** , for the two parameters **Destination Address** and **Destination Port** you leave the default setting *enabled*, the HTTPS packets with the same source IP address as the first HTTPS packet are routed via port 443 to the same **Destination Address** via the same interface as the first HTTPS packet.

14.3.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button create new entries.

Load Balancing Groups

Special Session Handling

Basic Parameters

Admin Status	<input checked="" type="checkbox"/> Enabled
Description	
Service	User-defined
Protocol	dont-verify
Destination IP Address/Netmask	Any
Destination Port/Range	-All- -1 to -1
Source Interface	None
Source IP Address/Netmask	Any
Source Port/Range	-All- -1 to -1
Special Handling Timer	900 Seconds

Advanced Settings

Frozen Parameters	<input checked="" type="checkbox"/> Source IP Address
	<input checked="" type="checkbox"/> Destination Address
	<input checked="" type="checkbox"/> Destination Port

OK

Cancel

Fig. 93: **Networking->Load Balancing->Special Session Handling->New**

The **Networking->Load Balancing->Special Session Handling->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Admin Status	<p>Select whether the Special Session Handling should be activated.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Description	<p>Enter a name for the entry.</p>
Service	<p>Select one of the preconfigured services, if required. The extensive range of services configured ex works includes the following:</p> <ul style="list-style-type: none">• <i>activity</i>• <i>apple-qt</i>• <i>auth</i>• <i>charge</i>• <i>clients_1</i>• <i>daytime</i>• <i>dhcp</i>• <i>discard</i> <p>The default value is <i>User defined</i>.</p>
Protocol	<p>Select a protocol, if required. The <i>Any</i> option (default value) matches any protocol.</p>
Destination IP Address/Netmask	<p>Enter, if required, the destination IP address and netmask of the data packets.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <i>Host</i>: Enter the IP address of the host.• <i>Network</i>: Enter the network address and the related netmask.

Field	Description
Destination Port/Range	<p>Enter, if required, a destination port number or a range of destination port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The destination port is not specified.• <i>Specify port</i>: Enter a destination port.• <i>Specify port range</i>: Enter a destination port range.
Source Interface	<p>If required, select your device's source interface.</p>
Source IP Address/Netmask	<p>Enter, if required, the source IP address and netmask of the data packets.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <i>Host</i>: Enter the IP address of the host.• <i>Network</i>: Enter the network address and the related netmask.
Source Port/Range	<p>Enter, if required, a source port number or a range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The destination port is not specified.• <i>Specify port</i>: Enter a destination port.• <i>Specify port range</i>: Enter a destination port range.
Special Handling Timer	<p>Enter the time period during which the specified data packets are to be routed via the route that has been defined.</p> <p>The default value is <i>900</i> seconds.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Frozen Parameters	<p>Specify whether, when data packets are subsequently sent, the two parameters Destination Address and Destination Port must have the same value as the first data packet, i. e. whether</p>

Field	Description
	<p>the subsequent data packets must be routed via the same Destination Port to the same Destination Address.</p> <p>The two parameters Destination Address and Destination Port are enabled by default.</p> <p>If you leave the default setting <i>Enabled</i> for one or both parameters, the value of the parameter concerned must be the same as in the first data packet with data packets sent subsequently.</p> <p>You can disable one or both parameters if you wish.</p> <p>The Source IP Address parameter must always have the same value in data packets sent subsequently as it did in the first data packet. So it cannot be disabled.</p>

14.4 QoS

QoS (Quality of Service) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them. This is an advantage, especially for time-critical applications such as VoIP.

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data

14.4.1 QoS Filter

In the **Networking->QoS->QoS Filter** menu IP filters are configured.

The list also displays any configured entries from **Networking->Access Rules->Rule Chains**.

14.4.1.1 New

Choose the **New** button to define more IP filters.

QoS Filter

QoS Classification

QoS Interfaces/Policies

Basic Parameters

Description

Service

User-defined

Protocol

Any

Destination IP Address/Netmask

Any

Source IP Address/Netmask

Any

DSCP/TOS Filter (Layer 3)

Ignore

COS Filter (802.1p/Layer 2)

Ignore

OK

Cancel

Fig. 94: **Networking->QoS->QoS Filter->New**

The **Networking->QoS->QoS Filter->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the filter.
Service	<div>Select one of the preconfigured services. The extensive range of services configured ex works includes the following:</div> <div><ul style="list-style-type: none">activityapple-qtauthchargeclients_1daytimedhcpdiscard</div> <div>The default value is <i>User defined</i>.</div>
Protocol	<div>Select a protocol.</div> <div>The <i>Any</i> option (default value) matches any protocol.</div>
Type	Only for Protocol = <i>ICMP</i>

Field	Description
	<p>Select the type.</p> <p>Possible values: <i>Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply.</i></p> <p>See RFC 792.</p> <p>The default value is <i>Any</i>.</p>
Connection State	<p>With Protocol = <i>TCP</i>, you can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.• <i>Any</i> (default value): All TCP packets match the filter.
Destination IP Address/Netmask	<p>Enter the destination IP address of the data packets and the corresponding netmask.</p>
Destination Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a destination port number or a range of destination port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The destination port is not specified.• <i>Specify port</i>: Enter a destination port.• <i>Specify port range</i>: Enter a destination port range.
Source IP Address/Netmask	<p>Enter the source IP address of the data packets and the corresponding netmask.</p>
Source Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a source port number or a range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The destination port is not specified.• <i>Specify port</i>: Enter a destination port.• <i>Specify port range</i>: Enter a destination port range.

Field	Description
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Ignore</i> (default value): The type of service is ignored.• <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit).• <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).• <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format).• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Value range 0 to 7.</p> <p>The default value is 0.</p>

14.4.2 QoS Classification

The data traffic is classified in the **Networking->QoS->QoS Classification** menu, i.e. the data traffic is associated using class IDs of various classes. To do this, create class plans for classifying IP packets based on pre-defined IP filters. Each class plan is associated to at least one interface via its first filter.

14.4.2.1 New

Choose the **New** button to create additional data classes.

QoS Filter

QoS Classification

QoS Interfaces/Policies

Basic Parameters

Class map

New

Description

Filter

Select one

Direction

Outgoing

High Priority Class

☐

Class ID

1

Set DSCP/TOS value (Layer 3)

Preserve

Set COS value (802.1p/Layer 2)

Preserve

Interfaces

Interface

Add

OK


Cancel

Fig. 95: **Networking->QoS->QoS Classification->New**

The **Networking->QoS->QoS Classification->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Class map	<p>Choose the class plan you want to create or edit.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>New</i> (default value): You can create a new class plan with this setting.• <i><Name of class plan></i>: Shows a class plan that has already been created, which you can select and edit. You can add new filters.
Description	<p>Only for Class map = <i>New</i></p> <p>Enter the name of the class plan.</p>
Filter	<p>Select an IP filter.</p> <p>If the class plan is new, select the filter to be set at the first point of the class plan.</p> <p>If the class plan already exists, select the filter to be attached to the class plan.</p>

Field	Description
	To select a filter, at least one filter must be configured in the Networking->QoS->QoS Filter menu.
Direction	<p>Select the direction of the data packets to be classified.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Incoming</i>: Incoming data packets are assigned to the class (Class ID) that is then to be defined.• <i>Outgoing</i> (default value): Outgoing data packets are assigned to the class (Class ID) that is then to be defined.• <i>Both</i>: Incoming and outgoing data packets are assigned to the class (Class ID) that is then to be defined.
High Priority Class	<p>Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority 0 is set automatically.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Class ID	<p>Only for High Priority Class not active.</p> <p>Choose a number which assigns the data packets to a class.</p>
	<div>Note<p>The class ID is a label to assign data packets to specific classes. (The class ID does not define the priority.)</p></div>
	Possible values are whole numbers between <i>1</i> and <i>254</i> .
Set DSCP/TOS value (Layer 3)	<p>Here you can set or change the DSCP/TOS value of the IP data packets, based on the class (Class ID) that has been defined.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Preserve</i> (default value): The DSCP/TOS value of the IP data packets remains unchanged.• <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format).

Field	Description
	<ul style="list-style-type: none">• <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).• <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format).• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
Set COS value (802.1p/Layer 2)	<p>Here you can set/change the service class (Layer 2 priority) in the VLAN Ethernet header of the IP packets, based on the class (Class ID) that has been defined.</p> <p>Possible values are whole numbers between 0 and 7.</p> <p>The default value is <i>Preserve</i>.</p>
Interfaces	<p>Only for Class map = New</p> <p>When creating a new class plan, select the interfaces to which you want to link the class plan. A class plan can be assigned to multiple interfaces.</p>

14.4.3 QoS Interfaces/Policies

In the **Networking->QoS->QoS Interfaces/Policies** menu, you set prioritisation of data.



Note

Data can only be prioritized in the outgoing direction.

Packets in the high-priority class always take priority over data with class IDs 1 - 254.

It is possible to assign or guarantee each queue and thus each data class a certain part of the total bandwidth of the interface. In addition, you can optimise the transmission of voice data (real time data).

Depending on the respective interface, a queue is created automatically for each class, but only for data traffic classified as outgoing and for data traffic classified in both directions. A priority is assigned to these automatic queues. The value of the priority is equal to the value of the class ID. You can change the default priority of a queue. If you add new queues, you can also use classes in other class plans via the class ID.

14.4.3.1 New

Choose the **New** button to create additional prioritisations.

QoS Filter

QoS Classification

QoS Interfaces/Policies

Basic Parameters

Interface

en1-0

Prioritisation Algorithm

Priority Queueing

Traffic shaping

☐ Enabled

Queues/Policies

By creating a QoS policy a default entry with the lowest priority will be automatically generated

Description	Type	Class ID	Priority	Bandwidth for Traffic Shaping
<div>Add</div>				

OK

Cancel

Fig. 96: Networking->QoS->QoS Interfaces/Policies->New

The **Networking->QoS->QoS Interfaces/Policies->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface for which QoS is to be configured.
Prioritisation Algorithm	<div>Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface.</div> <div>Possible values:</div> <ul style="list-style-type: none"><i>Priority Queueing</i>: QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority.<i>Weighted Round Robin</i>: QoS is activated on the interface. The available bandwidth is distributed according to the weighting (weight) of the queue. Exception: High-priority pack-

Field	Description
	<p>ets are always handled with priority.</p> <ul style="list-style-type: none">• <i>Weighted Fair Queueing</i>: QoS is activated on the interface. The available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows in a queue. Exception: High-priority packets are always handled with priority.• <i>Disabled</i> (default value): QoS is deactivated on the interface. The existing configuration is not deleted, but can be activated again if required.
Traffic shaping	<p>Activate or deactivate data rate limiting in the send direction.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Maximum Upload Speed	<p>Only for Traffic shaping = enabled.</p> <p>Enter a maximum data rate for the queue in the send direction in kbits.</p> <p>Possible values are <i>0</i> to <i>1000000</i>.</p> <p>The default value is <i>0</i>, i.e. no limits are set, the queue can occupy the maximum bandwidth.</p>
Protocol Header Size below Layer 3	<p>Only for Traffic shaping = enabled.</p> <p>Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>User defined</i>: Value in byte. <p>Possible values are <i>0</i> to <i>100</i>.</p> <ul style="list-style-type: none">• <i>Undefined (Protocol Header Offset=0)</i> (default value) <p>Can only be selected for Ethernet interfaces</p> <ul style="list-style-type: none">• <i>Ethernet</i>• <i>Ethernet and VLAN</i>• <i>PPP over Ethernet</i>

Field	Description
	<ul style="list-style-type: none">• <i>PPP over Ethernet and VLAN</i> <p>Can only be selected for IPSec interfaces:</p> <ul style="list-style-type: none">• <i>IPSec over Ethernet</i>• <i>IPSec over Ethernet and VLAN</i>• <i>IPSec via PPP over Ethernet</i>• <i>IPSec via PPPoE and VLAN</i>
Encryption Method	<p>Only if an IPSec Peers is selected as Interface, Traffic shaping is <i>Active</i> and Protocol Header Size below Layer 3 is not <i>Undefiniert (Protocol Header Offset=0)</i>.</p> <p>Select the encryption method used for the IPSec connection. The encryption algorithm determines the length of the block cipher which is taken into account during bandwidth calculation.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>DES, 3DES, Blowfish, Cast - (cipher block size = 64 Bit)</i>• <i>AES128, AES192, AES256, Twofish - (cipher block size = 128 Bit)</i>
Real Time Jitter Control	<p>Only for Traffic shaping = enabled</p> <p>Real Time Jitter Control optimises latency when forwarding real time datagrams. The function ensures that large data packets are fragmented according to the available upload bandwidth.</p> <p>Real Time Jitter Control is useful for small upload bandwidths (< 800 kbps).</p> <p>Activate or deactivate Real Time Jitter Control.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Control Mode	<p>Only for Real Time Jitter Control = enabled.</p> <p>Select the mode for optimising voice transmission.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>All RTP Streams</i>: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected.• <i>Inactive</i>: Voice data transmission is not optimised.• <i>Controlled RTP Streams only</i>: This mode is used if either the VoIP Application Layer Gateway (ALG) or the VoIP Media Gateway (MGW) is active. Real Time Jitter Control is activated by the control instances ALG or MGW.• <i>Always</i>: Real Time Jitter Control is always active, even if no real time data is routed.
Queues/Policies	<p>Configure the desired QoS queues.</p> <p>For each class created from the class plan, which is associated with the selected interface, a queue is generated automatically and displayed here (only for data traffic classified as outgoing and for data traffic classified as moving in both directions).</p> <p>Add new entries with Add. The Edit Queue/Policy menu opens.</p> <p>By creating a QoS policy a DEFAULT entry with the lowest priority 255 is automatically created.</p>

The menu **Edit Queue/Policy** consists of the following fields:

Fields in the Edit Queue/Policy menu.

Field	Description
Description	Enter the name of the queue/policy.
Outbound Interface	Shows the interface for which the QoS queues are being configured.
Prioritisation queue	<p>Select the queue priority type.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Class Based</i> (default value): Queue for data classified as “normal”• <i>High Priority</i>: Queue for data classified as “high priority”

Field	Description
	<ul style="list-style-type: none">• <i>Default:</i> Queue for data that has not been classified or data of a class for which no queue has been configured.
Class ID	<p>Only for Prioritisation queue = <i>Class Based</i></p> <p>Select the QoS packet class to which this queue is to apply.</p> <p>To do this, at least one class ID must be given in the Network-ing->QoS->QoS Classification menu.</p>
Priority	<p>Only for Prioritisation queue = <i>Class Based</i></p> <p>Choose the priority of the queue. Possible values are <i>1</i> (high priority) to <i>254</i> (low priority).</p> <p>The default value is <i>1</i>.</p>
Weight	<p>Only for Prioritisation Algorithm = <i>Weighted Round Robin</i> or <i>Weighted Fair Queueing</i></p> <p>Choose the priority of the queue. Possible values are <i>1</i> to <i>254</i>.</p> <p>The default value is <i>1</i>.</p>
RTT Mode (Realtime Traffic Mode)	<p>Active or deactivate the real time transmission of the data.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>RTT mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams.</p> <p>It is possible to configure multiple queues when RTT mode is enabled. Queues with enabled RTT mode must always have a higher priority than queues with disabled RTT mode.</p>
Traffic Shaping	<p>Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction.</p> <p>The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.)</p> <p>The function is enabled with <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.
Maximum Upload Speed	<p>Only for Traffic Shaping = enabled.</p> <p>Enter a maximum data rate for the queue in kbits.</p> <p>Possible values are <i>0</i> to <i>1000000</i>.</p> <p>The default value is <i>0</i>.</p>
Overbooking allowed	<p>Only for Traffic Shaping = enabled.</p> <p>Enable or disable the function. The function controls the bandwidth limit.</p> <p>If Overbooking allowed is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface.</p> <p>If Overbooking allowed is deactivated, the queue can never occupy bandwidth beyond the bandwidth limit that has been set.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Burst size	<p>Only for Traffic Shaping = enabled.</p> <p>Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached.</p> <p>Possible values are <i>0</i> to <i>64000</i>.</p> <p>The default value is <i>0</i>.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Dropping Algorithm	<p>Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>Tail Drop</i> (default value): The newest packet received is dropped.• <i>Head Drop</i>: The oldest packet in the queue is dropped.• <i>Random Drop</i>: A randomly selected packet is dropped from the queue.
Congestion Avoidance (RED)	<p>Enable or disable preventative deletion of data packets.</p> <p>Packets which have a data size of between Min. queue size and Max. queue size are preventively dropped to prevent queue overflow (RED=Random Early Detection). This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses.</p> <p>The function is activated with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Min. queue size	<p>Enter the lower threshold value for the process Congestion Avoidance (RED) in bytes.</p> <p>Possible values are <i>0</i> to <i>262143</i>.</p> <p>The default value is <i>0</i>.</p>
Max. queue size	<p>Enter the upper threshold value for the process Congestion Avoidance (RED) in bytes.</p> <p>Possible values are <i>0</i> to <i>262143</i>.</p> <p>The default value is <i>16384</i>.</p>

14.5 Access Rules

Accesses to data and functions are restricted with access lists (which user gets to use which services and files).

You define filters for IP packets in order to allow or block access from or to the various hosts in connected networks. This enables you to prevent undesired connections being set up via the gateway. Access lists define the type of IP traffic the gateway is to accept or deny. The access decision is based on information contained in the IP packets, e.g.:

- source and/or destination IP address
- packet protocol
- source and/or destination port (port ranges are supported)

Access lists are an effective means if, for example, sites with LANs interconnected over a bintec elmeg gateway wish to deny all incoming FTP requests or only allow Telnet sessions between certain hosts.

Access filters in the gateway are based on the combination of filters and actions for filter rules (= rules) and the linking of these rules to form rule chains. They act on the incoming data packets to allow or deny access to the gateway for certain data.

A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, netmask, protocol and source and/or destination port.

You use the rules that you set up in the access lists to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

There are various approaches for the definition of rules and rule chains:

Allow all packets that are not explicitly denied, i.e.:

- Deny all packets that match Filter 1.
- Deny all packets that match Filter 2.
- ...
- Allow the rest.

or

Allow all packets that are explicitly allowed, i.e.:

- Allow all packets that match Filter 1.
- Allow all packets that match Filter 2.
- ...
- Deny the rest.

or

Combination of the two possibilities described above.

A number of separate rule chains can be created. The same filter can also be used in different rule chains.

You can also assign a rule chain individually to each interface.



Caution

Make sure you don't lock yourself out when configuring filters:

If possible, access your gateway for filter configuration over the serial console interface or ISDN Login.

14.5.1 Access Filter

This menu is for configuration of access filter Each filter describes a certain part of the IP traffic and defines, for example, the IP addresses, the protocol, the source port or the destination port.

A list of all access filters is displayed in the **Networking->Access Rules->Access Filter** menu.

Access FilterRule ChainsInterface Assignment


View 20 per page<<>>Filter inNoneequalGo

Index	Description	Source	Destination	TOS Decimal Value
Page: 1				

New

Fig. 97: **Networking->Access Rules->Access Filter**

14.5.1.1 Edit or New

Choose the  icon to edit existing entries. To configure access fitters, select the **New** button.

Access Filter

Rule Chains

Interface Assignment

Basic Parameters

Description

Service

User-defined

Protocol

Any

Destination IP Address/Netmask

Any

Source IP Address/Netmask

Any

DSCP/TOS Filter (Layer 3)

Ignore

COS Filter (802.1p/Layer 2)

Ignore

OK

Cancel

Fig. 98: **Networking->Access Rules->Access Filter->New**

The **Networking->Access Rules->Access Filter->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the filter.
Service	<div>Select one of the preconfigured services. The extensive range of services configured ex works includes the following:</div> <div><ul style="list-style-type: none">activityapple-qtauthchargeclients_1daytimedhcpdiscard</div> <div>The default value is <i>User defined</i>.</div>
Protocol	<div>Select a protocol.</div> <div>The <i>Any</i> option (default value) matches any protocol.</div>
Type	Only if Protocol = <i>ICMP</i>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i>• <i>Echo reply</i>• <i>Destination unreachable</i>• <i>Source quench</i>• <i>Redirect</i>• <i>Echo</i>• <i>Time exceeded</i>• <i>Timestamp</i>• <i>Timestamp reply</i> <p>The default value is <i>Any</i>.</p> <p>See RFC 792.</p>
Connection State	<p>Only if Protocol = <i>TCP</i></p> <p>You can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value): All TCP packets match the filter.• <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.
Destination IP Address/Netmask	<p>Enter the destination IP address and netmask of the data packets.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <i>Host</i>: Enter the IP address of the host.• <i>Network</i>: Enter the network address and the related netmask.
Destination Port/Range	<p>Only if Protocol = <i>TCP, UDP</i></p> <p>Enter a destination port number or a range of destination port numbers that matches the filter.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The filter is valid for all port numbers• <i>Specify port</i>: Enables the entry of a port number.• <i>Specify port range</i>: Enables the entry of a range of port numbers.
Source IP Address/ Netmask	Enter the source IP address and netmask of the data packets.
Source Port/Range	<p>Only if Protocol = <i>TCP, UDP</i></p> <p>Enter a source port number or the range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The filter is valid for all port numbers• <i>Specify port</i>: Enables the entry of a port number.• <i>Specify port range</i>: Enables the entry of a range of port numbers.
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Ignore</i> (default value): The type of service is ignored.• <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit).• <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).• <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format).• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.

Field	Description
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Possible values are whole numbers between 0 and 7.</p> <p>The default value is <i>Ignore</i>.</p>

14.5.2 Rule Chains

Rules for IP filters are configured in the **Rule Chains** menu. These can be created separately or incorporated in rule chains.

In the **Networking->Access Rules->Rule Chains** menu, all created filter rules are listed.

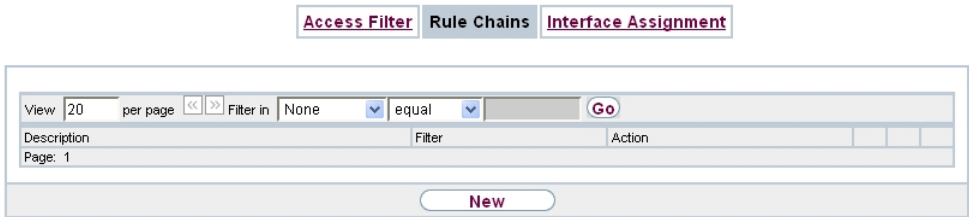



Fig. 99: **Networking->Access Rules->Rule Chains**

14.5.2.1 Edit or New

Choose the  icon to edit existing entries. To configure access lists, select the **New** button.

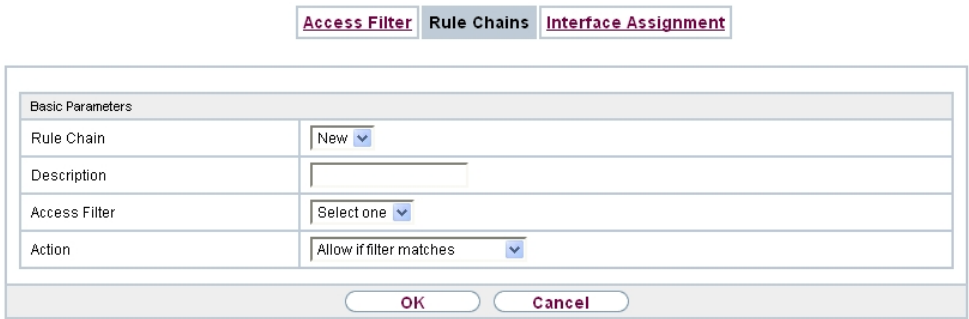



Fig. 100: **Networking->Access Rules->Rule Chains->New**

The **Networking->Access Rules->Rule Chains->New** menu consists of the following

fields:

Fields in the Basic Parameters menu.

Field	Description
Rule Chain	<p>Select whether to create a new rule chain or to edit an existing one.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>New</i> (default value): You can create a new rule chain with this setting.• <i><Name of the rule chain></i>: Select an already existing rule chain, and thus add another rule to it.
Description	<p>Enter the name of the rule chain.</p>
Access Filter	<p>Select an IP filter.</p> <p>If the rule chain is new, select the filter to be set at the first point of the rule chain.</p> <p>If the rule chain already exists, select the filter to be attached to the rule chain.</p>
Action	<p>Define the action to be taken for a filtered data packet.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Allow if filter matches</i> (default value): Allow packet if it matches the filter.• <i>Allow if filter does not match</i>: Allow packet if it does not match the filter.• <i>Deny if filter matches</i>: Deny packet if it matches the filter.• <i>Deny if filter does not match</i>: Deny packet if it does not match the filter.• <i>Ignore</i>: Use next rule.

To set the rules of a rule chain in a different order select the  button in the list menu for the entry to be shifted. A dialog box opens, in which you can decide under **Move** whether the entry *below* (default value) or *above* another rule of this rule chain is to be shifted.

14.5.3 Interface Assignment

In this menu, the configured rule chains are assigned to the individual interfaces and the gateway's behavior is defined for denying IP packets.

A list of all configured interface assignments is displayed in the **Networking->Access Rules->Interface Assignment** menu.

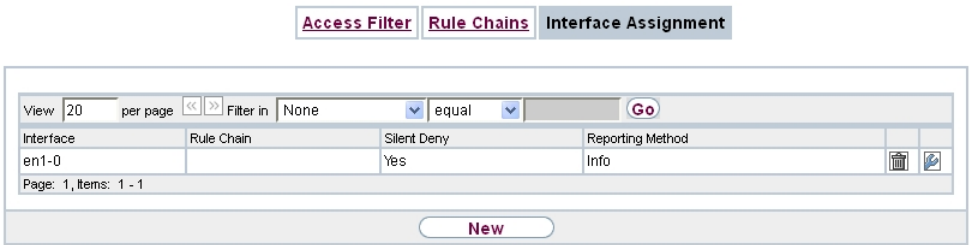



Fig. 101: **Networking->Access Rules->Interface Assignment**

14.5.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure additional assignments.

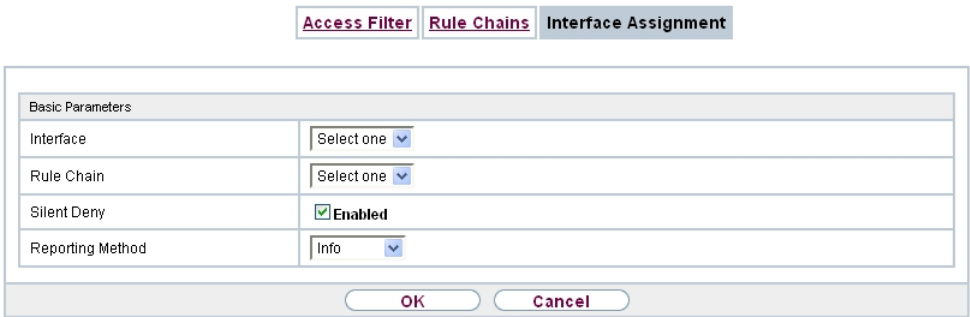


Fig. 102: **Networking->Access Rules->Interface Assignment->New**

The **Networking->Access Rules->Interface Assignment->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.

Field	Description
Rule Chain	Select a rule chain.
Silent Deny	<p>Define whether the sender is to be informed if an IP packet is denied.</p> <ul style="list-style-type: none">• <i>Enabled</i> (default value): The sender is not informed.• <i>Disabled</i>: The sender receives an ICMP message.
Reporting Method	<p>Define whether a syslog message is to be generated if a packet is denied.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>No report</i>: No syslog message.• <i>Info</i> (default value): A syslog message is generated with the protocol number, source IP address and source port number.• <i>Dump</i>: A syslog message is generated with the contents of the first 64 bytes of the denied packet.

14.6 Drop In

"Drop-in mode" allows you to split a network into smaller segments without having to divide the IP network into subnets. Several interfaces can be combined in a drop-in group and assigned to a network to do this. All of the interfaces are then configured with the same IP address.

Within a segment, network components which are connected to a connection can then be grouped and, for example, be protected by firewall. Data traffic from network components between individual segments which are assigned to different ports are then controlled according to the configured firewall rules.

14.6.1 Drop In Groups

The **Networking->Drop In->Drop In Groups** menu displays a list of all the **Drop In Groups**. Each **Drop In** group represents a network.

14.6.1.1 New

Select the **New** button to set up other **Drop In Groups**.

Drop In Groups

Basic Parameters

Group Description

Mode

Transparent

Exclude from NAT (DMZ)

☐ Enabled

Network Configuration

Static

Network Address

Netmask

Local IP Address

ARP Lifetime

3600

Seconds

DNS assignment via DHCP

Unchanged

Interface Selection

Interface

Add

OK

Cancel

Fig. 103: Networking->Drop In->Drop In Groups->New

The **Networking->Drop In->Drop In Groups->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Group Description	Enter a unique name for the Drop In group.
Mode	<p>Select which mode is to be used to send the MAC addresses of network components.</p> <p>Possible values:</p> <ul style="list-style-type: none"><i>Transparent</i> (default value): ARP packets and IP packets belonging to the drop-in network are routed transparently (unchanged).<i>Proxy</i>: ARP packets and IP packets related to the drop-in network are forwarded with the MAC address of the corresponding interface.
Exclude from NAT (DMZ)	<p>Here you can take data traffic from NAT.</p> <p>Use this function to, for example, ensure that certain web servers in a DMZ can be accessed.</p> <p>The function is enabled with <i>Enabled</i>.</p>

Field	Description
	The function is disabled by default.
Network Configuration	<p>Select how an IP address / netmask is assigned to the Drop In network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i> (default value) • <i>DHCP</i>
Network Address	<p>Only for Network Configuration = <i>Static</i></p> <p>Enter the network address of the Drop In network.</p>
Netmask	<p>Only for Network Configuration = <i>Static</i></p> <p>Enter the corresponding netmask.</p>
Local IP Address	<p>Only for Network Configuration = <i>Static</i></p> <p>Enter the local IP address. This IP address must be identical for all the Ethernet ports in a network.</p>
DHCP Client on Interface	<p>Only for Network Configuration = <i>DHCP</i></p> <p>Here you can select an Ethernet interface on your router which is to act as the DHCP client.</p> <p>You need this setting, for example, if your provider's router is being used as the DHCP server.</p> <p>You can choose from the interfaces available to your device; however the interface must be a member of the drop-in group.</p>
ARP Lifetime	<p>Determines the time period for which the ARP entries will be held in the cache.</p> <p>The default value is <i>3600</i> seconds.</p>
DNS assignment via DHCP	<p>The gateway can modify DHCP packets which pass through the drop-in group and identify itself as an available DNS server.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Unchanged</i> (default value)

Field	Description
	<ul style="list-style-type: none">• <i>Own IP Address</i>
Interface Selection	<p>Select all the ports which are to be included in the Drop In group (in the network).</p> <p>Add new entries with Add.</p>

Chapter 15 Routing Protocols

15.1 RIP

The entries in the routing table can be defined statically or the routing table can be updated constantly by dynamic exchange of routing information between several devices. This exchange is controlled by a Routing Protocol, e.g. RIP (Routing Information Protocol). By default, about every 30 seconds (this value can be changed in **Update Timer**), a device sends messages to remote networks using information from its own current routing table. The complete routing table is always exchanged in this process. If triggered RIP is used, information is only exchanged if the routing information has changed. In this case, only the changed information is sent.

Observing the information sent by other devices enables new routes and shorter paths for existing routes to be saved in the routing table. As routes between networks can become unreachable, RIP removes routes that are older than 5 minutes (i.e. routes not verified in the last 300 seconds - **Garbage Collection Timer** + **Route Timeout**). Routes learnt with triggered RIP are not deleted.

Your device supports both version 1 and version 2 of RIP, either individually or together.

15.1.1 RIP Interfaces

A list of all RIP interfaces is displayed in the **Routing Protocols->RIP->RIP Interfaces** menu.

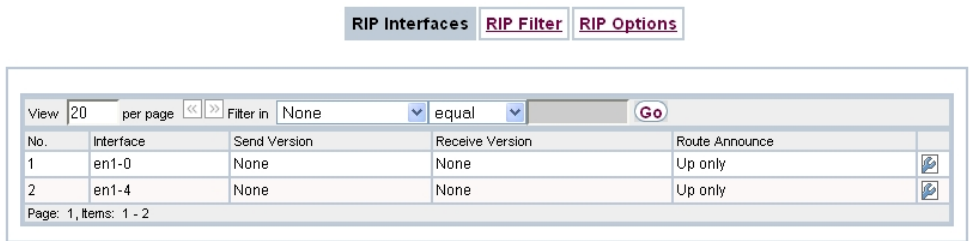


Fig. 104: Routing Protocols->RIP->RIP Interfaces

15.1.1.1 Edit


For every RIP interface, go to the  menu to select the options *Send Version*, *Receive Version* and *Route Announce*.



Fig. 105: Routing Protocols->RIP->RIP Interfaces->

The menu **Networking->RIP->RIP Interfaces->** consists of the following fields:

Fields in the RIP Parameters for menu.

Field	Description
Send Version	<p>Decide whether routes are to be propagated via RIP and if so, select the RIP version for sending RIP packets over the interface in send direction.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): RIP is not enabled.• <i>RIP V1</i>: Enables sending and receiving of version 1 RIP packets.• <i>RIP V2</i>: Enables sending and receiving of version 2 RIP packets.• <i>RIP V1/V2</i>:Enables sending and receiving RIP packets of both version 1 and 2.• <i>RIP V2 Multicast</i>: For sending RIP V2 messages over multicast address 224.0.0.9.• <i>RIP V1 Triggered</i>: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP).• <i>RIP V2 Triggered</i>: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Receive Version	<p>Decide whether routes are to be imported via RIP and if so, select the RIP version for receiving RIP packets over the interface in receive direction.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>None</i> (default value): RIP is not enabled.• <i>RIP V1</i>: Enables sending and receiving of version 1 RIP packets.• <i>RIP V2</i>: Enables sending and receiving of version 2 RIP packets.• <i>RIP V1/V2</i>:Enables sending and receiving RIP packets of both version 1 and 2.• <i>RIP V1 Triggered</i>: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP).• <i>RIP V2 Triggered</i>: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Route Announce	<p>Select this option if you want to set the time at which any activated routing protocols (e.g. RIP) are to propagate the IP routes defined for this interface.</p> <p>Note: This setting does not affect the interface-specific RIP configuration mentioned above.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Up or Dormant</i> (not for LAN interfaces, interfaces in Bridge mode and interfaces for leased lines): Routes are propagated if the interface status is up or ready.• <i>Up only</i> (default value): Routes are only propagated if the interface status is up.• <i>Always</i>: Routes are always propagated independently of operational status.

15.1.2 RIP Filter

In this menu, you can specify exactly which routes are to be exported or imported.

You can use the following strategies for this:

- You explicitly deactivate the import or export of certain routes. The import or export of all other routes that are not listed is still allowed.
- You explicitly activate the import or export of certain routes. In this case, you must also explicitly deactivate the import or export of all other routes. This is achieved using a filter for **IP Address / Netmask** = no entry (this corresponds to IP address 0.0.0.0 with netmask 0.0.0.0). To make sure this filter is used last, it must be placed at the lowest posi-

tion.


You configure a filter for a default route with the following values:


- **IP Address / Netmask** = no entry for IP address (this corresponds to IP address 0.0.0.0), for netmask = 255.255.255.255

A list of all RIP filters is displayed in the **Routing Protocols->RIP->RIP Filter** menu.



Fig. 106: **Routing Protocols->RIP->RIP Filter**

You can use the  button to insert another filter above the list entry. The configuration menu for creating a new window opens.

You can use the  button to move the list entry. A dialog box opens, in which you can select the position to which the filter is to be moved.

15.1.2.1 New

Choose the **New** button to set up more RIP filters.



Fig. 107: **Routing Protocols->RIP->RIP Filter->New**

The menu **Routing Protocols->RIP->RIP Filter->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface to which the rule to be configured applies.
IP Address / Netmask	<p>Enter the IP address and netmask to which the rule is to be applied. This address can be in the LAN or WAN.</p> <p>The rules for incoming and outgoing RIP packets (import or export) for the same IP address must be separately configured.</p> <p>You can enter individual host addresses or network addresses.</p>
Direction	<p>Select whether the filter applies to the export or import of routes.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Import</i> (default value)• <i>Export</i>
Metric Offset for Active Interfaces	<p>Select the value to be added to the route metric if the status of the interface is "up". During export, the value is added to the exported metric if the interface status is "up".</p> <p>Possible values are <i>-16</i> to <i>16</i>.</p> <p>The default value is <i>0</i>.</p>
Metric Offset for Inactive Interfaces	<p>Select the value to be added to the route metric if the status of the interface is "dormant". During export, the value is added to the exported metric if the interface status is "dormant".</p> <p>Possible values are <i>-16</i> to <i>16</i>.</p> <p>The default value is <i>0</i>.</p>

15.1.3 RIP Options

RIP InterfacesRIP FilterRIP Options

Global RIP Parameters

RIP UDP Port	520
Default Route Distribution	<input checked="" type="checkbox"/> Enabled
Poisoned Reverse	<input type="checkbox"/> Enabled
RFC 2453 Variable Timer	<input checked="" type="checkbox"/> Enabled
RFC 2091 Variable Timer	<input type="checkbox"/> Enabled
Timer for RIP V2 (RFC 2453)	
Update Timer	30 Seconds
Route Timeout	180 Seconds
Garbage Collection Timer	120 Seconds

OKCancel

Fig. 108: Routing Protocols->RIP->RIP Options

The menu **Routing Protocols->RIP->RIP Options** consists of the following fields:

Fields in the Global RIP Parameters menu.

Field	Description
RIP UDP Port	The setting option UDP Port, which is used for sending and receiving RIP updates, is only for test purposes. If the setting is changed, this can mean that your device sends and listens at a port that no other devices use. The default value 520 should be retained.
Default Route Distribution	Select whether the default route of your device is to be propagated via RIP updates. The function is enabled with <i>Enabled</i> . The function is enabled by default.
Poisoned Reverse	Select the procedure for preventing routing loops. With standard RIP, the routes learnt are propagated over all interfaces with RIP SEND activated. With Poisoned Reverse , however, your device propagates over the interface via which it learnt the routes, with the metric (Next Hop Count) 16

Field	Description
	<p>(=“Network is not reachable”).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
RFC 2453 Variable Timer	<p>For the timers described in RFC 2453, select whether the same values that you can configure in the Timer for RIP V2 (RFC 2453) menu should be used.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>If you deactivate the function, the times defined in RFC are retained for the timeouts.</p>
RFC 2091 Variable Timer	<p>For the timers described in RFC 2091, select whether the same values that you can configure in the Timer for Triggered RIP (RFC 2091) menu should be used.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If the function is not activated, the times defined in RFC are retained for the timeouts.</p>

Fields in the Timer for RIP V2 (RFC 2453) menu.

Field	Description
Update Timer	<p>Only for RFC 2453 Variable Timer = <i>Enabled</i></p> <p>An RIP update is sent on expiry of this period of time.</p> <p>The default value is <i>30</i> (seconds).</p>
Route Timeout	<p>Only for RFC 2453 Variable Timer = <i>Enabled</i></p> <p>After the last update of a route, the route time is active.</p> <p>After timeout, the route is deactivated and the Garbage Collection Timer is started.</p> <p>The default value is <i>180</i> (seconds).</p>

Field	Description
Garbage Collection Timer	<p>Only for RFC 2453 Variable Timer = <i>Enabled</i></p> <p>The Garbage Collection Timer is started as soon as the route timeout has expired.</p> <p>After this timeout, the invalid route is deleted from the IPROUTETABLE if no update is carried out for the route.</p> <p>The default value is <i>120</i> (seconds).</p>

Fields in the Timer for Triggered RIP (RFC 2091) menu.

Field	Description
Hold Down Timer	<p>Only for RFC 2091 Variable Timer = <i>Enabled</i></p> <p>The hold down timer is activated as soon as your device receives an unreachable route (metric 16). The route may deleted once this period has elapsed.</p> <p>The default value is <i>120</i> (seconds).</p>
Retransmission Timer	<p>Only for RFC 2091 Variable Timer = <i>Enabled</i></p> <p>After this timeout, update request or update response packets are sent again until an update flush or update acknowledge packet arrives.</p> <p>The default value is <i>5</i> (seconds).</p>

15.2 OSPF

OSPF (Open Shortest Path First) is a dynamic routing protocol that is frequently used in larger networks as an alternative to RIP. It was originally developed to avoid a number of limitations of RIP (when used in larger networks).

The problems (with RIP) avoided by OSPF include:

- Reduced network load: After a short initialization phase, routing information is not sent periodically as with RIP, but only changed routing information.
- Authentication: Gateway authentication can be configured to increase the security when exchanging routing information.
- Routing Traffic Control: Gateways can be combined to form areas to limit the traffic created by exchanging routing information.

- Connection costs: OSPF differs from RIP in that the connection costs are not calculated from the number of next hops, but from the bandwidth of the respective transport medium.
- No limitation of the number of hops: The limitation of the maximum number of 16 hops for RIP does not exist for OSPF.

Although the OSPF protocol is considerably more complex than RIP, the basic concept is the same, i.e. OSPF also determines the best path for forwarding the packets in each case.

OSPF is an Interior Gateway Protocol that is used to distribute routing information within an autonomous system (AS). The Link State Updates are exchanged between the gateways by flooding. Each change of routing information is passed to all gateways in the network. OSPF areas are defined to limit the number of Link State Updates. All gateways of an area have an identical Link State database.

An area is interface-specific. Gateways whose interfaces belong to several areas and connect these to the backbone are called Area Border Routers (ABR). ABRs therefore contain the information of the backbone area and all areas connected. A gateway whose interfaces are all incorporated in one area are called Internal Routers (IR).

There are four types of Link State packets: Router links show the state of the interfaces of a gateway that belong to a certain area. Summary links are generated by the ABR to define how the information on reachability in the network is exchanged between areas. Usually all information is sent to the backbone area, which then passes the information to the other areas. Network links are sent by Designated Routers (DS) within a segment and propagate all gateways that are connected to a certain multi-access segment like Ethernet, Token Ring and FDDI (also NBMA). External links point to networks outside the AS. These networks are incorporated in OSPF using redistribution. In this case, an Autonomous System Border Router (ASBR) incorporates these external routes in the AS.

It is possible to increase security by authenticating the OSPF packets, so that the gateways can participate in Routing Domains using predefined passwords.

It is recommended that several areas are defined in larger networks. If more than one area is configured, one of these areas must possess the area ID 0.0.0.0, which defines the backbone area. This must be the centre point of all areas, i.e. all areas must be physically connected to the backbone area. Occasionally, gateways cannot be physically connected directly to the backbone area and virtual links must be set up.

The purpose of virtual links is to connect areas in which no physical connection to the backbone is possible and to maintain the connection of the backbone in case of a failure of the 0.0.0.0 area.

Summarizing is the term given to the consolidation of the various routes into a single advertisement (summary link). This is usually done by the ABR at the area borders.

Certain areas can be defined as stub areas in OSPF. This prevents external networks, e.g. those propagated from other protocols by redistribution in OSPF, being propagated into the stub area. Externally routing of such areas is propagated with a default route. The configuration of a stub area reduces the database size in the area and reduces the amount of storage space needed on the gateways incorporated in the area.

15.2.1 Areas

OSPF areas must be defined before the gateway interface can be assigned to an area.

A list of all configured OSPF areas is displayed in the **Routing Protocols->OSPF->Areas** menu.

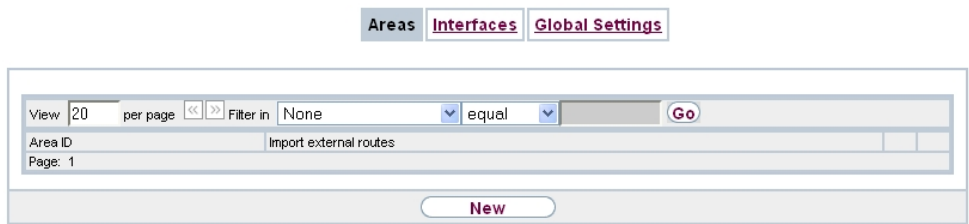



Fig. 109: Routing Protocols->OSPF->Areas

15.2.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional areas.

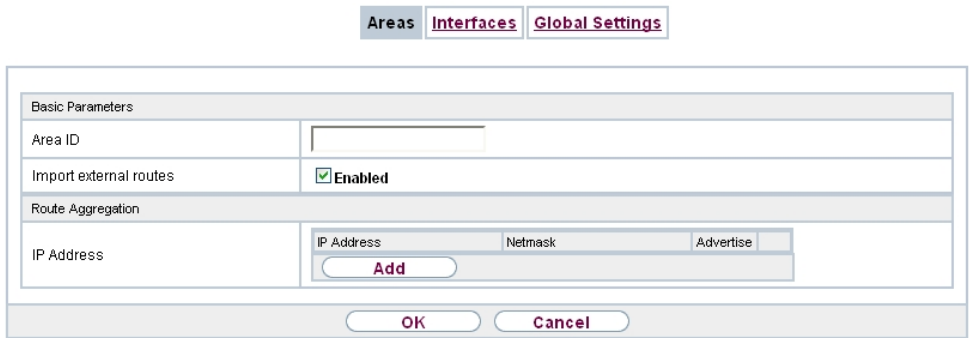


Fig. 110: Routing Protocols->OSPF->Areas->New

The **Routing Protocols->OSPF->Areas->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Area ID	Enter the ID to identify the OSPF aea. The backbone area is <i>0.0.0.0</i> .
Import external routes	<p>Specifies whether the gateway routing information generated from external autonomous systems (not areas) is to be imported.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is activated by default.</p>
Import summary routes	<p>Only for Import external routes = <i>Disabled</i></p> <p>Define whether summary LSAs (routing information generated by Area Border Gateway) are to be sent to the stub area.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Enabled</i> (default value): Activates import.• <i>Disabled</i>: Deactivates the import.
Create area default route (only ABR)	<p>Only for Import external routes = <i>Disabled</i></p> <p>Select whether the Area Border Gateway shall send no LSA's in the stub area, but rather only propagate a default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is not activated by default.</p>

Fields in the Route Aggregation menu.

Field	Description
IP Address	<p>Define the OSPF area.</p> <ul style="list-style-type: none">• <i>IP Address</i>: Here you enter the IP address of the area to be combined.• <i>Netmask</i>: Enter the netmask here.• <i>Advertise</i>: Subnetworks that are combined into areas either initiate propagation of the given combination (<i>Yes</i>, default value), or cause the subnetwork not to be propagated outside the area at all (<i>No</i>), i.e. neither the actual subnetworks nor the combined overall subnetwork are propagated. <p>Add new entries with Add.</p>

15.2.2 Interfaces

In the **Routing Protocols->OSPF->Interfaces** menu, a list of all interfaces is displayed.

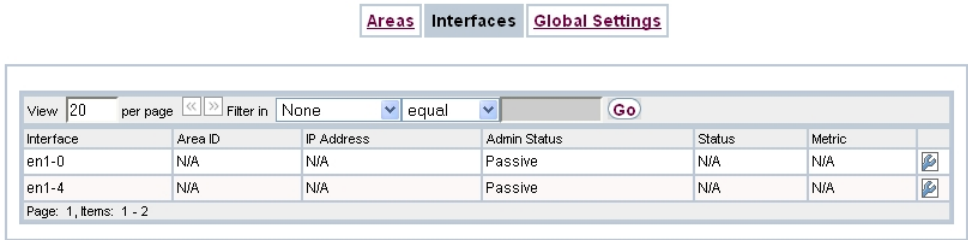


Fig. 111: Routing Protocols->OSPF->Interfaces



Caution

If your interfaces are not only to be assigned to Backbone Area 0.0.0.0, you must first define OSPF areas in the **Routing Protocols->OSPF->Areas** menu.

15.2.2.1 Edit

Select the symbol to modify the OSPF settings for the interfaces.



Fig. 112: Routing Protocols->OSPF->Interfaces->

The **Routing Protocols->OSPF->Interfaces->** menu consists of the following fields:

Fields in the OSPF Interface Configuration menu.

Field	Description
Admin Status	The status of an OSPF interface defines whether routes are propagated and/or OSPF protocol packets are sent over the interface. If OSPF is not yet activated, only the Admin Status field is shown (in this case changes are irrelevant).

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface.• <i>Passive</i>: OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces.• <i>Inactive</i>: OSPF is completely disabled for this interface.
Area ID	<p>Select the ID of the area to which this interface shall be assigned.</p> <p>If your interface is not only to be assigned to Backbone Area 0.0.0.0, you must first define OSPF areas in the Routing Protocols->OSPF->Areas menu.</p>
Metric Determination	<p>Defines how the metric of this interface is calculated.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Auto (Interface Speed)</i> (default value): The metric is automatically set on the basis of the interface speed.• <i>Fixed</i>: Enter a specific value in Metric (direct routes).
Metric (direct routes)	<p>Enter the base metric value. The basis of the metric actually used for a route is a base metric value, which is obtained from the bandwidth of the interface: $BMV = 100,000,000 / \text{bandwidth in bps}$ For Metric Determination <i>Auto (Interface Speed)</i> the automatically calculated value is displayed here and cannot be modified.</p> <p>The basic metric value for bandwidths $\geq 100.000.000$ bps is always <i>1</i>. So the basic metric value of Gigabit interfaces and 100 Mbit interfaces is identical. To change this, you need to specify a fixed value in Metric Determination.</p>
Authentication Type	<p>Select the type of authentication used if OSPF packets are sent over this OSPF interface (or incoming packets checked). Defines how the key in the Authentication Key field is used.</p> <p>The default value is <i>none</i>. In <i>Clear Text</i>, the key is sent as a text string in each packet. In <i>MD5</i>, the key is used to create a</p>

Field	Description
	hash, which is sent with each packet
Authentication Key	Enter a text string to be used in combination with the defined Authentication Type .
Export indirect static routes	If this value is set to <i>No</i> (default), only direct routes (i.e. routes to networks reached directly over this interface) are propagated over active OSPF interfaces (see Admin Status). If the value is set to <i>Yes</i> , indirect static routes are also propagated over active interfaces.
Demand Circuit Options	Define whether Demand OSPF procedures (Hello suppression on FULL Neighbors and setting of DoNotAge flags on the propagated LSA) shall be performed (Yes, default value) or not (<i>No</i>). This option should be enabled particularly in the case of connections for which the costs are calculated based on time (e.g. ISDN dialup connections, Internet connections with no flat rate).

15.2.3 Global Settings

The **Routing Protocols->OSPF->Global Settings** menu contains global OSPF parameters. OSPF is activated on the gateway.

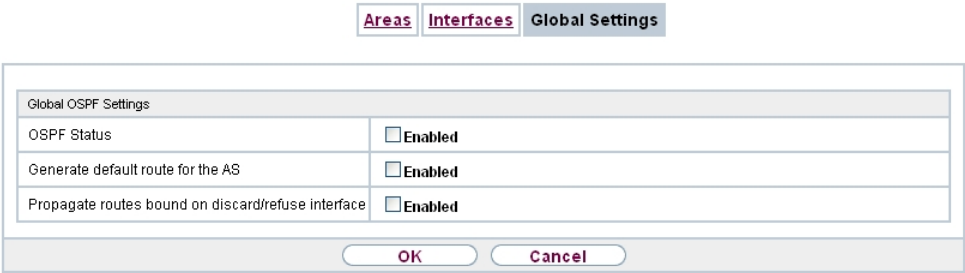


Fig. 113: Routing Protocols->OSPF->Global Settings

The **Routing Protocols->OSPF->Global Settings** menu consists of the following fields:

Fields in the Global OSPF Settings menu.

Field	Description
OSPF Status	Enable or disable OSPF. The function is disabled by default.

Field	Description
Generate default route for the AS	<p>If this option is activated, the gateway propagates a default route over all active OSPF interfaces.</p> <p>The function is disabled by default.</p>
Propagate routes bound on discard/re-fuse interface	<p>The logical interfaces REFUSE and IGNORE have the following meaning:</p> <p>REFUSE means (if a route exists on this) that packets from this interface are discarded and an ICMP Unreachable Reply is generated.</p> <p>IGNORE means (if a route exists on this) that packets from this interface are discarded without comment.</p> <p>If the option is activated, routes connected to the two discard/re-fuse interfaces are saved by OSPF in its database. If the option is deactivated, these routes are ignored.</p> <p>The function is disabled by default.</p>
Dynamic LS Update Compression	<p>Only for RXL1250 / RXL12100</p> <p>Enable or disable the function.</p> <p>The function is disabled by default.</p>

Chapter 16 Multicast

What is multicasting?

Many new communication technologies are based on communication from one sender to several recipients. Therefore, modern telecommunication systems such as voice over IP or video and audio streaming (e.g. IPTV or Webradio) focus on reducing data traffic, e.g. by offering TriplePlay (voice, video, data). Multicast is a cost-effective solution for effective use of bandwidth because the sender of the data packet, which can be received by several recipients, only needs to send the packet once. The packet is sent to a virtual address defined as a multicast group. Interested recipients log in to these groups.

Other areas of use

One classic area in which multicast is used is for conferences (audio/video) with several recipients. The most well-known are probably the MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) and Whiteboard (WB). VAT can be used to hold audio conferences. All subscribers are displayed in a window and the speaker(s) are indicated by a black box. Other areas of use are of particular interest to companies. Here, multicasting makes it possible to synchronise the databases of several servers, which is valuable for multinationals or even companies with just a few locations.

Address range for multicast

For IPv4 the IP addresses 224.0.0.0 to 239.255.255.255 (224.0.0.0/4) are reserved for multicast in the class D network. An IP address from this range represents a multicast group to which several recipients can log in. The multicast router then forwards the required packets to all subnets with logged in recipients.

Multicast basics

Multicast is connectionless, which means that any trouble-shooting or flow control needs to be guaranteed at application level.

At transport level, UDP is used almost exclusively, as, in contrast to TCP, it is not based on a point-to-point connection.

At IP level, the main difference is therefore that the destination address does not address a

dedicated host, but rather a group, i.e. during the routing of multicast packets, the decisive factor is whether a recipient is in a logged-in subnet.

In the local network, all hosts are required to accept all multicast packets. For Ethernet or FDD, this is based on MAC mapping, where the group address is encoded into the destination MAC address. For routing between several networks, the routers first need to make themselves known to all potential recipients in the subnet. This is achieved by means of Membership Management protocols such as IGMP for IPv4 and MLP for IPv6.

Membership Management protocol

In IPv4, IGMP (Internet Group Management Protocol) is a protocol that hosts can use to provide the router with multicast membership information. IP addresses of the class D address range are used for addressing. An IP address in this class represents a group. A sender (e.g. Internet radio) sends data to this group. The addresses (IP) of the various senders within a group are called the source (addresses). Several senders (with different IP addresses) can therefore transmit to the same multicast group, leading to a 1-to-n relationship between groups and source addresses. This information is forwarded to the router by means of reports. In the case of incoming multicast data traffic, a router can use this information to decide whether a host in its subnet wants to receive it. Your device supports the current version IGMP V3, which is upwardly compatible, which means that both V3 and V1/V2 hosts can be managed.

Your device supports the following multicast mechanisms:

- Forwarding: This relates to static forwarding, i.e. incoming data traffic for a group is passed in all cases. This is a useful option if multicast data traffic is to be permanently passed.
- IGMP: IGMP is used to gather information about the potential recipients in a subnet. In the case of a hop, incoming multicast data traffic can thus be selected.



Tip

With multicast, the focus is on excluding data traffic from unwanted multicast groups. Note that if forwarding is combined with IGMP, the packets can be forwarded to the groups specified in the forwarding request.

16.1 General

16.1.1 General

In the **Multicast->General->General** menu you can disable or enable the multicast function.

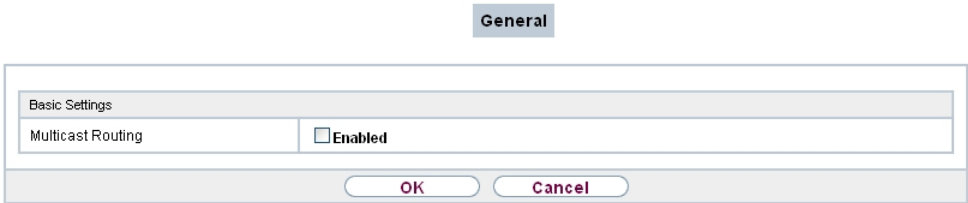


Fig. 114: **Multicast->General->General**

The **Multicast->General->General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Multicast Routing	Select whether Multicast Routing should be used. The function is enabled with <i>Enabled</i> . The function is disabled by default.

16.2 IGMP

IGMP (Internet Group Management Protocol, see RFC 3376) is used to signal the information about group (membership) in a subnet. As a result, only the packets explicitly wanted by a host enter the subnet.

Special mechanisms ensure that the requirements of the individual clients are taken into consideration. At the moment there are three versions of IGMP (V1 - V3); most current systems use V3, and less often V2.


Two packet types play a central role in IGMP: queries and reports.

Queries are only transmitted from a router. If several IGMP routers exist in a network, the router with the lowest IP address is the "querier". We differentiate here between a general query (sent to 224.0.0.1), a group-specific query (sent to a group address) and the group-and-source-specific query (sent to a specific group address). Reports are only sent by hosts to respond to queries.

16.2.1 IGMP

In this menu, you configure the interfaces on which IGMP is to be enabled.

16.2.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure IGMP on other interfaces.

IGMPOptions

IGMP Settings

Interface	None
Query Interval	125Seconds
Maximum Response Time	10,0Seconds
Robustness	2
Last Member Query Interval	1,0Seconds
IGMP State Limit	0Messages per Second
Mode	<input type="radio"/> Host <input checked="" type="radio"/> Routing

Advanced Settings

IGMP Proxy	<input type="checkbox"/> Enabled
------------	----------------------------------

OKCancel

Fig. 115: Multicast->IGMP->IGMP->New

The **Multicast->IGMP->IGMP->New** menu consists of the following fields:

Fields in the IGMP Settings menu.

Field	Description
Interface	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values are 0 to 600. The default value is 125.
Maximum Response	For the sending of queries, enter the time interval in seconds

Field	Description
Time	<p>within which hosts must respond. The hosts randomly select a time delay from this interval before sending the response. This spreads the load in networks with several hosts, improving performance.</p> <p>Possible values are <i>0,0</i> to <i>25,0</i>.</p> <p>The default value is <i>10,0</i>.</p>
Robustness	<p>Select the multiplier for controlling the timer values. A higher value can e.g. compensate for packet loss in a network susceptible to loss. If the value is too high, however, the time between logging off and stopping of the data traffic can be increased (leave latency).</p> <p>Possible values are <i>2</i> to <i>8</i>.</p> <p>The default value is <i>2</i>.</p>
Last Member Query Interval	<p>Define the time after a query for which the router waits for an answer.</p> <p>If you shorten the interval, it will be more quickly detected that the last member has left a group so that no more packets for this group should be forwarded to this interface.</p> <p>Possible values are <i>0,0</i> to <i>25,0</i>.</p> <p>The default value is <i>1,0</i>.</p>
IGMP State Limit	<p>Limit the number of reports/queries per second for the selected interface.</p>
Mode	<p>Specify whether the interface defined here only works in host mode or in both host mode and routing mode.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Routing</i> (default value): The interface is operated in Routing mode.• <i>Host</i>: The interface is only operated in host mode.

IGMP Proxy

IGMP Proxy enables you to simulate several locally connected interfaces as a subnet to an adjacent router. Queries coming in to the IGMP Proxy interface are forwarded to the local subnets. Local reports are forwarded on the IPGM Proxy interface.

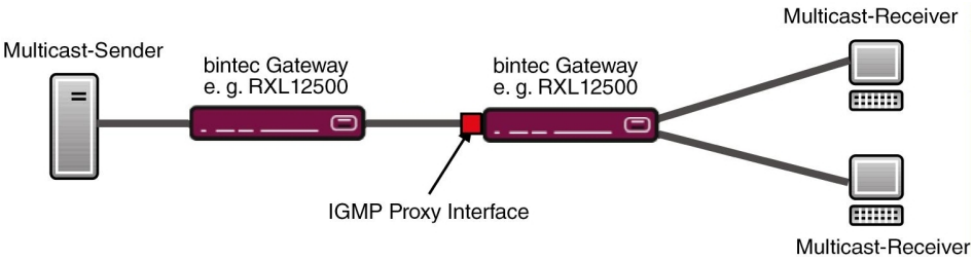


Fig. 116: IGMP Proxy

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
IGMP Proxy	Select whether your device is to forward the hosts' IGMP messages in the subnet via its defined Proxy Interface .
Proxy Interface	Only for IGMP Proxy = enabled Select the interface on your device via which queries are to be received and collected.

16.2.2 Options

In this menu, you can enable and disable IGMP on your system. You can also define whether IGMP is to be used in compatibility mode or only IGMP V3 hosts are to be accepted.

IGMP

Options

Basic Settings

IGMP Status	<div><div><input type="radio"/> Up</div><div><input type="radio"/> Down</div><div><input checked="" type="radio"/> Auto</div></div>
Mode	<div><div><input checked="" type="radio"/> Compatibility Mode</div><div><input type="radio"/> Version 3 only</div></div>
Maximum Groups	<div><div>64</div></div>
Maximum Sources	<div><div>64</div></div>
IGMP State Limit	<div><div>0</div><div>Messages per Second</div></div>

OK

Cancel

Fig. 117: Multicast->IGMP->Options

The **Multicast->IGMP->Options** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
IGMP Status	<p>Select the IGMP status.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Auto</i> (default value): Multicast is activated automatically for hosts if the hosts open applications that use multicast.• <i>Up</i>: Multicast is always on.• <i>Down</i>: Multicast is always off.
Mode	<p>Only for IGMP Status = <i>Up</i> or <i>Auto</i></p> <p>Select Multicast Mode.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Compatibility Mode</i> (default value): The router uses IGMP version 3. If it notices a lower version in the network, it uses the lowest version it could detect.• <i>Version 3 only</i>: Only IGMP version 3 is used.
Maximum Groups	<p>Enter the maximum number of groups to be permitted, both internally and in reports.</p>
Maximum Sources	<p>Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed sources per group.</p>

Field	Description
IGMP State Limit	<p>Enter the maximum permitted total number of incoming queries and messages per second.</p> <p>The default value is 0, i.e. the number of IGMP status messages is not limited.</p>

16.3 Forwarding

16.3.1 Forwarding

In this menu, you specify which multicast groups are always passed between the interfaces of your device.

16.3.1.1 New

Choose the **New** button to create forwarding rules for new multicast groups.

Forwarding

Basic Parameters

All Multicast Groups	<input type="checkbox"/> Enabled
Multicast Group Address	<input type="text"/>
Source Interface	None
Destination Interface	None

OKCancel

Fig. 118: Multicast->Forwarding->Forwarding->New

The **Multicast->Forwarding->Forwarding->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
All Multicast Groups	<p>Select whether all multicast groups, i.e. the complete multicast address range 224.0.0.0/4, are to be forwarded from the defined Source Interface to the defined Destination Interface. To do this, check <i>Enabled</i></p> <p>Disable the option if you only want to forward one defined multicast group to a particular interface.</p>

Field	Description
	The option is deactivated by default.
Multicast Group Address	Only for All Multicast Groups = not active. Enter here the address of the multicast group you want to forward from a defined Source Interface to a defined Destination Interface .
Source Interface	Select the interface on your device to which the selected multicast group is sent.
Destination Interface	Select the interface on your device to which the selected multicast group is to be forwarded.

16.4 PIM

Protocol Independent Multicast (PIM) is a multicast-routing process that makes possible dynamic routing from multicast packets. With PIM the distribution of information is regulated via a central point, which is known as the rendezvous point. Data packets are initially routed here before being made available to other recipient routers.

Multicast routing protocols differentiates between sparse mode and dense mode. In dense mode, all packets are forwarded and only packets to groups that have been explicitly cancelled are rejected. In sparse mode, packets are only forward to groups if they have been ordered. Your device uses PIM in sparse mode.

16.4.1 PIM Interfaces

A list of all PIM interfaces is displayed in the **Multicast->PIM->PIM Interfaces** menu.

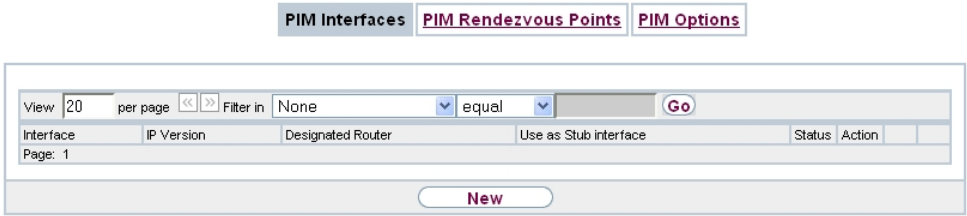



Fig. 119: Multicast->PIM->PIM Interfaces

16.4.1.1 Edit or New

Choose the  icon to edit existing entries. To configure PIM lists, select the **New** button.

PIM InterfacesPIM Rendezvous PointsPIM Options

PIM Interface Settings

Interface	Select one ▾	
PIM Mode	Sparse Mode	
Use as Stub interface	<input type="checkbox"/> Enabled	
Designated Router Priority	1	

Advanced Settings

Hello Interval	30	Seconds
Triggered Hello Interval	5	Seconds
Hello Hold Time	105	Seconds
Join/Prune Interval	60	Seconds
Join/Prune Hold Time	210	Seconds
Propagation Delay	1	Seconds
Override Interval	3	Seconds

OKCancel

Fig. 120: Multicast->PIM->PIM Interfaces->New

The **Multicast->PIM->PIM Interfaces->New** menu consists of the following fields:

Fields in the PIM Interface Settings menu.

Field	Description
Interface	Choose the interface used for PIM, i.e. over which multicast routing is operated.
PIM Mode	Indicates the mode to be used for PIM. Your device uses PIM in sparse mode. The entry cannot be changed.
Use as Stub interface	<p>Determine whether or not the interface is used for PIM data packets. This parameter allows you to use an interface for IG-MP, for example, whilst preventing (fake) PIM messages.</p> <p>If this function is deactivated (default value), the PIM data packets for this interface are blocked.</p> <p>If the function is active, the interface for the PIM data packets</p>

Field	Description
	are released.
Designated Router Priority	<p>Define the value of the designated router priority entered in the Designated Router Priority option.</p> <p>The higher the value, the greater the probability that the corresponding router will be used as the designated router.</p> <p>The default value is <i>1</i>.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Hello Interval	<p>Define the interval (in seconds) at which PIM Hello messages are sent over this interface.</p> <p>The value <i>0</i> means that no PIM Hello messages are sent on this interface.</p> <p>Possible values: <i>0</i> to <i>18000</i> seconds.</p> <p>The default value is <i>30</i>.</p>
Triggered Hello Interval	<p>Define the maximum waiting time until a PIM Hello message is sent after a system boot or after a reboot of a neighbour.</p> <p>The value <i>0</i> means that PIM Hello messages are always sent straight away.</p> <p>Possible values: <i>0</i> to <i>60</i> seconds.</p> <p>The default value is <i>5</i>.</p>
Hello Hold Time	<p>Define the value of the holdtime field in a PIM Hello message.</p> <p>This indicates how long a PIM route is available. As soon as the Hello Hold Time has expired and no other Hello messages have been received, the PIM router will be classed as unavailable.</p> <p>Possible values: <i>0</i> to <i>65535</i> seconds.</p> <p>The default value is <i>105</i>.</p>

Field	Description
Join/Prune Interval	<p>Define the frequency at which the PIM Join/Prune messages are sent on the interface.</p> <p>The value <i>0</i> means that no periodic PIM Join/Prune messages are sent on this interface.</p> <p>Possible values: <i>0</i> to <i>18000</i> seconds.</p> <p>The default value is <i>60</i>.</p>
Join/Prune Hold Time	<p>Define the value entered in the holdtime field of a PIM Join/Prune message.</p> <p>This is the time for which a recipient must maintain the Join/Prune state.</p> <p>Possible values: <i>0</i> to <i>65535</i> seconds.</p> <p>The default value is <i>210</i>.</p>
Propagation Delay	<p>Define the value entered in the Propagation Delay field. This field is part of the LAN Prune Delay option in the PIM Hello messages, which are sent on this interface.</p> <p>Propagation Delay and Override Interval represent the so-called LAN-Prune-Delay settings. These result in a delay in processing prune messages for upstream routers.</p> <p>If the Propagation Delay is too short, the transfer of multicast packets may be cancelled before a downstream router has sent a prune override message.</p> <p>Possible values: <i>0</i> to <i>32</i> seconds.</p> <p>The default value is <i>1</i>.</p>
Override Interval	<p>Define the value that the gateway enters in the Override_Interval field for the LAN Prune Delay option.</p> <p>Override Interval defines the maximum time a downstream router can wait until sending a prune override message.</p> <p>Possible values: <i>0</i> to <i>65</i> seconds.</p> <p>The default value is <i>3</i>.</p>

16.4.2 PIM Rendezvous Points

In menu **Multicast->PIM->PIM Rendezvous Points** you determine which Rendezvous Point is responsible for which group.

A list of all PIM Rendezvous Points is displayed.

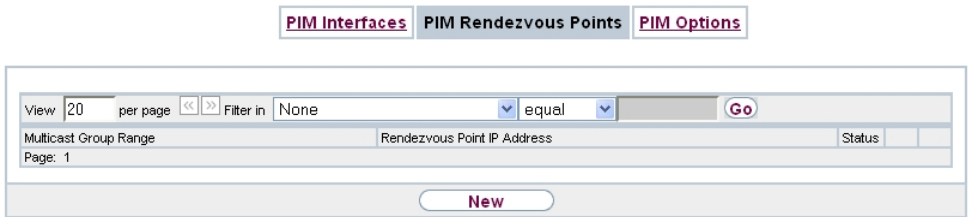



Fig. 121: Multicast->PIM->PIM Rendezvous Points

16.4.2.1 Edit or New

Choose the  icon to edit existing entries. To configure PIM Rendezvous Points, select the **New** button.

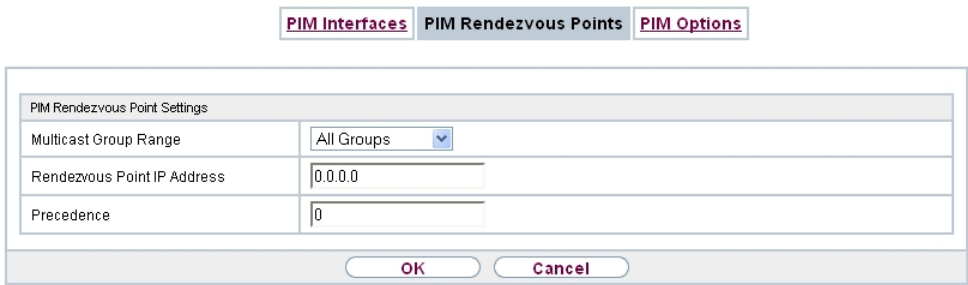


Fig. 122: Multicast->PIM->PIM Rendezvous Points->New

The **Multicast->PIM->PIM Rendezvous Points->New** menu consists of the following fields:

Fields in the PIM Rendezvous Point Settings menu.

Field	Description
Multicast Group Range	Select the Multicast group for the PIM Rendezvouz point. You can enter <i>All Groups</i> (default value), or specify a multicast network segment by selecting <i>Specific Range</i> .
Multicast Group Ad- dress	Only if Multicast Group Range = <i>Specific Range</i>

Field	Description
	Here you enter the IP address of the multicast network segment.
Multicast Group Prefix Length	<p>Only if Multicast Group Range = <i>Specific Range</i></p> <p>Here you enter the network mask length of the multicast network segment.</p> <p>224.0.0.0/4 indicates the entire multicast class D segment.</p> <p>Possible values: 4 (default value) to 32.</p>
Rendezvous Point IP Address	Enter the IP address or the hostname of the rendezvous points.
Precedence	<p>Enter the value for pimGroupMappingPrecedence to be used for static RP configurations. This allows precise control over which configuration is to be replaced by this static configuration.</p> <p>When the function is activated pimStaticRPOVERRIDEdynamic is ignored. The absolute values of this object are only significant on the local router and need not be synchronised with other routers.</p> <p>The function is deactivated with the default value 0. If the function is not activated by setting a value not 0, this can have different consequences for other routers. Hence, avoid using this function if exact control of the behaviour of the static RP is not required.</p>

16.4.3 PIM Options

PIM InterfacesPIM Rendezvous PointsPIM Options

Basic Settings

PIM Status

☐Enabled

Keepalive Period

210

Seconds

Register Suppression Timer

60

Seconds

OK

Cancel

Fig. 123: Multicast->PIM->PIM Options

The **Multicast->PIM->PIM Options** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
PIM Status	<p>Select whether PIM should be activated. The function is activated by selecting <i>Enable</i>.</p> <p>The function is disabled by default.</p>
Keepalive Period	<p>Enter the interval in seconds within which a KeepAlive message must be sent.</p> <p>Possible values: <i>0</i> to <i>65535</i>.</p> <p>The default value is <i>210</i>.</p>
Register Suppression Timer	<p>Enter the time in seconds after which a PIM Designated Router (DR) should no longer send any register-encapsulated data to the Rendezvous Point (RP) once the Register-Stop-Message has been received. This object is used to employ timers at the DR as well as at the RP. This timespan is named Register_Suppression_Time in the PIM-SM specification.</p> <p>Possible values: <i>0</i> to <i>65535</i>.</p> <p>The default value is <i>60</i>.</p>

Chapter 17 WAN

This menu offers various options for configuring accesses or connections from your LAN to the WAN. You can also optimise voice transmission here for telephone calls over the Internet.

17.1 Internet + Dialup

In this menu, you can set up Internet access or dialup connections.

In addition, you can create address pools for the dynamic assignment of IP addresses.

To enable your device to set up connections to networks or hosts outside your LAN, you must configure the partners you want to connect to on your device. This applies to outgoing connections (your device dials its WAN partner) and incoming connections (a remote partner dials the number of your device).

If you want to set up Internet access, you must set up a connection to your Internet Service Provider (ISP). For broadband Internet access, your device provides the PPP-over-Ethernet (PPPoE), PPP-over-PPTP and PPP-over-ATM (PPPoA) protocols. You can also configure Internet access over ISDN.



Note




Note your provider's instructions.


Dialin connections over ISDN are used to establish a connection to networks or hosts outside your LANs.

All the entered connections are displayed in a list, which contains the **Description**, the **User Name**, the **Authentication** and the current **Status**.

The **Status** field can have the following values:

Possible values for Status

Field	Description
	connected
	not connected (dialup connection); connection setup possible
	not connected (e.g. because of an error during setup of an outgoing connection, a renewed attempt is only possible after a

Field	Description
	specified number of seconds)
	administratively set to down (deactivated); connection setup not possible for leased lines:

Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. Access to the Internet should always be set up as the default route to the Internet Service Provider (ISP). Further information on possible route types can be found under **Networking->Routes**.

Activating NAT

With Network Address Translation (NAT), you conceal your whole network to the outside world behind one IP address. You should certainly do this for your connection to the Internet Service Provider (ISP).

Only outgoing sessions are allowed initially if NAT is activated. To allow certain connections from outside to hosts within the LAN, these must be explicitly defined and admitted.

Connection Idle Timeout

The connection idle timeout is determined in order to clear the connection automatically if it is not being used, i.e. if data is no longer being sent, to help you save costs.

Block after Connection Failure

You use this function to set up a waiting time for outgoing connection attempts after which your device's connection attempt is regarded as having failed.

Authentication

When a call is received on ISDN connections, the calling party number is always sent over the ISDN D-channel. This number enables your device to identify the caller (CLID), provided the caller is entered on your device. After identification with CLID, your device can additionally carry out PPP authentication with the connection partner before it accepts the call.

Your device needs the necessary data for this, which you should enter here, for all PPP connections. Establish the type of authentication process that should be performed, then

enter a common password and two codes. You get this information, for example, from your Internet Service Provider (ISP) or the system administrator at your head office. If the data you entered on your device is the same as the caller's data, the call is accepted. The call is rejected if the data is not the same.

Callback

The callback mechanism can be used for every connection over an ISDN or over an AUX interface to obtain additional security regarding the connection partner or to clearly allocate the costs of connections. A connection is not set up until the calling party has been clearly identified by calling back. Your device can answer an incoming call with a callback or request a callback from a connection partner. Identification can be based on the calling party number or PAP/CHAP/MS-CHAP authentication. Identification is made in the former case without call acceptance, as the calling party number is transferred over the ISDN D-channel, and in the latter case with call acceptance.

Channel Bundling

Your device supports dynamic and static channel bundling for dialup connections. Channel bundling can only be used for ISDN connections for a bandwidth increase or as a backup. Only one B-channel is initially opened when a connection is set up.

Dynamic

Dynamic channel bundling means that your device connects other ISDN B-channels to increase the throughput for connections if this is required, e.g. for large data rates. If the amount of data traffic drops, the additional B-channels are closed again.

If devices from other manufacturers are to be used at the far end, ensure that these support dynamic channel bundling for a bandwidth increase or as a backup.

Static

In static channel bundling, you specify right from the start how many B-channels your device is to use for connections, regardless of the transferred data rate.

17.1.1 PPPoE

A list of all PPToE interfaces is displayed in the **WAN->Internet + Dialup->PPPoE** menu.

PPP over Ethernet (PPPoE) is the use of the Point-to-Point Protocol (PPP) network protocol over an Ethernet connection. Today, PPPoE is used for ADSL connections in Germany. In Austria, the Point To Point Tunnelling Protocol (PPTP) was originally used for ADSL access. However, PPPoE is now offered here too by some providers.

17.1.1.1 New

Choose the **New** button to set up new PPPoE interfaces.

PPPoE

PPTP

PPPoA

ISDN

AUX

IP Pools

Basic Parameters	
Description	
PPPoE Mode	<input checked="" type="radio"/> Standard <input type="radio"/> Multilink
PPPoE Ethernet Interface	Select one
User Name	
Password	••••••••
Always on	<input type="checkbox"/> Enabled
Connection Idle Timeout	300 Seconds
IP Mode and Routes	
IP Address Mode	<input type="radio"/> Static <input checked="" type="radio"/> Get IP Address
Default Route	<input checked="" type="checkbox"/> Enabled
Create NAT Policy	<input checked="" type="checkbox"/> Enabled

Advanced Settings

Block after connection failure for	60 Seconds
Maximum Number of Dialup Retries	5
Authentication	PAP
DNS Negotiation	<input checked="" type="checkbox"/> Enabled
Prioritize TCP ACK Packets	<input type="checkbox"/> Enabled
LCP Alive Check	<input checked="" type="checkbox"/> Enabled
MTU	<input checked="" type="checkbox"/> Automatic

OK

Cancel

Fig. 124: WAN->Internet + Dialup->PPPoE->New

The menu **WAN->Internet + Dialup->PPPoE->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number No special characters or umlauts must be used.
PPPoE Mode	Select whether you want to use a standard Internet connection over PPPoE (<i>standard</i>) or your Internet access is to be set

Field	Description
	<p>up over several interfaces (<i>Multilink</i>). If you choose <i>Multilink</i>, you can connect several DSL connections from a provider over PPP as a static bundle in order to obtain more bandwidth. Each of these DSL connections should use a separate Ethernet connection for this. At the moment, many providers are still in the process of preparing the PPPoE Multilink function.</p> <p>For PPPoE Multilink, we recommend using your device's Ethernet switch in Split-Port mode and to use a separate Ethernet interface e.g. <i>en1-1</i>, <i>en1-2</i> for each PPPoE connection.</p> <p>If you also want to use an external modem for PPPoE Multilink, you must run your device's Ethernet switch in Split-Port mode.</p>
PPPoE Ethernet Interface	<p>Only for PPPoE Mode = <i>Standard</i></p> <p>Select the Ethernet interface specified for a standard PPPoE connection.</p> <p>If you want to use an external DSL modem, select the Ethernet port to which the modem is connected.</p> <p>When using the internal DSL modem, select here the EthoA interface configured in WAN->ATM->Profiles->New.</p>
PPPoE Interfaces for Multilink	<p>Only for PPPoE Mode = <i>Multilink</i></p> <p>Select the interfaces you want to use for your Internet connection. Click the Add button to create new entries.</p>
User Name	Enter the user name.
Password	Enter the password.
VLAN	Certain Internet service providers require a VLAN-ID. Activate this function to be able to enter a value under VLAN ID .
VLAN ID	<p>Only if VLAN is enabled.</p> <p>Enter the VLAN-ID that you received from your provider.</p>
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Field	Description
	Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are 0 to 3600 (seconds). 0 deactivates the short hold.</p> <p>The default value is 300.</p> <p>Example: 10 for FTP transmission, 20 for LAN-to-LAN transmission, 90 for Internet connections.</p>

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.• <i>Static</i>: You enter a static IP address.
Default Route	<p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Create NAT Policy	<p>Specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Field	Description
Local IP Address	Only if IP Address Mode = <i>Static</i> Enter the static IP address of the connection partner.
Route Entries	Only if IP Address Mode = <i>Static</i> Define other routing entries for this connection partner. Add new entries with Add . <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or network. • <i>Netmask</i>: Netmask for Remote IP Address. If no entry is made, your device uses a default netmask. • <i>Metric</i>: The lower the value, the higher the priority of the route (range of values <i>0... 15</i>). The default value is <i>1</i>.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is <i>60</i> .
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are <i>0</i> to <i>100</i> . The default value is <i>5</i> .
Authentication	Select the authentication protocol for this connection partner. Select the authentication specified by your provider. Possible values: <ul style="list-style-type: none"> • <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.

Field	Description
	<ul style="list-style-type: none">• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).• <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.)• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.• <i>None</i>: Some providers use no authentication. In this case, select this option.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the connection partner or sends these to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
MTU	<p>Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the connection.</p> <p>With default value <i>Automatic</i>, the value is specified by link control at connection setup.</p> <p>If you disable <i>Automatic</i>, you can enter a value.</p> <p>Possible values are <i>1</i> to <i>8192</i>.</p>

Field	Description
	The default value is 0.

17.1.2 PPTP

A list of all PPTP interfaces is displayed in the **WAN->Internet + Dialup->PPTP** menu.

In this menu, you configure an Internet connection that uses the Point Tunnelling Protocol (PPTP) to set up a connection. This is required in Austria, for example.

17.1.2.1 New

Choose the **New** button to set up new PPTP interfaces.

PPPoE

PPTP

PPPoA

IP Pools

Basic Parameters

Description

PPTP Ethernet Interface

Select one

User Name

Password

••••••••

Always on

☐ Enabled

Connection Idle Timeout

300

Seconds

IP Mode and Routes

IP Address Mode

☐ Static ☒ Get IP Address

Default Route

☒ Enabled

Create NAT Policy

☒ Enabled

Advanced Settings

Block after connection failure for

60

Seconds

Maximum Number of Dialup Retries

5

Authentication

PAP

DNS Negotiation

☒ Enabled

Prioritize TCP ACK Packets

☐ Enabled

PPTP Address Mode

Static

Local PPTP IP Address

10.0.0.140

Remote PPTP IP Address

10.0.0.138

LCP Alive Check

☒ Enabled

OK

Cancel

Fig. 125: **WAN->Internet + Dialup->PPTP->New**

The menu **WAN->Internet + Dialup->PPTP->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	<p>Enter a name for uniquely identifying the internet connection.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used.</p>
PPTP Ethernet Interface	<p>Select the IP interface over which packets are to be transported to the remote PPTP terminal.</p> <p>If you want to use an external DSL modem, select the Ethernet port to which the modem is connected.</p> <p>When using the internal DSL modem, select here the EthoA interface configured in Physical Interfaces->ATM->Profiles->New, e.g. <i>ethoa50-0</i>.</p>
User Name	Enter the user name.
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Only activate this option if you have Internet access with a flat-rate charge.</p>
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the timeout.</p> <p>The default value is <i>300</i>.</p> <p>Example: <i>10</i> for FTP transmission, <i>20</i> for LAN-to-LAN transmission, <i>90</i> for Internet connections.</p>

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Get IP Address</i> (default value): Your device is automatically assigned a temporarily valid IP address from the provider. • <i>Static</i>: You enter a static IP address.
Default Route	<p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Create NAT Policy	<p>Specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Local IP Address	<p>Only for IP Address Mode = <i>Static</i></p> <p>Assign an IP address from your LAN to the PPT interface, which is to be used as your device's internal source address.</p>
Route Entries	<p>Only if IP Address Mode = <i>Static</i></p> <p>Define other routing entries for this PPTP partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none"> • <i>Remote IP Address</i>: IP address of the destination host or network. • <i>Netmask</i>: Netmask for Remote IP Address. If no entry is made, your device uses a default netmask. • <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is <i>60</i> .
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are <i>0</i> to <i>100</i> . The default value is <i>5</i> .
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: <ul style="list-style-type: none">• <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).• <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.)• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.• <i>None</i>: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the connection partner or sends these to the connection partner. The function is enabled with <i>Enabled</i> . The function is enabled by default.
Prioritize TCP ACK	Select whether the TCP download is to be optimised in the

Field	Description
Packets	<p>event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
PPTP Address Mode	<p>Displays the address mode. The value cannot be changed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Static</i>: The Local PPTP IP Address will be assigned to the selected Ethernet port.
Local PPTP IP Address	<p>Assign the PPTP interface an IP address that is used as the source address.</p> <p>The default value is <i>10.0.0.140</i>.</p>
Remote PPTP IP Address	<p>Enter the IP address of the PPTP partner.</p> <p>The default value is <i>10.0.0.138</i>.</p>
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

17.1.3 UMTS/LTE



Note

Please note that the **UMTS/LTE** menu is only available for devices with an integrated UMTS/HSDPA modem, or with devices supporting the use of a UMTS/HSDPA/LTE USB stick!

A list of all configured GPRS/UMTS/LTE connections is displayed in the **WAN->Internet + Dialup->UMTS/LTE** menu.

With mobile standards GPRS, UMTS and LTE, you can establish an internet connection via the mobile network.

17.1.3.1 New

Choose the **New** button to create additional connections.

PPPoE

PPTP

UMTS/LTE

IP Pools

Basic Parameters

Description

UMTS/LTE Interface

UMTS-6-0

User Name

Password

Always on

☐ Enabled

Connection Idle Timeout

300

Seconds

IP Mode and Routes

IP Address Mode

☐ Static ☒ Get IP Address

Default Route

☒ Enabled

Create NAT Policy

☒ Enabled

Advanced Settings

Block after connection failure for

60

Seconds

Maximum Number of Dialup Retries

5

Authentication

PAP

DNS Negotiation

☒ Enabled

Prioritize TCP ACK Packets

☐ Enabled

LCP Alive Check

☒ Enabled

OK

Cancel

Fig. 126: WAN->Internet + Dialup->UMTS/LTE->New

The **WAN->Internet + Dialup->UMTS/LTE->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the internet connection. The first character in this field must not be a number No special characters or umlauts must be used.
UMTS/LTE Interface	Select the UMTS/LTE interface. In RS120wu the integrated modem with slot 6 unit 0 UMTS is preselected; for devices with an

Field	Description
	optional plug-in UMTS/LTE stick the USB port of the device is preselected.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with <i>Enabled</i> . The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if Always on is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the short hold. The default value is <i>300</i> .

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: <ul style="list-style-type: none">• <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.• <i>Static</i>: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with <i>Enabled</i> . The function is enabled by default.

Field	Description
Create NAT Policy	<p>Specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Local IP Address	<p>Only if IP Address Mode = <i>Static</i></p> <p>Enter the static IP address of the connection partner.</p>
Route Entries	<p>Only if IP Address Mode = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none">• <i>Remote IP Address</i>: IP address of the destination host or network.• <i>Netmask</i>: Netmask for Remote IP Address If no entry is made, your device uses a default netmask.• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values <i>0... 15</i>). The default value is <i>1</i>.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is <i>60</i>.</p>
Maximum Number of Dialup Retries	<p>Enter the number of unsuccessful attempts to setup a connection before the interface is blocked.</p> <p>Possible values are <i>0 to 100</i>.</p> <p>The default value is <i>5</i>.</p>
Authentication	<p>Select the authentication protocol for this connection partner. Select the authentication specified by your provider.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>PAP</i> (default value): Only run <i>PAP</i> (PPP Password Authentication Protocol); the password is transferred unencrypted.• <i>CHAP</i>: Only run <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).• <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.)• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.• <i>None</i>: Some providers use no authentication. In this case, select this option.
DNS Negotiation	<p>Select whether your device receives IP addresses for DNS Serverprimary domain name serverPrimary and DNS Serversecondary domain name serverSecondary from the connection partner or sends these to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

17.1.4 AUX

In the **WAN->Internet + Dialup->AUX** menu, a list of all AUX interfaces is displayed.

You can define various settings for communication between the gateway and modem in this menu. You require a special cable for the console port of your gateway (e.g. AUX Backup cable) to connect an external analogue modem to the AUX port on a bintec elmeg gateway.

17.1.4.1 New

Choose the **New** button to set up new AUX interfaces.

PPPoE

PPTP

ISDN

AUX

IP Pools

Basic Parameters

Description

User Name

Password

••••••••

Always on

☐ Enabled

Connection Idle Timeout

600

Seconds

IP Mode and Routes

IP Address Mode

☐ Static ☐ Provide IP Address ☒ Get IP Address

Default Route

☒ Enabled

Create NAT Policy

☒ Enabled

Advanced Settings

Block after connection failure for

50

Seconds

Maximum Number of Dialup Retries

5

Usage Type

☒ Standard ☐ Dialin only ☐ Multi-User (Dialin only)

Authentication

PAP

DNS Negotiation

☒ Enabled

Prioritize TCP ACK Packets

☐ Enabled

LCP Alive Check

☒ Enabled

Callback Mode

☒ None ☐ Active ☐ Passive

Dial Numbers

Entries

Mode

Number

Add

IP Options

Proxy ARP Mode

☒ Inactive ☐ Up or Dormant ☐ Up only

OK

Cancel

Fig. 127: WAN->Internet + Dialup->AUX->New

The **WAN->Internet + Dialup->AUX->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the WAN partner. The first character in this field must not be a number No special characters or umlauts must be used.

306

bintec RV Series

Field	Description
User Name	Enter the user name.
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Only activate this option if you have Internet access with a flat-rate charge.</p>
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the short hold.</p> <p>The default value is <i>600</i>.</p>

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically or whether it should be assigned this dynamically at the remote terminal.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.• <i>Static</i>: You enter a static IP address.• <i>Provide IP Address</i>: Your device dynamically assigns an IP address to the remote terminal.
Default Route	<p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p>

Field	Description
	The function is enabled by default.
Create NAT Policy	<p>Specify whether Network Address Translation (NAT) is to be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Local IP Address	<p>Only if IP Address Mode = <i>Static</i></p> <p>Enter the static IP address of the connection partner.</p>
Route Entries	<p>Only if IP Address Mode = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none">• <i>Remote IP Address</i>: IP address of the destination host or network.• <i>Netmask</i>: Netmask for Remote IP Address If no entry is made, your device uses a default netmask.• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values <i>0... 15</i>). The default value is <i>1</i>.
IP Assignment Pool	<p>Only if IP Address Mode = <i>Provide IP Address</i></p> <p>Select IP pools configured in the WAN->Internet + Dialup->IP Pools menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed.</p> <p>The default value is <i>50</i>.</p>
Maximum Number of Dialup Retries	<p>Enter the number of unsuccessful attempts to setup a connection before the interface is blocked.</p>

Field	Description
	<p>Possible values are <i>0</i> to <i>100</i>.</p> <p>The default value is <i>5</i>.</p>
Usage Type	<p>If necessary, select a special interface use.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Standard</i> (default value): No special type is selected.• <i>Dialin only</i>: The interface is used for incoming dialup connections and callbacks initiated externally.• <i>Multi-User (Dialin only)</i> : The interface is defined as multi-user connection partner, i.e. several clients dial in with the same user name and password.
Authentication	<p>Select the authentication protocol for this PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>PAP/CHAP/MS-CHAP</i>: Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.)• <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.• <i>None</i>: Some providers use no authentication. In this case, select this option.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the connection partner or sends these to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Field	Description
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This makes it possible to switch to a backup connection more quickly in the event of line faults.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Callback Mode	<p>Select the Callback Mode function.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): Your device does not call back. • <i>Active</i>: Select one of the following options: <ul style="list-style-type: none"> • <i>No PPP negotiation</i>: Your device calls the connection partner to request a callback. • <i>Windows Client Mode</i>: Your device calls the connection partner to request a callback via CBCP (Callback Control Protocol). Needed for Windows clients. • <i>Passive</i>: Select one of the following options: <ul style="list-style-type: none"> • <i>PPP Negotiation or CLID</i>: Your device calls back immediately when requested to do so by the connection partner. • <i>Windows Server Mode</i>: Your device calls back after a period of time suggested by the Microsoft client (NT: 10 seconds, new systems: 12 seconds. It uses the call number (Entries->Number) with the Mode <i>Outgoing</i> or <i>Both</i> entered for the connection partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. This setting should be avoided where possible for security reasons. Currently cannot be avoided for the connection of mobile Microsoft clients via DCN. • <i>Delayed, CLID only</i>: Your device calls back after ap-

Field	Description
	<p>prox. four seconds if your device is requested to do so by the connection partner. Only makes sense for CLID.</p> <ul style="list-style-type: none">• <i>Windows Server Mode, Callback optional</i>: like <i>Windows Server Mode</i> with the option of termination. This setting should be avoided for security reasons. The Microsoft client also has the option of aborting callback and maintaining the initial connection to your device without callback. This only applies if no fixed, outgoing number has been configured for the connection partner. This is done by pressing CANCEL to close the dialog box that appears.

Fields in the Dial Numbers menu.

Field	Description
Entries	Add new entries with Add .

Fields in the menu **Dial Number Configuration** entry: <1> (only appears for Entries = Add

Field	Description
Mode	<p>Only if Entries = <i>Add</i></p> <p>Defines whether Number should be used for incoming or outgoing calls or for both. Possible values:</p> <ul style="list-style-type: none">• <i>Both</i> (default value): For incoming and outgoing calls.• <i>Incoming</i>: For incoming calls, where your connection partner dials in to your device.• <i>Outgoing</i>: For outgoing calls, where you dial your connection partner. <p>The calling party number of the incoming call is compared with the number entered under Number.</p>
Call Number	Enter the connection partner's numbers.

Fields in the IP Options menu.

Field	Description
Proxy ARP Mode	<p>Select whether and how ARP requests from your own LAN are to be responded to for the specified connection partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Inactive</i> (default value): Deactivates Proxy ARP for this

Field	Description
	<p>connection partner.</p> <ul style="list-style-type: none"> • <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the connection partner is <i>Up</i> or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the connection partner is <i>Up</i>, i.e. a connection already exists to the connection partner.


17.1.5 IP Pools

The **IP Pools** menu displays a list of all IP pools.

Your device can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means that, if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address that was assigned to this partner the previous time.

17.1.5.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

PPPoE

PPTP

PPPoA

ISDN

IP Pools

Basic Parameters

IP Pool Name

IP Address Range

-

DNS Server

Primary

Secondary

OK

Cancel

Fig. 128: WAN->Internet + Dialup->IP Pools->New

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. Secondary: Optionally, enter the IP address of an alternative DNS server.

17.2 Leased Line

A leased line is a permanent (fixed) connection between two communication partners via a telecommunications network. Unlike a switched line, the entire transmission channels is always available. The leased line cannot be set up by the subscriber by dialling and therefore has no call number. The connection must be set up by the network operator.

17.2.1 Interfaces


In the **WAN->Leased Line->Interfaces** menu, a list of all is displayed. Automatic generation requires the corresponding ISDN interface to be configured.

Interfaces

Autogenerated from BRI (ISDN-S0)						
Description	Type	Protocol	Port	Status	Action	
bri2-0-1	Leased Line B1 64S	PPP	bri2-0			
Autogenerated from PRI (ISDN-S2M)						
Description	Type	Protocol	Port	Status	Action	
pri2-4-0	Leased Line, 1 Hyperchannel (G.703 + G.704)	PPP	pri2-4			

Fig. 129: **WAN->Leased Line->Interfaces**

17.2.1.1 Edit

Choose the  button to edit the configuration of the corresponding leased line for a BRI interface.

Interfaces

Basic Parameters

Description

IP Mode and Routes

Default Route

☐ Enabled

Local IP Address

Route Entries

Remote IP Address

Netmask

Metric

1

Add

Advanced Settings

LCP Alive Check

☒ Enabled

Prioritize TCP ACK Packets

☐ Enabled

Compression

☒ None ☐ STAC ☐ MS-STAC ☐ MPPC

IP Options

OSPF Mode


☒ Passive ☐ Active ☐ Inactive

Proxy ARP Mode

☒ Inactive ☐ Up or Dormant ☐ Up only

OK

Cancel

Fig. 130: WAN->Leased Line->Interfaces->Autogenerated from BRI (ISDN-S0)->

The WAN->Leased Line->Interfaces->Autogenerated from BRI (ISDN-S0)-> menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description for the connection.

Fields in the IP Mode and Routes menu.

Field	Description
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with <i>Enabled</i> . The function is disabled by default.

Field	Description
Local IP Address	Enter the IP address you received from your network operator.
Route Entries	Define other routing entries for this connection class. Add new entries with Add .

The menu **Advanced Settings** consists of the following fields:


Fields in the Advanced Settings menu.

Field	Description
LCP Alive Check	Select whether the reachability of the remote terminal is to be checked. The function is enabled with <i>Enabled</i> . The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. The function is enabled with <i>Enabled</i> . The function is disabled by default.
Compression	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: <ul style="list-style-type: none">• <i>None</i> (default value): Encryption is not used.• <i>STAC</i>• <i>MS-STAC</i>• <i>MPPC</i>: Microsoft Point-to-Point Compression

Fields in the IP Options menu.

Field	Description
OSPF Mode	Specify whether OSPF protocol packets are sent over the interface. Possible values:

Field	Description
	<ul style="list-style-type: none">• <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces.• <i>Active</i>: OSPF is not activated for this interface, i.e. OSPF protocol packets sent over this interface.• <i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	<p>Select whether and how ARP requests are to be responded to for the specified connection partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Inactive</i> (default value): Deactivates Proxy ARP for this connection partner.• <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the connection partner is <i>Up</i> or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.• <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the connection partner is <i>Up</i> , i.e. a connection already exists to the connection partner.

Choose the  button to edit the configuration of the corresponding leased line for a PRI interface.

Interfaces

Basic Parameters

Description

IP Mode and Routes

Default Route

☐ Enabled

Local IP Address

Route Entries

Remote IP Address

Netmask

Metric

1

Add

Advanced Settings

LCP Alive Check

☒ Enabled

Prioritize TCP ACK Packets

☐ Enabled

Compression

☒ None ☐ STAC ☐ MS-STAC ☐ MPPC

IP Options

OSPF Mode


☒ Passive ☐ Active ☐ Inactive

Proxy ARP Mode

☒ Inactive ☐ Up or Dormant ☐ Up only

OK

Cancel

Fig. 131: WAN->Leased Line->Interfaces->Autogenerated from PRI (ISDN-S2M)->

The WAN->Leased Line->Interfaces->Autogenerated from PRI (ISDN-S2M)-> menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description for the connection.

Fields in the IP Mode and Routes menu.

Field	Description
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with <i>Enabled</i> . The function is disabled by default.
Local IP Address	Enter the IP address you received from your network operator.
Route Entries	Define other routing entries for this connection class. Add new entries with Add .

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
LCP Alive Check	<p>Select whether the reachability of the remote terminal is to be checked.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Compression	<p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): Encryption is not used.• <i>STAC</i>• <i>MS-STAC</i>• <i>MPPC</i>: Microsoft Point-to-Point Compression

Fields in the IP Options menu.

Field	Description
OSPF Mode	<p>Specify whether OSPF protocol packets are sent over the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces.• <i>Active</i>: OSPF is not activated for this interface, i.e. OSPF

Field	Description
	protocol packets sent over this interface. <ul style="list-style-type: none"><i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether and how ARP requests are to be responded to for the specified connection partner. Possible values: <ul style="list-style-type: none"><i>Inactive</i> (default value): Deactivates Proxy ARP for this connection partner.<i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the connection partner is <i>Up</i> or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.<i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the connection partner is <i>Up</i>, i.e. a connection already exists to the connection partner.

17.3 Real Time Jitter Control

When telephoning over the Internet, voice data packets normally have the highest priority. Nevertheless, if the upstream bandwidth is low, noticeable delays in voice transmission can occur when other packets are routed at the same time.

The real time jitter control function solves this problem. So that the "line" is not blocked for too long for the voice data packets, the size of the other packets can be reduced, if required, during a telephone call.

17.3.1 Controlled Interfaces

In the **WAN->Real Time Jitter Control->Controlled Interfaces** a list of functions is displayed for which the Real Time Jitter Control function is configured.

17.3.1.1 New

Click the **New** button to optimise voice transmission for other interfaces.

Controlled Interfaces

Basic Settings

Interface

None

Control Mode

Controlled RTP Streams only

Maximum Upload Speed

0

kbps

OK

Cancel

Fig. 132: WAN->Real Time Jitter Control->Controlled Interfaces->New

The menu **WAN->Real Time Jitter Control->Controlled Interfaces->New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Interface	Define for which interfaces voice transmission is to be optimised.
Control Mode	<div>Select the mode for the optimisation.</div> <div>Possible values:</div> <ul style="list-style-type: none">Controlled RTP Streams only (default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission.All RTP Streams: All RTP streams are optimised.Inactive: Voice data transmission is not optimised.Always: Voice data transmission is always optimised.
Maximum Upload Speed	Enter the maximum available upstream bandwidth in kbp/s for the selected interface.

Chapter 18 VPN

A connection that uses the Internet as a "transport medium" but is not publicly accessible is referred to as a VPN (Virtual Private Network). Only authorised users have access to such a VPN, which is seemingly also referred to as a VPN tunnel. Normally the data transported over a VPN is encrypted.

A VPN allows field staff or staff working from home offices to access data on the company's network. Subsidiaries can also connect to head office over VPN.

Various protocols are available for creating a VPN tunnel, e.g. IPSec or PPTP.

The connection partner is authenticated with a password, using preshared keys or certificates.

With IPSec the data is encrypted using AES or 3DES, for example; with PPTP, you can use MPPE.

18.1 IPSec

IPSec enables secure connections to be set up between two locations (VPN). This enables sensitive business data to be transferred via an unsecure medium such as the Internet. The devices used function here as the endpoints of the VPN tunnel. IPSec involves a number of Internet Engineering Task Force (IETF) standards, which specify mechanisms for the protection and authentication of IP packets. IPSec offers mechanisms for encrypting and decrypting the data transferred in the IP packets. The IPSec implementation can also be smoothly integrated in a Public Key Infrastructure (PKI, see [Certificates](#) on page 97). IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

Additional Traffic Filter

bintec elmeg gateways support two different methods of setting up IPSec connections:

- a method based on policies and
- a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPSec phase 2 SAs. This allows for a very "fine-grained" filter to be applied to the IP packet, even at the level of the protocol and the port.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPSec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPSec phase 2 SAs. Although this method does simplify many configurations, problems may also be caused by competing routes or the "coarser" filtering of data traffic.

The **Additional Traffic Filter** parameter fixes this problem. You can apply a "finer" filter, i.e. you can enter the source IP address or the source port. If a **Additional Traffic Filter** is configured, this is used to negotiate the IPSec phase 2 SAs; the route now only determines which data traffic is to be routed.

If an IP packet does not match the defined **Additional Traffic Filter**, it is rejected.

If an IP packet meets the requirements in an **Additional Traffic Filter**, IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

**Note**

The parameter **Additional Traffic Filter** is exclusively relevant for the initiator of the IPSec connection, it is only used for outgoing traffic.

**Note**

Please note that the phase 2 policies must be configured identically on both of the IPSec tunnel endpoints.

18.1.1 IPSec Peers

An endpoint of a communication is defined as peer in a computer network. Each peer offers its services and uses the services of other peers.

A list of all configured IPSec Peers is displayed in the **VPN->IPSec->IPSec Peers** menu.

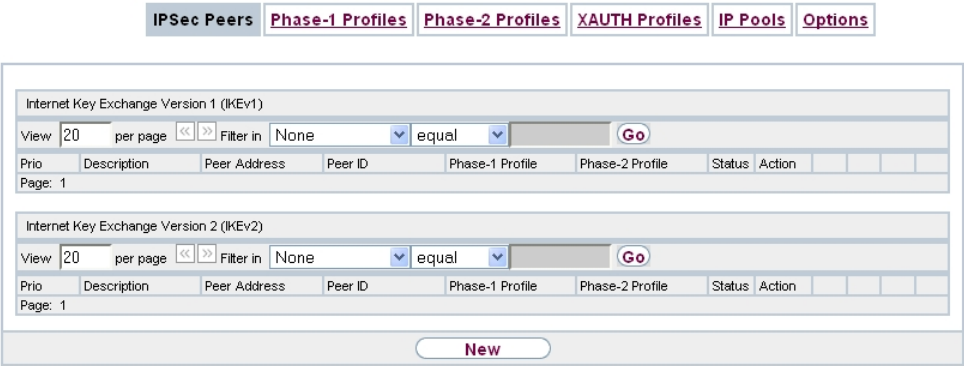



Fig. 133: VPN->IPSec->IPSec Peers

Peer Monitoring

The menu for monitoring a peer is called by selecting the  button for the peer in the peer list. See *Values in the IPsec Tunnels list* on page 501 .

18.1.1.1 New

Choose the **New** button to set up more IPsec peers.

IPSec Peers

Phase-1 Profiles

Phase-2 Profiles

XAUTH Profiles

IP Pools

Options

Peer Parameters

Administrative Status

☒ Up

☐ Down

Description

Peer-1

Peer Address

Peer ID

Fully Qualified Domain Name (FQDN)

Peer-1.

Internet Key Exchange

IKEv1

Preshared Key

Interface Routes

IP Address Assignment

Static

Default Route

☐ Enabled

Local IP Address

Route Entries

Remote IP Address

Netmask

Metric

1

Add

Additional Traffic Filter

Description

Protocol

Src. IPMask:Port

Dest. IPMask:Port

Add

Advanced Settings

Advanced IPSec Options

Phase-1 Profile

None (use default profile)

Phase-2 Profile

None (use default profile)

XAUTH Profile

Select one

Number of Admitted Connections

☒ One User ☐ Multiple Users

Start Mode

☒ On Demand ☐ Always up

Advanced IP Options

Public Interface

Chosen by Routing

Public Interface Mode

☒ Force ☐ Preferred

Public Source IP Address

☐ Enabled

Back Route Verify

☐ Enabled

Proxy ARP

☒ Inactive ☐ Up or Dormant ☐ Up only

IPSec Callback

Mode

Inactive

OK

Cancel

Fig. 134: VPN->IPSec->IPSec Peers->New

The menu **VPN->IPSec->IPSec Peers->New** consists of the following fields:

Fields in the menu Peer Parameters

Field	Description
Administrative Status	<p>Select the status to which you wish to set the peer after saving the peer configuration.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Up</i> (default value): The peer is available for setting up a tunnel immediately after saving the configuration.• <i>Down</i>: The peer is initially not available after the configuration has been saved.
Description	<p>Enter a description of the peer that identifies it.</p> <p>The maximum length of the entry is 255 characters.</p>
Peer Address	<p>Enter the official IP address of the peer or its resolvable host name.</p> <p>The entry can be omitted in certain configurations, whereby your device then cannot initiate an IPSec connection.</p>
Peer ID	<p>Select the ID type and enter the peer ID.</p> <p>This entry is not necessary in certain configurations.</p> <p>The maximum length of the entry is 255 characters.</p> <p>Possible ID types:</p> <ul style="list-style-type: none">• <i>Fully Qualified Domain Name (FQDN)</i>: Any string• <i>E-mail Address</i>• <i>IPv4 Address</i>• <i>ASN.1-DN (Distinguished Name)</i>• <i>Key ID</i>: Any string <p>On the peer device, this ID corresponds to the Local ID Value.</p>
Internet Key Exchange	<p>Not available for devices in the Wlxxxxn series. Those devices only support IKEv1.</p> <p>Select the version of the Internet Exchange Protocol to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>IKEv1</i> (default value): Internet Key Exchange Protocol Ver-

Field	Description
	<p>sion 1</p> <ul style="list-style-type: none">• <i>IKEv2</i>: Internet Kex Exchange Protocol Version 2
Authentication Method	<p>Only for Internet Key Exchange = <i>IKEv2</i></p> <p>Select the authentication method.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Preshared Keys</i> (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the IPSec Peers. The preshared key is the shared password.• <i>RSA Signature</i>: Phase 1 key calculations are authenticated using the RSA algorithm.
Local ID Type	<p>Only for Internet Key Exchange = <i>IKEv2</i></p> <p>Select the local ID type.</p> <p>Possible ID types:</p> <ul style="list-style-type: none">• <i>Fully Qualified Domain Name (FQDN)</i>• <i>E-mail Address</i>• <i>IPV4 Address</i>• <i>ASN.1-DN (Distinguished Name)</i>• <i>Key ID</i>: Any string
Local ID	<p>Only for Internet Key Exchange = <i>IKEv2</i></p> <p>Enter the ID of your device.</p> <p>For Authentication Method = <i>DSA Signature</i> or <i>RSA Signature</i> the option Use Subject Name from certificate is displayed.</p> <p>When you enable the option Use Subject Name from certificate, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used.</p> <p>Note: If you use certificates for authentication and your certificate contains alternative subject names (see Certificates on page 97), you must make sure your device selects the first al-</p>

Field	Description
	ternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.
Preshared Key	<p>Enter the password agreed with the peer.</p> <p>The maximum length of the entry is 50 characters. All characters are possible except for <i>0x</i> at the start of the entry.</p>

Fields in the menu Interface Routes

Field	Description
IP Address Assignment	<p>Select the configuration mode of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Static</i> (default value): Enter a static IP address.• <i>IKE Config Mode Client</i>: Can only be selected for IKEv1. Select this option if your gateway receives an IP address from the server as IPSec client.• <i>IKE Config Mode Server</i>: Select this option if your gateway assigns an IP address as server for connecting clients. This is taken from the selected IP Assignment Pool.
Config Mode	<p>Only where IP Address Assignment = <i>IKE Config Mode Server</i> or <i>IKE Config Mode Client</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Pull</i> (default value): The client requests the IP address and the gateway answers the request.• <i>Push</i>: The gateway suggests an IP address to the client and the client must either accept or reject this. <p>This value must be identical for both sides of the tunnel.</p>
IP Assignment Pool	<p>Only if IP Address Assignment = <i>IKE Config Mode Server</i></p> <p>Select an IP pool configured in the VPN->IPSec->IP Pools menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.</p>
Default Route	Only for IP Address Assignment = <i>Static</i> or <i>IKE Config</i>

Field	Description
	<p><i>Mode Client</i></p> <p>Select whether the route to this IPSec peer is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Local IP Address	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Server</i></p> <p>Enter the WAN IP address of your IPSec tunnel. This can be the same IP address as the address configured on your router as the LAN IP address.</p>
Metric	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Client</i> and Default Route = <i>Enabled</i></p> <p>Select the priority of the route.</p> <p>The lower the value, the higher the priority of the route.</p> <p>Value range from <i>0</i> to <i>15</i>. The default value is <i>1</i>.</p>
Route Entries	<p>Only for IP Address Assignment = <i>Static</i> or <i>IKE Config Mode Client</i></p> <p>Define routing entries for this connection partner.</p> <ul style="list-style-type: none">• <i>Remote IP Address</i>: IP address of the destination host or LAN.• <i>Netmask</i>: Netmask for <i>Remote IP Address</i>.• <i>Metric</i>: The lower the value, the higher the priority of the route (possible values <i>0..15</i>). The default value is <i>1</i>.

Fields in the menu Additional Traffic Filter

Field	Description
Additional Traffic Filter	<p>Only for Internet Key Exchange = <i>IKEv1</i></p> <p>Use Add to create a new filter.</p>

Additional data traffic filters

bintec elmeg Gateways support two different methods for establishing IPSec connections:

- a method based on policies and
- a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPSec phase 2 SAs. This enables the filtering of the IP packets to be very "fine grained" down to protocol and port level.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPSec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPSec phase 2 SAs. While it is true that this method simplifies many configurations, at the same time there can be problems due to competing routes or the "coarser" filtering of the data traffic.

The **Additional Traffic Filter** parameter fixes this problem. You can filter more "finely", i. e. you can, e. g., specify the source IP address or the source port. If there is a **Additional Traffic Filter** configured, it is used to negotiate the IPSec phase 2 SAs; the route only determines which data traffic is to be routed.

If an IP packet does not match the defined **Additional Traffic Filter** it is discarded.

If an IP packet meets the requirements in an **Additional Traffic Filter**, IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.



Note

The parameter **Additional Traffic Filter** is only relevant to the initiator of the IPSec connection, it only applies to outgoing data traffic.



Note

Please note that the phase 2 policies must be configured identically on both of the IPSec tunnel endpoints.

Add new entries with **Add**.

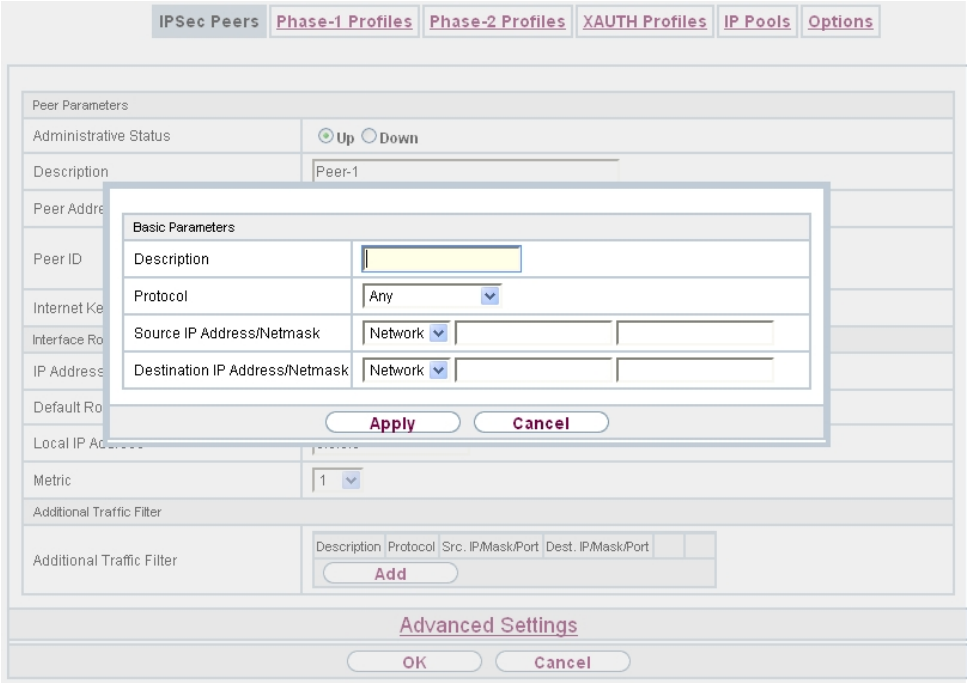


Fig. 135: VPN->IPsec->IPsec Peers->New->Add

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the filter.
Protocol	Select a protocol. The <i>Any</i> option (default value) matches all protocols.
Source IP Address/Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: <ul style="list-style-type: none">• <i>Any</i>• <i>Host</i>: Enter the IP address of the host.• <i>Network</i> (default value): Enter the network address and the related netmask.
Source Port	Only for Protocol = <i>TCP</i> or <i>UDP</i> Enter the source port of the data packets. The default setting –

Field	Description
	<i>All</i> - (= -1) means that the port remains unspecified.
Destination IP Address/Netmask	Enter the destination IP address and corresponding netmask of the data packets.
Destination Port	Only for Protocol = <i>TCP</i> or <i>UDP</i> Enter the destination port of the data packets. The default setting <i>-All</i> - (= -1) means that the port remains unspecified.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu **Advanced IPsec Options**

Field	Description
Phase-1 Profile	Select a profile for Phase 1. Besides user-defined profiles, pre-defined profiles are available. Possible values: <ul style="list-style-type: none">• <i>None (use default profile)</i>: Uses the profile marked as standard in VPN->IPsec->Phase-1 Profiles• <i>Multi-Proposal</i>: Uses a special profile which contains the proposals for Phase 1 3DES/MD5, AES/MD5 and Blowfish/MD5 regardless of the proposal selection in menu VPN->IPsec->Phase-1 Profiles.• <i><Profilname></i>: Uses a profile configured in menu VPN->IPsec->Phase-1 Profiles for Phase 1.
Phase-2 Profile	Select a profile for Phase 2. Besides user-defined profiles, pre-defined profiles are available. Possible values: <ul style="list-style-type: none">• <i>None (use default profile)</i>: Uses the profile marked as standard in VPN->IPsec->Phase-2 Profiles• <i>Multi-Proposal</i>: Uses a special profile which contains the proposals for Phase 2 3DES/MD5, AES-128/MD5 and Blowfish/MD5 regardless of the proposal selection in menu VPN->IPsec->Phase-2 Profiles.• <i><Profilname></i>: Uses a profile configured in menu VPN->IPsec->Phase-2 Profiles for Phase 2.

Field	Description
XAUTH Profile	<p>Select a profile created in VPN->IPSec->XAUTH Profiles if you wish to use this IPSec peer XAuth for authentication.</p> <p>If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.</p>
Number of Admitted Connections	<p>Choose how many users can connect using this peer profile.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>One User</i> (default value): Only one peer can be connected with the data defined in this profile.• <i>Multiple Users</i>: Several peers can be connected with the data defined in this profile. The peer entry is duplicated for each connection request with the data defined in this profile. <p>The dynamic peer configuration on the gateway must not specify a peer ID or a peer IP address. Clients connecting to the gateway, however, must have a peer ID specified in the client peer configuration, since the ID is still used to differentiate the tunnels created via the dynamic peer.</p> <p>The resulting gateway peer would match all incoming tunnel requests. It is, therefore, essential to put it at the end of the IPSec peer list on the gateway. Otherwise all peers that follow the dynamic peer in the peer list would be inactive.</p>
Start Mode	<p>Select how the peer is to be switched to the active state.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>On Demand</i> (default value): The peer is switched to the active state by a trigger.• <i>Always up</i>: The peer is always active.

Fields in the menu Advanced IP Options

Field	Description
Public Interface	<p>Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select <i>Chooosen by Routing</i>, the decision as to via which interface the data traffic is routed is made based on the current routing table. If you select an interface, the interface is used taking into consideration the</p>

Field	Description
	setting under Public Interface Mode .
Public Interface Mode	<p>Specify how strictly the setting under Public Interface is handled. Possible values:</p> <ul style="list-style-type: none"> • <i>Enforce</i>: Only the selected interface is used, whatever the priorities in the current routing table. • <i>Preferred</i>: Depending on the priorities in the current routing table, the selected interface is used if no more favourable route is available via a different interface.
Public Source IP Address	<p>If you are operating more than one Internet connection in parallel, here you can specify the public IP address that is to be used as the source address for the peer's data traffic. Select whether the Public Source IP Address is to be enabled.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>In the input field, enter the public IP address that is to be used as the sender address.</p> <p>The function is disabled by default.</p>
Back Route Verify	<p>Select whether a check on the back route should be activated for the interface to the connection partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
MobiKE	<p>Only for peers with IKEv2.</p> <p>MobiKE In cases of changing public IP addresses, enables only these addresses to be updated in the SAs without the SAs themselves having to be renegotiated.</p> <p>The function is enabled by default.</p> <p>Note that MobiKE requires a current IPSec client, e. g. the current Windows 7 or Windows 8 client or the latest version of the bintec elmeg IPSec client.</p>
Proxy ARP	<p>Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific connection partner.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>Inactive</i> (default value): Deactivates Proxy ARP for this IPSec peer.• <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the IPSec peer is <i>Up</i> (active) or <i>Dormant</i> (dormant). In the case of <i>Dormant</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.• <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the IPSec peer is <i>Up</i> (active), i.e. a connection already exists to the IPSec peer.

IPSec Callback

bintec elmeg devices support the DynDNS service to enable hosts without fixed IP addresses to obtain a secure connection over the Internet. This service enables a peer to be identified using a host name that can be resolved by DNS. You do not need to configure the IP address of the peer.

The DynDNS service does not signal whether a peer is actually online and cannot cause a peer to set up an Internet connection to enable an IPSec tunnel over the Internet. This possibility is created with IPSec callback: Using a direct ISDN call to a peer, you can signal that you are online and waiting for the peer to set up an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. This ISDN call costs nothing (depending on country), as it does not have to be accepted by your device. The identification of the caller from his or her ISDN number is enough information to initiate setting up a tunnel.

To set up this service, you must first configure a call number for IPSec callback on the passive side in the **Physical Interfaces->ISDN Ports->MSN Configuration->New** menu. The value *IPSec* is available for this purpose in the field **Service**. This entry ensures that incoming calls for this number are routed to the IPSec service.

If callback is active, the peer is caused to initiate setting up an IPSec tunnel by an ISDN call as soon as this tunnel is required. If callback is set to passive, setting up a tunnel to the peer is always initiated if an ISDN call is received on the relevant number (**MSN** in menu **Physical Interfaces->ISDN Ports->MSN Configuration->New** for **Service** *IPSec*). This ensures that both peers are reachable and that the connection can be set up over the Internet. The only case in which callback is not executed is if SAs (Security Associations) already exist, i.e. the tunnel to the peer already exists.

**Note**

If a tunnel is to be set up to a peer, the interface over which the tunnel is to be implemented is activated first by the IPSec Daemon. If IPSec with DynDNS is configured on the local device, the own IP address is propagated first and then the ISDN call is sent to the remote device. This ensures that the remote device can actually reach the local device if it initiates the tunnel setup.

Transfer of IP Address over ISDN

Transferring the IP address of a device over ISDN (in the D channel and/or B channel) opens up new possibilities for the configuration of IPSec VPNs. This enables restrictions that occur in IPSec configuration with dynamic IP addresses to be avoided.

**Note**

To use the IP address transfer over ISDN function, you must obtain a free-of-charge extra licence.

You can obtain the licence data for extra licences via the online licensing pages in the support section at www.bintec-elmeg.com. Please follow the online licensing instructions.

Before System Software Release 7.1.4, IPSec ISDN callback only supported tunnel setup if the current IP address of the initiator could be determined by indirect means (e.g. via DynDNS). However, DynDNS has serious disadvantages, such as the latency until the IP address is actually updated in the database. This can mean that the IP address propagated via DynDNS is not correct. This problem is avoided by transferring the IP address over ISDN. This type of transfer of dynamic IP addresses also enables the more secure ID Protect mode (main mode) to be used for tunnel setup.

Method of operation: Various modes are available for transferring your own IP address to the peer: The address can be transferred free in the D channel or in the B channel, but here the call must be accepted by the remote station and therefore incurs costs. If a peer whose IP address has been assigned dynamically wants to arrange for another peer to set up an IPSec tunnel, it can transfer its own IP address as per the settings described in *Fields in the menu IPSec Callback* on page 337. Not all transfer modes are supported by all telephone companies. If you are not sure, automatic selection by the device can be used to ensure that all the available possibilities can be used.

**Note**

The callback configuration should be the same on the two devices so that your device is able to identify the IP address information from the called peer.

The following roles are possible:

- One side takes on the active role, the other the passive role.
- Both sides can take on both roles (both).

The IP address transfer and the start of IKE phase 1 negotiation take place in the following steps:

- (1) Peer A (the callback initiator) sets up a connection to the Internet in order to be assigned a dynamic IP address and be reachable for peer B over the Internet.
- (2) Your device creates a token with a limited validity and saves it together with the current IP address in the MIB entry belonging to peer B.
- (3) Your device sends the initial ISDN call to peer B, which transfers the IP address of peer A and the token as per the callback configuration.
- (4) Peer B extracts the IP address of peer A and the token from the ISDN call and assigns them to peer A based on the calling party number configured (the ISDN number used by peer A to send the initial call to peer B).
- (5) The IPSec Daemon at peer B's device can use the transferred IP address to initiate phase 1 negotiation with peer A. Here the token is returned to peer A in part of the payload in IKE negotiation.
- (6) Peer A is now able to compare the token returned by peer B with the entries in the MIB and so identify the peer without knowing its IP address.

As peer A and peer B can now mutually identify each other, negotiations can also be conducted in the ID Protect mode using preshared keys.

**Note**

In some countries (e.g. Switzerland), the call in the D channel can also incur costs. An incorrect configuration at the called side can mean that the called side opens the B channel the calling side incurs costs.

The following options are only available on devices with an ISDN connection:

Fields in the menu IPSec Callback

Field	Description
Mode	<p>Select the Callback Mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Inactive</i> (default value): IPSec callback is deactivated. The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device. • <i>Passive</i>: The local device only reacts to incoming ISDN calls and, if necessary, initiates setting up an IPSec tunnel to the peer. No ISDN calls are sent to the remote device to cause this to set up an IPSec tunnel. • <i>Active</i>: The local device sends an ISDN call to the remote device to cause this to set up an IPSec tunnel. The device does not react to incoming ISDN calls. • <i>Both</i>: Your device can react to incoming ISDN calls and send ISDN calls to the remote device. The setting up of an IPSec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).
Incoming Phone Number	<p>Only for Mode = <i>Passive</i> or <i>Both</i></p> <p>Enter the ISDN number from which the remote device calls the local device (calling party number). Wildcards may also be used.</p>
Outgoing Phone Number	<p>Only for Mode = <i>Active</i> or <i>Both</i></p> <p>Enter the ISDN number with which the local device calls the remote device calls (called party number). Wildcards may also be used.</p>
Transfer own IP address over ISDN/GSM	<p>Select whether the IP address of your own device is to be transferred over ISDN for IPSec callback.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Transfer Mode	<p>Only for Transfer own IP address over ISDN/GSM = enabled</p> <p>Select the mode in which your device is to attempt to transfer its IP address to the peer.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>Autodetect best mode</i>: Your device automatically determines the most favourable mode. It first tries all D channel modes before switching to the B channel. (Costs are incurred for using the B channel.)• <i>Autodetect only D Channel Modes</i>: Your device automatically determines the most favourable D channel mode. The use of the B channel is excluded.• <i>Use specific D Channel Mode</i>: Your device tries to transfer the IP address in the mode set in the Mode field.• <i>Try specific D Channel Mode, fall back to B Channel</i>: Your device tries to transfer the IP address in the mode set in the Mode field. If this does not succeed, the IP address is transferred in the B channel. (This incurs costs.)• <i>Use only B Channel Mode</i>: Your device transfers the IP address in the B channel. This incurs costs.
D Channel Mode	<p>Only for Transfer Mode = <i>Use specific D Channel Mode</i> or <i>Try specific D Channel Mode, fall back to B Channel</i></p> <p>Select the D channel mode in which your device tries to transfer the IP address.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>LLC</i> (default value): The IP address is transferred in the "LLC information elements" of the D channel.• <i>SUBADDR</i>: The IP address is transferred in the subaddress "information elements" of the D channel.• <i>LLC and SUBADDR</i>: The IP address is transferred in both the "LLC" and "subaddress information elements".

18.1.2 Phase-1 Profiles

A list of all configured tunnel profiles is displayed in the **VPN->IPSec->Phase-1 Profiles** menu.

IPSec PeersPhase-1 ProfilesPhase-2 ProfilesXAUTH ProfilesIP PoolsOptions

Internet Key Exchange Version 1 (IKEv1)

View 20 per page<<>>Filter in NoneequalGo

Default	Description	Proposals	Authentication	Mode	DH Group	Lifetime

Page: 1

Create new IKEv1 ProfileNew

Internet Key Exchange Version 2 (IKEv2)

View 20 per page<<>>Filter in NoneequalGo

Default	Description	Proposals	Lifetime

Page: 1

Create new IKEv2 ProfileNew

OK

Cancel

Fig. 136: VPN->IPSec->Phase-1 Profiles

In the **Default** column, you can mark the profile to be used as the default profile.

18.1.2.1 New

Choose the **New** (at **Create new IKEv1 Profile** or **Create new IKEv2 Profile**) button to create additional profiles.

IPSec PeersPhase-1 ProfilesPhase-2 ProfilesXAUTH ProfilesIP PoolsOptions

Phase-1 (IKE) Parameters

DescriptionIKE-1

Proposals

EncryptionAuthenticationEnabled

AESMD5

AESMD5

AESMD5

DH Group

1(768 Bit)2(1024 Bit)5(1536 Bit)

Lifetime

14400Seconds0kBytes

Authentication Method

Preshared Keys

Mode

Main Mode (ID Protect)AggressiveStrict

Local ID Type

Fully Qualified Domain Name (FQDN)

Local ID Value

r4402

Advanced Settings

Alive CheckAutodetect

Block Time30Seconds

NAT TraversalEnabled

OKCancel

Fig. 137: VPN->IPSec->Phase-1 Profiles->New

The menu VPN->IPSec->Phase-1 Profiles->New consists of the following fields:

Fields in the Phase-1 (IKE) Parameters menu.

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	<p>In this field, you can select any combination of encryption and message hash algorithms for IKE phase 1 on your device. The combination of six encryption algorithms and four message hash algorithms gives 24 possible values in this field. At least one proposal must exist. Therefore the first line of the table can-not be deactivated.</p> <p>Encryption algorithms (Encryption):</p> <ul style="list-style-type: none">• <i>3DES</i> (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported.• <i>Twofish</i>: Twofish was a final candidate for the AES

bintec RV Series

341

Field	Description
	<p>(Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower.</p> <ul style="list-style-type: none">• <i>Blowfish</i>: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish.• <i>CAST</i>: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES.• <i>DES</i>: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits.• <i>AES</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. The partner's AES key length is used here. If this has also selected the parameter <i>AES</i> , a key length of 128 bits is used.• <i>AES-128</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits.• <i>AES-192</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits.• <i>AES-256</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. <p>Hash algorithms (Authentication):</p> <ul style="list-style-type: none">• <i>MD5</i> (default value): MD5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec.• <i>SHA1</i>: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec.• <i>RipeMD 160</i>: RipeMD 160 is a 160 bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD.• <i>Tiger192</i>: Tiger 192 is a relatively new and very fast algorithm. <p>Please note that the description of the encryption and authentic-</p>

Field	Description
	<p>ation or the hash algorithms is based on the author's knowledge and opinion at the time of creating this User Guide. In particular, the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.</p>
DH Group	<p>Only for Phase-1 (IKE) Parameters</p> <p>The Diffie-Hellman group defines the parameter set used as the basis for the key calculation during phase 1. "MODP" as supported by bintec elmeg devices stands for "modular exponentiation".</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>1 (768 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material.• <i>2 (1024 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material.• <i>5 (1536 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	<p>Create a lifetime for phase 1 keys.</p> <p>The following options are available for defining the Lifetime:</p> <ul style="list-style-type: none">• Input in Seconds: Enter the lifetime for phase 1 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is <i>14400</i>, which means the key must be renewed once four hours have elapsed.• Input in kBytes: Enter the lifetime for phase 1 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is <i>0</i>, which means that the number of transmitted kBytes is irrelevant.
Authentication Method	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the authentication method.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>Preshared Keys</i> (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the VPN->IPSec->IPSec Peers. The preshared key is the shared password.• <i>DSA Signature</i>: Phase 1 key calculations are authenticated using the DSA algorithm.• <i>RSA Signature</i>: Phase 1 key calculations are authenticated using the RSA algorithm.• <i>RSA Encryption</i>: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	<p>Only for Phase-1 (IKE) Parameters</p> <p>Only for Authentication Method = <i>DSA Signature</i>, <i>RSA Signature</i> or <i>RSA Encryption</i></p> <p>This field enables you to select one of your own certificates for authentication. It shows the index number of this certificate and the name under which it is saved. This field is only shown for authentication settings based on certificates and indicates that a certificate is essential.</p>
Mode	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the phase 1 mode.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Aggressive</i> (default value): The Aggressive Mode is necessary if one of the peers does not have a static IP address and preshared keys are used for authentication. It requires only three messages to configure a secure channel.• <i>Main Mode (ID Protect)</i>: This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. <p>Also define whether the selected mode is used exclusively (Strict), or the peer can also propose another mode.</p>

Field	Description
Local ID Type	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the local ID type.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Fully Qualified Domain Name (FQDN)</i>• <i>E-mail Address</i>• <i>IPV4 Address</i>• <i>ASN.1-DN (Distinguished Name)</i>
Local ID Value	<p>Only for Phase-1 (IKE) Parameters</p> <p>Enter the ID of your device.</p> <p>For Authentication Method = <i>DSA Signature</i>, <i>RSA Signature</i> or <i>RSA Encryption</i> the Use Subject Name from certificate option is displayed.</p> <p>When you enable the Use Subject Name from certificate option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used.</p> <p>Note: If you use certificates for authentication and your certificate contains alternative subject names (see Certificates on page 97), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.</p>

Alive Check

During communication between two IPSec peers, one of the peers may become unavailable, e.g. due to routing problems or a reboot. However, this can only be detected when the end of the lifetime of the security connection is reached. Up until this point the data packets are lost. These are various methods of performing an alive check to prevent this happening. In the **Alive Check** field you can specify whether a method should be used to check the availability of a peer.

Two methods are available: Heartbeats and Dead Peer Detection.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Alive Check	<p>Only for Phase-1 (IKE) Parameters</p> <p>Select the method to be used to check the functionality of the IPSec connection.</p> <p>In addition to the default method Dead Peer Detection (DPD), the (proprietary) Heartbeat method is implemented. This sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Autodetect</i> (default value): Your device detects and uses the mode supported by the remote terminal.• <i>Inactive</i>: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers.• <i>Heartbeats (Expect only)</i>: Your device expects a heartbeat from the peer but does not send one itself.• <i>Heartbeats (Send only)</i>: Your device expects no heartbeat from the peer, but sends one itself.• <i>Heartbeats (Send &Expect)</i>: Your device expects a heartbeat from the peer and sends one itself.• <i>Dead Peer Detection</i>: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option only checks the availability of the peer if data is to be sent to it.• <i>Dead Peer Detection (Idle)</i>: Use DPD (dead peer detection) in accordance with RFC 3706. DPD uses a request-reply protocol to check the availability of the remote terminal and can be configured independently on both sides. This option is used to carry out a check at certain intervals depending on forthcoming data transfers. <p>Only for Phase-1 (IKEv2) Parameters</p> <p>Enable or disable alive check.</p> <p>The function is enabled by default.</p>

Field	Description
Block Time	<p>Define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This only affects locally initiated setup attempts.</p> <p>Possible values are <i>-1</i> to <i>86400</i> (seconds); <i>-1</i> means the value in the default profile is used and <i>0</i> means that the peer is never blocked.</p> <p>The default value is <i>30</i>.</p>
NAT Traversal	<p>NAT Traversal (NAT-T) also enables IPSec tunnels to be opened via one or more devices on which network address translation (NAT) is activated.</p> <p>Without NAT-T, incompatibilities may arise between IPSec and NAT (see RFC 3715, section 2). These primarily prevent the setup of an IPSec tunnel from a host within a LANs and behind a NAT device to another host or device. NAT-T enables these kinds of tunnels without conflicts with NAT device, activated NAT is automatically detected by the IPSec Daemon and NAT-T is used.</p> <p>Only for <i>IKEv1 profiles</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Enabled</i> (default value): NAT Traversal is enabled.• <i>Disabled</i>: NAT Traversal is disabled.• <i>Force</i>: The device always behaves as it would if NAT were in use. <p>Only for <i>IKEv2 profiles</i></p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
CA Certificates	<p>Only for Phase-1 (IKE) Parameters</p> <p>Only for Authentication Method = <i>DSA Signature</i>, <i>RSA Signature</i> or <i>RSA Encryption</i></p> <p>If you enable the Trust the following CA certificates option, you can select up to three CA certificates that are accepted for this profile.</p>

Field	Description
	This option can only be configured if certificates are loaded.

18.1.3 Phase-2 Profiles

You can define profiles for phase 2 of the tunnel setup just as for phase 1.

In the **VPN->IPSec->Phase-2 Profiles** menu, a list of all configured IPSec phase 2 profiles is displayed.

IPSec PeersPhase-1 ProfilesPhase-2 ProfilesXAUTH ProfilesIP PoolsOptions

View20per page<<>>Filter inNoneequalGo

Default	Description	Proposals	PFS Group	Lifetime
Page: 1				

NewOKCancel

Fig. 138: VPN->IPSec->Phase-2 Profiles

In the **Default** column, you can mark the profile to be used as the default profile.

18.1.3.1 New

Choose the **New** button to create additional profiles.

IPSec Peers

Phase-1 Profiles

Phase-2 Profiles

XAUTH Profiles

IP Pools

Options

Phase-2 (IPSEC) Parameters

Description

IPSec-2

Proposals

Encryption	Authentication	Enabled
AES	MD5	<input type="checkbox"/>
AES	MD5	<input type="checkbox"/>
AES	MD5	<input type="checkbox"/>

Use PFS Group

☒ Enabled
☐ 1(768 Bit) ☒ 2(1024 Bit) ☐ 5(1536 Bit)

Lifetime

7200 Seconds 0 kBytes Rekey after 80 % Lifetime

Advanced Settings

IP Compression

☐ Enabled

Alive Check

Autodetect

Propagate PMTU

☒ Enabled

OK

Cancel

Fig. 139: VPN->IPSec->Phase-2 Profiles->New

The menu VPN->IPSec->Phase-2 Profiles->New consists of the following fields:

Fields in the Phase-2 (IPSEC) Parameters menu.

Field	Description
Description	<p>Enter a description that uniquely identifies the profile.</p> <p>The maximum length of the entry is 255 characters.</p>
Proposals	<p>In this field, you can select any combination of encryption and message hash algorithms for IKE phase 2 on your default. The combination of six encryption algorithms and two message hash algorithms gives 12 possible values in this field.</p> <p>Encryption algorithms (Encryption):</p> <ul style="list-style-type: none">• 3DES (default value): 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported.• -- ALL --: All options can be used.• AES: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. The partner's AES key length is used here. If this has also selected the parameter

Field	Description
	<p><i>AES</i> , a key length of 128 bits is used.</p> <ul style="list-style-type: none">• <i>AES-128</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 128 bits.• <i>AES-192</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits.• <i>AES-256</i>: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits.• <i>Twofish</i>: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower.• <i>Blowfish</i>: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish.• <i>CAST</i>: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES.• <i>DES</i>: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. <p>Hash algorithms (Authentication):</p> <ul style="list-style-type: none">• <i>MD5</i> (default value): MD5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec.• <i>-- ALL --</i>: All options can be used.• <i>SHA1</i>: SHA1 (Secure Hash Algorithm #1) is a hash algorithm developed by NSA (United States National Security Association). It is rated as secure, but is slower than MD5. It is used with a 96 bit digest length for IPSec. <p>Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.</p>
Use PFS Group	<p>As PFS (Perfect Forward Secrecy) requires another Diffie-Hellman key calculation to create new encryption material, you must select the exponentiation features. If you enable PFS (<i>Enabled</i>), the options are the same as for the configuration of DH Group in the VPN->IPSec->Phase-1 Profiles menu. PFS is</p>

Field	Description
	<p>used to protect the keys of a renewed phase 2 SA, even if the keys of the phase 1 SA have become known.</p> <p>The field has the following options:</p> <ul style="list-style-type: none">• <i>1 (768 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 768 bits is used to create the encryption material.• <i>2 (1024 Bit)</i> (default value): During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material.• <i>5 (1536 Bit)</i>: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	<p>Define how the lifetime is defined that will expire before phase 2 SAs need to be renewed.</p> <p>The new SAs are negotiated shortly before expiry of the current SAs. As for RFC 2407, the default value is eight hours, which means the key must be renewed once eight hours have elapsed.</p> <p>The following options are available for defining the Lifetime:</p> <ul style="list-style-type: none">• Input in Seconds: Enter the lifetime for phase 2 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is 7200.• Input in kBytes: Enter the lifetime for phase 2 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is 0. <p>Rekey after: Specify the percentage in the course of the lifetime at which the phase 2 keys are to be regenerated.</p> <p>The percentage entered is applied to both the lifetime in seconds and the lifetime in kBytes.</p> <p>The default value is 80 %.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
IP Compression	<p>Select whether compression is to be activated before data encryption. If data is compressed effectively, this can result in higher performance and a lower volume of data to be transferred. In the case of fast lines or data that cannot be compressed, you are advised against using this option as the performance can be significantly affected by the increased effort during compression.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Alive Check	<p>Select whether and how IPSec heartbeats are used.</p> <p>A bintec elmeg IPSec heartbeat is implemented to determine whether or not a Security Association (SA) is still valid. This function sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Autodetect</i> (default value): Automatic detection of whether the remote terminal is a bintec elmeg device. If it is, <i>Heartbeats (Send &Expect)</i> (for a remote terminal with bintec elmeg) or <i>Inactive</i> (for a remote terminal without bintec elmeg) is set.• <i>Inactive</i>: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers.• <i>Heartbeats (Expect only)</i>: Your device expects a heartbeat from the peer but does not send one itself.• <i>Heartbeats (Send only)</i>: Your device expects no heartbeat from the peer, but sends one itself.• <i>Heartbeats (Send &Expect)</i>: Your device expects a heartbeat from the peer and sends one itself.
Propagate PMTU	<p>Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

18.1.4 XAUTH Profiles

In the **XAUTH Profiles** menu a list of all XAUTH profiles is displayed.

Extended Authentication for IPSec (XAuth) is an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or as a client:

- As a server the gateway requires a proof of authorisation.
- As a client the gateway provides proof of authorisation.

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server. If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

18.1.4.1 New

Choose the **New** button to create additional profiles.

IPSec PeersPhase-1 ProfilesPhase-2 ProfilesXAUTH ProfilesIP PoolsOptions

Basic Parameters

Description	
Role	Server
Mode	radius
RADIUS Server Group ID	No Radius Server configured for XAUTH

OKCancel

Fig. 140: VPN->IPSec->XAUTH Profiles->New

The **VPN->IPSec->XAUTH Profiles->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for this XAuth profile.
Role	<p>Select the role of the gateway for XAuth authentication.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Server</i> (default value): The gateway requires a proof of authorisation.• <i>Client</i>: The gateway provides proof of authorisation.
Mode	<p>Only for Role = <i>Server</i></p> <p>Select how authentication is carried out.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>RADIUS</i> (default value): Authentication is carried out via a Radius server. It is configured in the System Management->Remote Authentication->RADIUS menu and selected in the RADIUS Server Group ID field.• <i>Local</i>: Authentication is carried out via a local list.
Name	<p>Only for Role = <i>Client</i></p> <p>Enter the authentication name of the client.</p>
Password	<p>Only for Role = <i>Client</i></p> <p>Enter the authentication password.</p>
RADIUS Server Group ID	<p>Only for Role = <i>Server</i></p> <p>Select the desired list in System Management->Remote Authentication->RADIUS configured RADIUS group.</p>
Users	<p>Only for Role = <i>Server</i> and Mode = <i>Local</i></p> <p>If your gateway is configured as an XAuth server, the clients can be authenticated via a locally configured user list. Define the members of the user group of this XAUTH profile here by</p>


Field	Description
	entering the authentication name of the client (Name)) and the authentication password (Password). Add new members with Add .

18.1.5 IP Pools

In the **IP Pools** menu a list of all IP pools for your configured IPSec connections is displayed.

If for an IPSec peer you have set **IP Address Assignment** *IKE Config Mode Server*, you must define the IP pools here from which the IP addresses are assigned.

18.1.5.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

IPSec PeersPhase-1 ProfilesPhase-2 ProfilesXAUTH ProfilesIP PoolsOptions

Basic Parameters

IP Pool Name

IP Address Range

 -

DNS Server

Primary

Secondary

OK

Cancel

Fig. 141: VPN->IPSec->IP Pools->New

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. Secondary: Optionally, enter the IP address of an alternative

Field	Description
	DNS server.

18.1.6 Options

IPSec PeersPhase-1 ProfilesPhase-2 ProfilesXAUTH ProfilesIP PoolsOptions

Global Options

Enable IPSec	<input type="checkbox"/> Enabled
Delete complete IPSec configuration	
IPSec Debug Level	Debug

Advanced Settings

IPSec over TCP	<input type="checkbox"/> NCP Path Finder Technology
Send Initial Contact Message	<input checked="" type="checkbox"/> Enabled
Sync SAs with ISP interface state	<input type="checkbox"/> Enabled
Use Zero Cookies	<input checked="" type="checkbox"/> Enabled
Zero Cookie Size	32 Bit
Dynamic RADIUS Authentication	<input type="checkbox"/> Enabled

PKI Handling Options

Ignore Certificate Request Payloads	<input type="checkbox"/> Enabled
Send Certificate Request Payloads	<input checked="" type="checkbox"/> Enabled
Send Certificate Chains	<input checked="" type="checkbox"/> Enabled
Send CRLs	<input type="checkbox"/> Enabled
Send Key Hash Payloads	<input checked="" type="checkbox"/> Enabled

OKCancel

Fig. 142: VPN->IPSec->Options

The menu **VPN->IPSec->Options** consists of the following fields:

Fields in the Global Options menu.

Field	Description
Enable IPSec	Select whether you want to activate IPSec. The function is enabled with <i>Enabled</i> . The function is active as soon as an IPSec Peer is configured.
Delete complete IPSec configuration	If you click the icon, delete the complete IPSec configuration of your device.

Field	Description
	<p>This cancels all settings made during the IPSec configuration. Once the configuration is deleted, you can start with a completely new IPSec configuration.</p> <p>You can only delete the configuration if Enable IPSec = not activated.</p>
IPSec Debug Level	<p>Select the priority of the syslog messages of the IPSec subsystem to be recorded internally.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Emergency</i> (highest priority)• <i>Alert</i>• <i>Critical</i>• <i>Error</i>• <i>Warning</i>• <i>Notice</i>• <i>Information</i>• <i>Debug</i> (default value, lowest priority) <p>Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level "debug".</p>

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other bintec elmeg devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
IPSec over TCP	<p>Determine whether IPSec over TCP is to be used.</p> <p>IPSec over TCP is based on NCP pathfinder technology. This technology insures that data traffic (IKE, ESP, AH) between peers is integrated into a pseudo HTTPS session.</p>

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Send Initial Contact Message	<p>Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Sync SAs with ISP interface state	<p>Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from <i>Up</i> to <i>Down</i>, <i>Dormant</i> or <i>Blocked</i>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Use Zero Cookies	<p>Select whether zeroed ISAKMP Cookies are to be sent.</p> <p>These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, your device can use zeroes for all values of the cookie. In this case, select <i>Enabled</i>.</p>
Zero Cookie Size	<p>Only for Use Zero Cookies = enabled.</p> <p>Enter the length in bytes of the zeroed SPI used in IKE proposals.</p> <p>The default value is <i>32</i>.</p>
Dynamic RADIUS Authentication	<p>Select whether RADIUS authentication is to be activated via IPSec.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the PKI Handling Options menu.

Field	Description
Ignore Certificate Re-	Select whether certificate requests received from the remote

Field	Description
quest Payloads	<p>end during IKE (phase 1) are to be ignored.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Send Certificate Request Payloads	<p>Select whether certificate requests are to be sent during IKE (phase 1).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Send Certificate Chains	<p>Select whether complete certificate chains are to be sent during IKE (phase 1).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>Deactivate this function if you do not wish to send the peer the certificates of all levels (from your level to the CA level).</p>
Send CRLs	<p>Select whether CRLs are to be sent during IKE (phase 1).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Send Key Hash Payloads	<p>Select whether key hash payloads are to be sent during IKE (phase 1).</p> <p>In the default setting, the public key hash of the remote end is sent together with the other authentication data. Only applies for RSA encryption. Activate this function with <i>Enabled</i> to suppress this behaviour.</p>

18.2 L2TP

The layer 2 tunnel protocol (L2TP) enables PPP connections to be tunnelled via a UDP connection.

Your bintec elmeg device supports the following two modes:

- L2TP LNS Mode (L2TP Network Server): for incoming connections only
- L2TP LAC Mode (L2TP Access Concentrator): for outgoing connections only

Note the following when configuring the server and client: An L2TP tunnel profile must be created on each of the two sides (LAC and LNS). The corresponding L2TP tunnel profile is used on the initiator side (LAC) to set up the connection. The L2TP tunnel profile is needed on the responder side (LNS) to accept the connection.

18.2.1 Tunnel Profiles

A list of all configured tunnel profiles is displayed in the **VPN->L2TP->Tunnel Profiles** menu.

18.2.1.1 New

Choose the **New** button to create additional tunnel profiles.

Tunnel ProfilesUsersOptions

Basic Parameters

Description

L2TP1

Local Hostname

Remote Hostname

Password

••••••••

LAC Mode Parameters

Remote IP Address

UDP Source Port

☐ Fixed

UDP Destination Port

1701

Advanced Settings

Local IP Address

Hello Intervall

30

Seconds

Minimum Time between Retries

1

Seconds

Maximum Time between Retries

16

Seconds

Maximum Retries

5

Data Packets Sequence Numbers

☐ Enabled

OK

Cancel

Fig. 143: VPN->L2TP->Tunnel Profiles ->New

The menu **VPN->L2TP->Tunnel Profiles ->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	<p>Enter a description for the current profile.</p> <p>The device automatically names the profiles <i>L2TP</i> and numbers them, but the value can be changed.</p>
Local Hostname	<p>Enter the host name for LNS or LAC.</p> <ul style="list-style-type: none">• <i>LAC</i>: The local hostname is used in outgoing tunnel setup messages to identify this device and is associated with the remote hostname of a tunnel profile configured on the LNS. These tunnel setup messages are SCCRQs (Start Control Connection Request) sent from the LAC and SCCRPs (Start Control Connection Reply) sent from the LNS.• <i>LNS</i>: Is the same as the value for Remote Hostname of the incoming tunnel setup message from the LAC.
Remote Hostname	<p>Enter the host name of the LNS or LAC.</p> <ul style="list-style-type: none">• <i>LAC</i>: Defines the value for Local Hostname of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). A Local Hostname configured in the LAC must match Remote Hostname configured for the intended profile in the LNS and vice versa.• <i>LNS</i>: Defines the Local Hostname of the LAC. If the Remote Hostname field remains empty on the LNS, the related profile qualifies as the standard entry and is used for all incoming calls for which a profile with a matching remote hostname cannot be found.
Password	<p>Enter the password to be used for tunnel authentication. Authentication between LAC and LNS takes place in both directions, i.e. the LNS checks the Local Hostname and the Password contained in the SCCRQ of the LAC and compares them with those specified in the relevant profile. The LAC does the same with the fields of the SCCRP of the LNS.</p> <p>If this field remains empty, authentication data in the tunnel setup messages are not sent and are ignored.</p>

Fields in the LAC Mode Parameters menu.

Field	Description
Remote IP Address	<p>Enter the fixed IP address of the LNS used as the destination address for connections based on this profile.</p> <p>The destination must be a device that can behave like an LNS.</p>
UDP Source Port	<p>Enter how the port number to be used as the source port for all outgoing L2TP connections based on this profile is to be determined.</p> <p>By default, the Fixed option is disabled, which means that ports are dynamically assigned to the connections that use this profile.</p> <p>If you want to enter a fixed port, enable the <i>Fixed</i> option. Select this option if you encounter problems with the firewall or NAT.</p> <p>The available values are 0 to 65535.</p>
UDP Destination Port	<p>Enter the destination port number to be used for all calls based on this profile. The remote LNS that receives the call must monitor this port on L2TP connections.</p> <p>Possible values are 0 to 65535.</p> <p>The default value is 1701 (RFC 2661).</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Local IP Address	<p>Enter the IP address to be used as the source address for all L2TP connections based on this profile.</p> <p>If this field is left empty, your device uses the IP address of the interface used to reach the remote IP Address by the L2TP tunnel.</p>
Hello Intervall	<p>Enter the interval (in seconds) between the sending of two L2TP HELLO messages. These messages are used to keep the tunnel open.</p> <p>The available values are 0 to 255, the default value is 30. The</p>

Field	Description
	value <i>0</i> means that no L2TP HELLO messages are sent.
Minimum Time between Retries	<p>Enter the minimum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response.</p> <p>The wait time is dynamically extended until it reaches the Maximum Time between Retries. The available values are <i>1</i> to <i>255</i>, the default value is <i>1</i>.</p>
Maximum Time between Retries	<p>Enter the maximum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response.</p> <p>The available values are <i>8</i> to <i>255</i>, the default value is <i>16</i>.</p>
Maximum Retries	<p>Enter the maximum number of times your device is to try to resend the L2TP control packet for which is received no response.</p> <p>The available values are <i>8</i> to <i>255</i>, the default value is <i>5</i>.</p>
Data Packets Sequence Numbers	<p>Select whether your device is to use sequence numbers for data packets sent through a tunnel on the basis of this profile.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

18.2.2 Users

A list of all configured interface L2TP partners is displayed in the **VPN->L2TP->Users** menu.

18.2.2.1 New

Choose the **New** button to set up new L2TP partners.

Tunnel Profiles

Users

Options

Basic Parameters

Description

Connection Type

LNS

LAC

User Name

Password

••••••

Always on

Enabled

Connection Idle Timeout

300

Seconds

IP Mode and Routes

IP Address Mode

Static

Provide IP Address

Default Route

Enabled

Create NAT Policy

Enabled

Local IP Address

Route Entries

Remote IP Address

Netmask

Metric

1

Add

Advanced Settings

Block after connection failure for

300

Seconds

Authentication

MS-CHAPv2

Encryption

None

Enabled

Windows compatible

LCP Alive Check

Enabled

Prioritize TCP ACK Packets

Enabled

IP Options

OSPF Mode

Passive

Active

Inactive

Proxy ARP Mode

Inactive

Up or Dormant

Up only

DNS Negotiation

Enabled

OK

Cancel

Fig. 144: VPN->L2TP->Users->New

The menu VPN->L2TP->Users->New consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	<p>Enter a name for uniquely identifying the L2TP partner.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used. The maximum length of the entry is 25 characters.</p>
Connection Type	Select whether the L2TP partner is to take on the role of the

Field	Description
	<p>L2TP network server (LNS) or the functions of a L2TP access concentrator client (LAC client).</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>LNS</i> (default value): If you select this option, the L2TP partner is configured so that it accepts L2TP tunnels and restores the encapsulated PPP traffic flow.• <i>LAC</i>: If you select this option, the L2TP partner is configured so that it encapsulates a PPP traffic flow in L2TP and sets up a L2TP tunnel to a remote LNS.
Tunnel Profile	<p>Only for Connection Type = <i>LAC</i></p> <p>Select a profile created in the Tunnel Profile menu for the connection to this L2TP partner.</p>
User Name	Enter the code of your device.
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Connection Idle Timeout	<p>Only if Always on is disabled</p> <p>Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the short hold. The default value is <i>300</i>.</p>

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none">• <i>Static</i> (default value): You enter a static IP address.• <i>Provide IP Address</i>: Only for Connection Type = <i>LNS</i>. Your device dynamically assigns an IP address to the remote terminal.• <i>Get IP Address</i>: Only for Connection Type = <i>LAC</i>. Your device is dynamically assigned an IP address.
Default Route	<p>Only for IP Address Mode = <i>Get IP Address</i> and <i>Static</i></p> <p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Create NAT Policy	<p>Only for IP Address Mode = <i>Get IP Address</i> and <i>Static</i></p> <p>Specify whether Network Address Translation (NAT) is to be activated for this connection.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
IP Assignment Pool (IPCP)	<p>Only for IP Address Mode = <i>Provide IP Address</i></p> <p>Select an IP pool configured in the WAN->Internet + Dialup->IP Pools menu.</p>
Local IP Address	<p>Only for IP Address Mode = <i>Static</i></p> <p>Enter the WAN IP address of your device.</p>
Route Entries	<p>Only for IP Address Mode = <i>Static</i></p> <p>Enter Remote IP Address and Netmask of the LANs for L2TP partners and the corresponding Metric. Add new entries with Add.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed.</p> <p>The default value is <i>300</i>.</p>
Authentication	<p>Select the authentication protocol for this L2TP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>PAP/CHAP/MS-CHAP</i> (default value): Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.)• <i>PAP</i>: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.• <i>None</i>: Some providers use no authentication. In this case, select this option.
Encryption	<p>If necessary, select the type of encryption that should be used for data traffic to the L2TP partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If Encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i>: MPP encryption is not used.• <i>Enabled</i> (default value): MPP encryption V2 with 128 bit is used to RFC 3078.• <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be</p>

Field	Description
	<p>checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Prioritize TCP ACK Packets	<p>Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the IP Options menu.

Field	Description
OSPF Mode	<p>Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces.• <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface.• <i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	<p>Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific L2TP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Inactive</i> (default value): Deactivates Proxy ARP for this L2TP partner.• <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the L2TP partner is <i>Up</i> (active) or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up un-

Field	Description
	til someone actually wants to use the route. <ul style="list-style-type: none">• <i>Up only</i>: Your device responds to an ARP request only if the status of the connection to the L2TP partner is <i>Up</i> (active), i.e. a connection already exists to the L2TP partner.
DNS Negotiation	Select whether your device receives IP addresses for Primary DNS Server und Secondary DNS Server and WINS Server Primary and Secondary from the L2TP partner or sends these to the L2TP partner. <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

18.2.3 Options



Fig. 145: VPN->L2TP->Options

The menu **VPN->L2TP->Options** consists of the following fields:

Fields in the Global Options menu.

Field	Description
UDP Destination Port	Enter the port to be monitored by the LNS on incoming L2TP tunnel connections. <p>Available values are all whole numbers from 1 to 65535, the default value is 1701, as specified in RFC 2661.</p>
UDP Source Port Selection	Select whether the LNS should only use the monitored port (UDP Destination Port) as the local source port for the L2TP connection. <p>The function is enabled with <i>Fixed</i>.</p>

Field	Description
	The function is disabled by default.

18.3 PPTP

The Point-to-Point Tunnelling Protocol (=PPTP) can be used to set up an encrypted PPTP tunnel to provide security for data traffic over an existing IP connection.

First a connection to an ISP (=Internet Service Provider) is set up at both sites. Once these connections are available, a tunnel is set up to the PPTP partner over the Internet using PPTP.

The PPTP subsystem sets up a control connection between the endpoints of the tunnel. This is used to send control data to set up, keep alive and terminate the connection between the two PPTP tunnel end-points. As soon as this control connection is set up, the PPTP transfers the traffic data packed in GRE packets (GRE = Generic Routing Encapsulation).

18.3.1 PPTP Tunnels

A list of all PPTP tunnels is displayed in the **PPTP Tunnels** menu.

18.3.1.1 New

Click on **New** to set up further PPTP partners.

PPTP TunnelsOptionsIP Pools

PPTP Partner Parameters

Description

PPTP Mode

☒PNS

☐Windows Client Mode

User Name

Password

••••••••

Always on

☐Enabled

Connection Idle Timeout

300

Seconds

Remote PPTP IP Address

IP Mode and Routes

IP Address Mode

☐Static

☐Provide IP Address

Default Route

☐Enabled

Create NAT Policy

☐Enabled

Local IP Address

Route Entries

Remote IP Address

Netmask

Metric

1

Add

Advanced Settings

Block after connection failure for

300

Seconds

Authentication

MS-CHAPv2

Encryption

☐None

☒Enabled

☐Windows compatible

Compression

☒None

☐STAC

☐MS-STAC

☐MPPC

LCP Alive Check

☒Enabled

IP Options

OSPF Mode

☒Passive

☐Active

☐Inactive

Proxy ARP Mode

☒Inactive

☐Up or Dormant

☐Up only

DNS Negotiation

☒Enabled

PPTP Callback

Callback

☐Enabled

OK

Cancel

Fig. 146: VPN->PPTP->PPTP Tunnels->New

The **VPN->PPTP->PPTP Tunnels->New** menu consists of the following fields:

Fields in the PPTP Partner Parameters menu.

Field	Description
Description	<p>Enter a unique name for the tunnel.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used.</p>
PPTP Mode	<p>Enter the role to be assigned to the PPTP interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>PNS</i> (default value): this assigns the PPTP interface the role of PPTP server. • <i>Windows Client Mode</i>: This assigns the PPTP interface the role of PPTP client.
User Name	Enter the user name.
Password	Enter the password.
Always on	<p>Select whether the interface should always be activated.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Connection Idle Timeout	<p>Only if Always on is disabled.</p> <p>Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection.</p> <p>Possible values are <i>0</i> to <i>3600</i> (seconds). <i>0</i> deactivates the timeout.</p> <p>The default value is <i>300</i>.</p> <p>Example: <i>10</i> for FTP transmission, <i>20</i> for LAN-to-LAN transmission, <i>90</i> for Internet connections.</p>
Remote PPTP IP Address	<p>Only for PPTP Mode = <i>PNS</i></p> <p>Enter the IP address of the PPTP partner.</p>
Remote PPTP IP Address/Host Name	<p>Only for PPTP Mode = <i>Windows Client Mode</i></p> <p>Enter the IP address of the PPTP partner.</p>

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	<p>Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Static</i> (default value): You enter a static IP address.• <i>Provide IP Address</i>: Only for PPTP Mode = PNS: Your device dynamically assigns an IP address to the remote terminal.• <i>Get IP Address</i>: Only for PPTP Mode = Windows Client Mode: Your device is dynamically assigned an IP address.
Default Route	<p>Only if IP Address Mode = Static</p> <p>Select whether the route to this connection partner is to be defined as the default route.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Create NAT Policy	<p>Only if IP Address Mode = Static</p> <p>When you configure an PPTP connection, specify whether Network Address Translation (NAT) is to be enabled.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Local IP Address	<p>Only for IP Address Mode = Static</p> <p>Assign the IP address from your LAN to the PPTP interface which is to be used as your device's internal source address.</p>
Route Entries	<p>Only if IP Address Mode = Static</p> <p>Define routing entries for this connection partner.</p> <ul style="list-style-type: none">• <i>Remote IP Address</i>: IP address of the destination host or LAN.• <i>Netmask</i>: Netmask for Remote IP Address

Field	Description
	<ul style="list-style-type: none">• <i>Metric</i>: The lower the value, the higher the priority of the route (possible values <i>0 . . . 15</i>). The default value is <i>1</i>.
IP Assignment Pool (IPCP)	<p>Only if PPTP Mode = <i>PNS</i>, IP Address Mode = <i>Provide IP Address</i></p> <p>Select a IP pool configured in the VPN->PPTP->IP Pools menu.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	<p>Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed.</p> <p>The default value is <i>300</i>.</p>
Authentication	<p>Select the authentication protocol for this PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>PAP</i>: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).• <i>PAP/CHAP/MS-CHAP</i>: Give priority to CHAP, if refused use the authentication protocol requested by the PPTP partner. (MSCHAP version 1 or 2 possible.)• <i>MS-CHAPv2</i> (default value): Run MS-CHAP version 2 only.• <i>None</i>: Some providers use no authentication. In this case, select this option.
Encryption	<p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. If Encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i>: MPP encryption is not used.• <i>Enabled</i> (default value): MPP encryption V2 with 128 bit is used to RFC 3078.• <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Compression	<p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): Encryption is not used.• <i>STAC</i>• <i>MS-STAC</i>• <i>MPPC</i>: Microsoft Point-to-Point Compression
LCP Alive Check	<p>Select whether the availability of the remote terminal is to be checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the IP Options menu.

Field	Description
OSPF Mode	<p>Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Passive</i> (default value): OSPF is not activated for this interface, i.e. no routes are propagated or OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces.• <i>Active</i>: OSPF is activated for this interface, i.e. routes are

Field	Description
	<p>propagated or OSPF protocol packets sent over this interface.</p> <ul style="list-style-type: none">• <i>Inactive</i>: OSPF is disabled for this interface.
Proxy ARP Mode	<p>Select whether your device is to answer APR requests from your LAN on behalf of the specific PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Inactive</i> (default value): Disables Proxy-ARP (Address Resolution Protocol) for this PPTP partner.• <i>Up or Dormant</i>: Your device only responds to an ARP request if the status of the connection to the PPTP partner is <i>Up</i> (active) or <i>Dormant</i>. In the case of <i>Idle</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.• <i>Up only</i>: Your device answers an APR request only if the status of the connection to the PPTP partner is <i>Active</i>, i.e. if a connection to the PPTP partner has already been established.
DNS Negotiation	<p>Select whether your device receives IP addresses for Primary DNS Server and Secondary DNS Server from the PPTP partner or sends these to the PPTP partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Fields in the PPTP Callback menu.

Field	Description
Callback	<p>Enables a PPTP tunnel through the Internet to be set up with a PPTP partner, even if the partner is currently inaccessible. As a rule, the PPTP partner will be requested by means of an ISDN call to go online and set up a PPTP connection.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>Note that you must activate the relevant option on the gateways of both partners. An ISDN connection is usually required for this function. Without ISDN, callback is only to be activated in spe-</p>

Field	Description
	cial applications.
Incoming ISDN Number	Only if Callback is enabled. Enter the ISDN number from which the remote device calls the local device (calling party number).
Outgoing ISDN Number	Only if Callback is enabled. Enter the ISDN number with which the local device calls the remote device calls (called party number).

Fields in the Dial Port Selection (only if callback = activated)

Field	Description
Selected Ports	Enter the ISDN port over which callback is carried out. Possible values: <ul style="list-style-type: none">• <i>All Ports</i>: The callback is routed over an available ISDN port.• <i>Specify port</i>: In Specific Ports You can select the required ISDN port.
Specific Ports	Only for Selected Ports = <i>Specify port</i> , you can select additional ports with Add .

18.3.2 Options

In this menu, you can make general settings of the global PPTP profile.

PPTP TunnelsOptionsIP Pools

Global Options

GRE Window Adaption	<input checked="" type="checkbox"/> Enabled
GRE Window Size	<input type="text" value="0"/>
Max. incoming control connections per remote IP Address	<input type="text" value="1"/>

OK

Cancel

Fig. 147: VPN->PPTP->Options

The **VPN->PPTP->Options** menu consists of the following fields:

Fields in the Global Options menu.

Field	Description
GRE Window Adaption	<p>Select whether the GRE Window Adaptation is to be enabled.</p> <p>This adaptation only becomes necessary if you have installed service pack 1 from Microsoft Windows XP. Since, in SP 1, Microsoft has changed the confirmation algorithm in the GRE protocol, the automatic window adaptation for GRE must be turned off for bintec elmeg devices.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
GRE Window Size	<p>Enter the maximum number of GRE packets that can be sent without confirmation.</p> <p>Windows XP uses a higher initial reception window in the GRE, which is why the maximum send window size must be adjusted here by the GRE Window Size value. Possible values are 0 to 256.</p> <p>The default value is 0.</p>
Max. incoming control connections per remote IP Address	<p>Enter the maximum number of control connections.</p>

18.3.3 IP Pools


The **IP Pools** menu displays a list of all IP pools for PPTP connections.

Your device can operate as a dynamic IP address server for PPTP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address assigned to this partner the last time.

Choose the **Add** button to set up new IP pools.

18.3.3.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

PPTP TunnelsOptionsIP Pools

Basic Parameters

IP Pool Name

IP Address Range

 -

DNS Server

Primary

Secondary

OK

Cancel

Fig. 148: VPN->PPTP->IP Pools->New

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. Secondary: Optionally, enter the IP address of an alternative DNS server.

18.4 GRE

Generic Routing Encapsulation (GRE) is a network protocol that encapsulates other protocols and transports them in the form of IP tunnels to the specified recipients.

The specification of the GRE protocol is available in two versions:

- GRE V.1 for use in PPTP connections (RFC 2637, configuration in the **PPTP** menu)
- GRE V.0 (RFC 2784) for general encapsulation using GRE

In this menu you can configure a virtual interface for using GRE V.0. The data traffic routed

over this interface is then encapsulated using GRE and sent to the specified recipient.

18.4.1 GRE Tunnels

A list of all configured GRE tunnels is displayed in the **VPN->GRE->GRE Tunnels** menu.

18.4.1.1 New

Choose the **New** button to set up new GRE tunnels.

GRE Tunnels

Basic Parameters

Description	<input type="text"/>												
Local GRE IP Address	<input type="text"/>												
Remote GRE IP Address	<input type="text"/>												
Default Route	<input type="checkbox"/> Enabled												
Local IP Address	<input type="text"/>												
Route Entries	<table><tr><td>Remote IP Address</td><td>Netmask</td><td>Metric</td><td></td></tr><tr><td><input type="text"/></td><td><input type="text"/></td><td>1</td><td><input type="button" value="v"/></td></tr><tr><td colspan="4"><input type="button" value="Add"/></td></tr></table>	Remote IP Address	Netmask	Metric		<input type="text"/>	<input type="text"/>	1	<input type="button" value="v"/>	<input type="button" value="Add"/>			
Remote IP Address	Netmask	Metric											
<input type="text"/>	<input type="text"/>	1	<input type="button" value="v"/>										
<input type="button" value="Add"/>													
MTU	<input type="text" value="1500"/>												
Use key	<input type="checkbox"/> Enabled												

Fig. 149: **VPN->GRE->GRE Tunnels->New**

The **VPN->GRE->GRE Tunnels->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE partner. If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.
Remote GRE IP Address	Enter the target IP address of the GRE packets to the GRE partner.

Field	Description
Default Route	<p>If you enable the Default Route, all data is automatically routed to one connection.</p> <p>The function is disabled by default.</p>
Local IP Address	<p>Here, enter the (LAN-side) IP address that is to be used as your device's source address for your own packets through the GRE tunnel.</p>
Route Entries	<p>Define other routing entries for this connection partner.</p> <p>Add new entries with Add.</p> <ul style="list-style-type: none">• <i>Remote IP Address</i>: IP address of the destination host or network.• <i>Netmask</i>: Netmask for Remote IP Address If no entry is made, your device uses a default netmask.• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values <i>0... 15</i>). The default value is <i>1</i>.
MTU	<p>Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners.</p> <p>Possible values are <i>1</i> to <i>8192</i>.</p> <p>The default value is <i>1500</i>.</p>
Use key	<p>Enable the key input for the GRE connection, which makes it possible to distinguish between several parallel GRE connections between two GRE partners (see RFC 1701).</p> <p>The identification is enabled with <i>Enabled</i></p> <p>The function is disabled by default.</p>
Key Value	<p>Only if Use key is enabled.</p> <p>Enter the GRE connection key.</p> <p>Possible values are <i>0</i> to <i>2147483647</i>.</p> <p>The default value is <i>0</i>.</p>

Chapter 19 Firewall

The Stateful Inspection Firewall (SIF) provided for bintec elmeg gateways is a powerful security feature.

The SIF with dynamic packet filtering has a decisive advantage over static packet filtering: The decision whether or not to send a packet cannot be made solely on the basis of source and destination addresses or ports but also using dynamic packet filtering based on the state of the connection to a partner.

This means packets that belong to an already active connection can also be forwarded. The SIF also accepts packets that belong to an "affiliated connection". The negotiation of an FTP connection takes place over port 21, for example, but the actual data exchange can take place over a completely different port.

SIF and other security features

The Stateful Inspection Firewall fits into the existing security architecture of bintec elmeg. The configuration work for the SIF is comparatively straightforward with systems like Network Address Translation (NAT) and IP Access Lists (IPAL).

As SIF, NAT and IPAL are active in the system simultaneously, attention must be given to possible interaction: If any packet is rejected by one of the security instances, this is done immediately. This is irrelevant whether another instance would accept it or not. Your need for security features should therefore be accurately analysed.

The essential difference between SIF and NAT/IPAL is that the rules for the SIF are generally applied globally, i.e. not restricted to one interface.

In principle, the same filter criteria are applied to the data traffic as those used in NAT and IPAL:

- Source and destination address of the packet (with an associated netmask)
- Service (preconfigured, e.g. Echo, FTP, HTTP)
- Protocol
- Port number(s)

To illustrate the differences in packet filtering, a list of the individual security instances and their method of operation is given below.

NAT

One of the basic functions of NAT is the translation of the local IP addresses of your LAN into the global IP addresses you are assigned by your ISP and vice versa. All connections initiated externally are first blocked, i.e. every packet your device cannot assign to an existing connection is rejected. This means that a connection can only be set up from inside to outside. Without explicit permission, NAT rejects every access from the WAN to the LAN.

IP Access Lists

Here, packets are allowed or rejected exclusively on the basis of the criteria listed above, i.e. the state of the connection is not considered (except for **Services** = *TCP*).

SIF

The SIF sorts out all packets that are not explicitly or implicitly allowed. The result can be a "deny", in which case no error message is sent to the sender of the rejected packet, or a "reject", where the sender is informed of the packet rejection.

The incoming packets are processed as follows:

- The SIF first checks if an incoming packet can be assigned to an existing connection. If so, it is forwarded. If the packet cannot be assigned to an existing connection, a check is made to see if a suitable connection is expected (e.g. as affiliated connection of an existing connection). If so, the packet is also accepted.
- If the packet cannot be assigned to any existing or expected connection, the SIF filter rules are applied: If a deny rule matches the packet, the packet is discarded without sending an error message to the sender of the packet; if a reject rule matches, the packet is discarded and an ICMP Host Unreachable message sent to the sender of the packet. The packet is only forwarded if an accept rule matches.
- All packets without matching rules are rejected without sending an error message to the sender when all the existing rules have been checked (=default behaviour).

19.1 Policies

19.1.1 Filter Rules

The default behaviour with **Action** = *Access* consists of two implicit filter rules: If an incoming packet can be assigned to an existing connection and if a suitable connection is expected (e.g. such as an affiliated connection of an existing connection), the packet is allowed.

The sequence of filter rules in the list is relevant: The filter rules are applied to each packet

in succession until a rule matches. If overlapping occurs, i.e. more than one filter rule matches a packet, only the first rule is executed. This means that if the first rule denies a packet, whereas a later rule allows it, the packet is rejected. A deny rule also has no effect if a relevant packet has previously been allowed by another filter rule.

A list of all configured filter rules is displayed in the **Firewall->Policies->Filter Rules** menu.

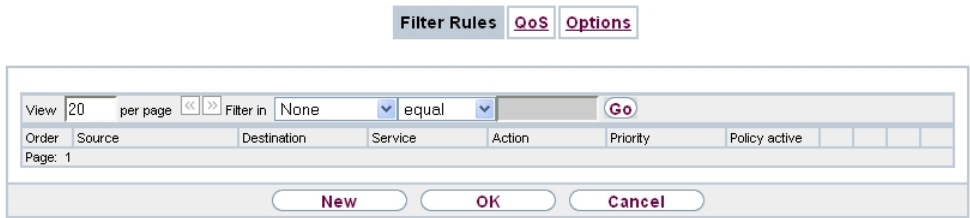




Fig. 150: Firewall->Policies->Filter Rules

You can use the  button to insert another policy above the list entry. The configuration menu for creating a new policy opens.

You can use the  button to move the list entry. A dialog box opens, in which you can select the position to which the policy is to be moved.

19.1.1.1 New

Choose the **New** button to create additional parameters.

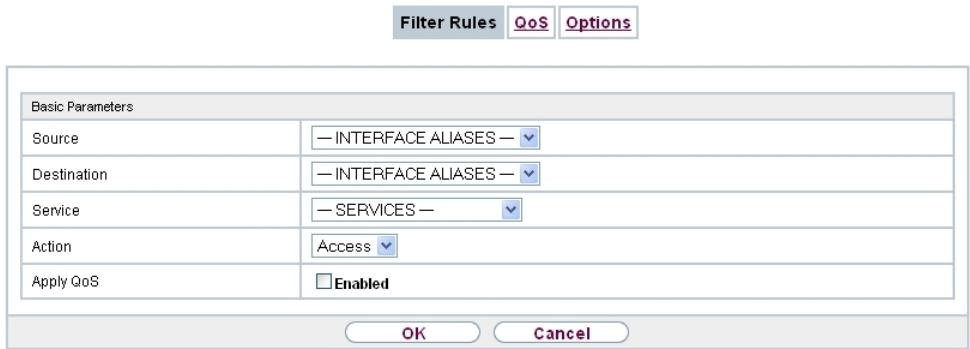


Fig. 151: Firewall->Policies->Filter Rules->New

The menu **Firewall->Policies->Filter Rules->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Source	<p>Select one of the preconfigured aliases for the source of the packet.</p> <p>In the list, all WAN/LAN interfaces, interface groups (see Firewall->Interfaces->Groups), addresses (see Firewall->Addresses->Address List) and address groups (see Firewall->Addresses->Groups) are available.</p> <p>The value <i>Any</i> means that neither the source interface nor the source address is checked.</p>
Destination	<p>Select one of the preconfigured aliases for the destination of the packet.</p> <p>In the list, all WAN/LAN interfaces, interface groups (see Firewall->Interfaces->Groups), addresses (see Firewall->Addresses->Address List) and address groups (see Firewall->Addresses->Groups).</p> <p>The value <i>Any</i> means that neither the destination interface nor the destination address is checked.</p>
Service	<p>Select one of the preconfigured services to which the packet to be filtered must be assigned.</p> <p>The extensive range of services configured ex works includes the following:</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>Additional services are created in Firewall->Services->Service List.</p> <p>In addition, the service groups configured in Firewall->Services->Groups can be selected.</p>

Field	Description
Action	<p>Select the action to be applied to a filtered packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Access</i> (default value): The packets are forwarded on the basis of the entries. • <i>Deny</i>: The packets are rejected. • <i>Reject</i>: The packets are rejected. An error message is issued to the sender of the packet.
Apply QoS	<p>Only for Action = <i>Access</i></p> <p>Select whether you want to enable QoS for this policy with the priority selected in Priority.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The option is deactivated by default.</p> <p>If QoS is not activated for this policy, bear in mind that the data cannot be prioritised on the sender side either.</p> <p>A policy for which QoS has been enabled is also set for the firewall. Make sure therefore that data traffic that has not been expressly authorised is blocked by the firewall!</p>
Priority	<p>Only for Action = <i>Access</i> and Apply QoS = <i>Enabled</i></p> <p>Select the priority with which the data specified by the policy is handled on the send side.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i> (default value): No priority. • <i>Low Latency</i>: Low Latency Transmission (LTT), i.e. handling of data with the lowest possible latency, e.g. suitable for VoIP data. • <i>High</i> • <i>Medium</i> • <i>Low</i>

19.1.2 QoS

More and more applications need increasingly larger bandwidths, which are not always available. Quality of Service (QoS) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them.

A list of all QoS rules is displayed in the **Firewall->Policies->QoS** menu.

19.1.2.1 New

Choose the **New** button to set up new QoS rules.



Fig. 152: Firewall->Policies->QoS->New

The **Firewall->Policies->QoS->New** menu consists of the following fields:

Fields in the Configure QoS Interface menu.

Field	Description
Interface	Select the interface on which bandwidth management is to be carried out.
Traffic Shaping	Select whether you want to activate bandwidth management for the selected interface. The function is enabled with <i>Enabled</i> . The function is disabled by default.
Specify bandwidth	Only for Traffic Shaping = <i>Enabled</i> Enter the maximum available bandwidth in kbps for the selected interface.

Field	Description
Filter Rules	<p>This field contains a list of all configured firewall policies for which QoS was activated (Apply QoS = <i>Enabled</i> under Firewall->Policies->Filter Rules->New).</p> <p>The following options are available for each list entry:</p> <ul style="list-style-type: none">• Use: Select whether this entry should be assigned to the QoS interface. The option is deactivated by default.• Bandwidth: Enter the maximum available bandwidth in Bit/s for the service specified under Service. 0 is entered by default.• Bounded: Select whether the bandwidth defined in Bandwidth can be exceeded in the longer term. By activating this field, you specify that it cannot be exceeded. If the option is deactivated, the bandwidth can be exceeded and the excess data rate is handled in accordance with the priority defined in the firewall policy. The option is deactivated by default.

19.1.3 Options

In this menu, you can disable or enable the firewall and can log its activities. In addition, you can define after how many seconds of inactivity a session shall be ended.

Filter Rules

QoS

Options

Global Firewall Options

Firewall Status	<input checked="" type="checkbox"/> Enabled
Logged Actions	All
Full Filtering	<input checked="" type="checkbox"/> Enable
Session Timer	
UDP Inactivity	180 Seconds
TCP Inactivity	3600 Seconds
PPTP Inactivity	86400 Seconds
Other Inactivity	30 Seconds

OK

Cancel

Fig. 153: Firewall->Policies->Options

The menu **Firewall->Policies->Options** consists of the following fields:

Fields in the Global Firewall Options menu.

Field	Description
Firewall Status	Enable or disable the firewall function. The function is enabled with <i>Enabled</i> The function is enabled by default.
Logged Actions	Select the firewall syslog level. The messages are output together with messages from other subsystems. Possible values: <ul style="list-style-type: none">• <i>All</i> (default value): All firewall activities are displayed.• <i>Deny</i>: Only reject and deny events are shown, see "Action".• <i>Accept</i>: Only accept events are shown.• <i>None</i>: Syslog messages are not generated.
Full Filtering	Here you define whether packets are only to be filtered if they are sent to an interface other than the interface that created the connection. With <i>Enable</i> , all the packets are filtered (default value).

Fields in the Session Timer menu.

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are <i>30</i> to <i>86400</i> . The default value is <i>180</i> .
TCP Inactivity	Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds). Possible values are <i>30</i> to <i>86400</i> . The default value is <i>3600</i> .
PPTP Inactivity	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds).

Field	Description
	Possible values are 30 to 86400. The default value is 86400.
Other Inactivity	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds). Possible values are 30 to 86400. The default value is 30.

19.2 Interfaces

19.2.1 Groups

A list of all configured interface routes is displayed in the **Firewall->Interfaces->Groups** menu.

You can group together the interfaces of your device. This makes it easier to configure fire-wall rules.

19.2.1.1 New

Choose the **New** button to set up new interface groups.

Groups

Basic Parameters

Description

Members

Interface	Selection
LOCAL	<input type="checkbox"/>
LAN_EN1-0	<input type="checkbox"/>
LAN_EN1-4	<input type="checkbox"/>

OK

Cancel

Fig. 154: **Firewall->Interfaces->Groups->New**

The menu **Firewall->Interfaces->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the Selection column.

19.3 Addresses

19.3.1 Address List

A list of all configured addresses is displayed in the **Firewall->Addresses->Address List** menu.

19.3.1.1 New

Choose the **New** button to create additional addresses.

Address List

Groups

Basic Parameters

Description

Address Type

☒ Address / Subnet

☐ Address Range

Address / Subnet

/

OK

Cancel

Fig. 155: Firewall->Addresses->Address List->New

The menu **Firewall->Addresses->Address List->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address.
Address Type	Select the type of address you want to specify. Possible values: <ul style="list-style-type: none"><i>Address / Subnet</i> (default value): Enter an IP address with subnet mask.

Field	Description
	<ul style="list-style-type: none"><i>Address Range</i>: Enter an IP address range with a start and end address.
Address / Subnet	<p>Only for Address Type = <i>Address / Subnet</i></p> <p>Enter the IP address of the host or a network address and the related netmask.</p> <p>The default value is <i>0.0.0.0</i>.</p>
Address Range	<p>Only for Address Type = <i>Address Range</i></p> <p>Enter the start and end IP address of the range.</p>

19.3.2 Groups

A list of all configured address groups is displayed in the **Firewall->Addresses->Groups** menu.

You can group together addresses. This makes it easier to configure firewall rules.

19.3.2.1 New

Choose the **New** button to set up additional address groups.

Address List

Groups

Basic Parameters

Description

Selection

Addresses

Selection

ANY

☐

OK

Cancel

Fig. 156: **Firewall->Addresses->Groups->New**

The menu **Firewall->Addresses->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address group.

Field	Description
Selection	Select the members of the group from the available Addresses . To do this, activate the Fields in the Selection column.

19.4 Services

19.4.1 Service List

In the **Firewall->Services->Service List** menu, a list of all available services is displayed.

19.4.1.1 New

Choose the **New** button to set up additional services.

Service List

Groups

Basic Parameters

Description

Protocol

Any

OK

Cancel

Fig. 157: **Firewall->Services->Service List->New**

The menu **Firewall->Services->Service List->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter an alias for the service you want to configure.
Protocol	Select the protocol on which the service is to be based. The most important protocols are available for selection.
Destination Port Range	<p>Only for Protocol = <i>TCP, UDP/TCP</i> or <i>UDP</i></p> <p>In the first field, enter the destination port via which the service is to run.</p> <p>If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously</p>

Field	Description
	<p>specified port number is verified. If a port range is to be checked, enter the upper limit here.</p> <p>Possible values are <i>1</i> to <i>65535</i>.</p>
Source Port Range	<p>Only for Protocol = <i>TCP</i>, <i>UDP/TCP</i> or <i>UDP</i></p> <p>In the first field, enter the source port to be checked, if applicable.</p> <p>If a port number range is specified, in the second field enter the last port of the port range. By default the field does not contain an entry. If a value is displayed, this means that the previously specified port number is verified. If a port range is to be checked, enter the upper limit here.</p> <p>Possible values are <i>1</i> to <i>65535</i>.</p>
Type	<p>Only for Protocol = <i>ICMP</i></p> <p>The Type field shows the class of ICMP messages, the Code field specifies the type of message in greater detail.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <i>Echo Reply</i>• <i>Destination Unreachable</i>• <i>Source Quench</i>• <i>Redirect</i>• <i>Echo</i>• <i>Time Exceeded</i>• <i>Parameter Problem</i>• <i>Timestamp</i>• <i>Timestamp Reply</i>• <i>Information Request</i>• <i>Information Reply</i>• <i>Address Mask Request</i>• <i>Address Mask Reply</i>

Field	Description
Code	<p>Selection options for the ICMP codes are only available for Type = <i>Destination Unreachable</i></p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Any</i> (default value)• <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>

19.4.2 Groups

A list of all configured service groups is displayed in the **Firewall->Services->Groups** menu.

You can group together services. This makes it easier to configure firewall rules.

19.4.2.1 New

Choose the **New** button to set up additional service groups.

Service List

Groups

Basic Parameters

Description

Members

Service	Selection
KaZaA	<input type="checkbox"/>
activity	<input type="checkbox"/>
any	<input type="checkbox"/>
apple-qt	<input type="checkbox"/>
auth	<input type="checkbox"/>
chargen	<input type="checkbox"/>
clients_1	<input type="checkbox"/>
clients_2	<input type="checkbox"/>
daytime	<input type="checkbox"/>
dhcp	<input type="checkbox"/>
discard	<input type="checkbox"/>
dns	<input type="checkbox"/>
echo	<input type="checkbox"/>
exec	<input type="checkbox"/>
unpriv	<input type="checkbox"/>
ups	<input type="checkbox"/>
uucp-path	<input type="checkbox"/>
who	<input type="checkbox"/>
whois	<input type="checkbox"/>
wins	<input type="checkbox"/>
x400	<input type="checkbox"/>

OK

Cancel

Fig. 158: Firewall->Services->Groups->New

The menu **Firewall->Services->Groups->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the Fields in the Selection column.

Chapter 20 VoIP

Voice over IP (VoIP) uses the IP protocol for voice and video transmission.

The main difference compared with conventional telephony is that the voice information is not transmitted over a switched connection in a telephone network, but divided into data packets by the Internet protocol and these packets are then passed to the destination over undefined paths in a network. This technology uses the existing network infrastructure for voice transmission and shares this with other communication services.

The Session Initiation Protocol (SIP) is used to establish, clear and control a communication session.

20.1 SIP

SIP serves as a translation instance between different telecommunications networks, e.g between the plain old phone network and the next generation networks (IP networks).

20.1.1 Options

In the **VoIP->SIP->Options** menu, you can make global settings for the SIP.

Options

Basic Parameters	
SIP Proxy	<input type="checkbox"/> Enabled
SIP Port	5060
Prioritize SIP Calls	<input type="checkbox"/> Enabled

OKCancel

Fig. 159: VoIP->SIP->Options

The **VoIP->SIP->Options** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
SIP Proxy	Select whether you want to activate the SIP proxy. The function is enabled with <i>Enabled</i> .

Field	Description
	The function is disabled by default.
SIP Port	<p>Enter the port to be supervised by the proxy.</p> <p>You must configure a proxy for each destination port to which VoIP clients from the LAN can connect.</p> <p>The ports can be provider-specific.</p> <p>The default value is <i>5060</i>.</p>
Prioritize SIP Calls	<p>Select whether you want to prioritise SIP Calls.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

20.2 RTSP

In this menu, you configure the use of the RealTime Streaming protocol (RTSP).

RTSP is a network protocol for controlling multimedia traffic flows in IP-based networks. Payload data is not transferred using RTSP. Rather, it is used to control a multimedia session between sender and recipient.

If you want to use RTSP, the firewall and NAT must be configured accordingly. In the **VoIP->RTSP** menu, you can activate the RTSP proxy to enable requested RTSP sessions over the defined port if required.

20.2.1 RTSP Proxy

In the **VoIP->RTSP->RTSP Proxy** menu, you configure the use of the RealTime Streaming protocol.

RTSP Proxy

Basic Parameters

RTSP Proxy

☐ Enabled

RTSP Port

554

OK

Cancel

Fig. 160: **VoIP->RTSP->RTSP Proxy**

The **VoIP->RTSP->RTSP Proxy** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
RTSP Proxy	<p>Select whether you want to permit RTSP sessions.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
RTSP Port	<p>Select the port over which the RTSP messages are to come in and go out.</p> <p>Possible values are <i>0</i> to <i>65535</i>.</p> <p>The default value is <i>554</i>.</p>

Chapter 21 Local Services

This menu offers services for the following application areas:

- Name resolution (DNS)
- Configuration via web browser (HTTPS)
- Locating of dynamic IP addresses using a DynDNS provider
- Configuration of gateway as a DHCP server (assignment of IP addresses)
- Access restriction on the Internet (web filter)
- Automation of tasks according to schedule (scheduling)
- Alive checks for hosts or interfaces, ping tests
- Realtime video/audio conferences (Messenger services, universal plug & play)
- Provision of public Internet accesses (hotspot).
- Use of a redundant gateway (BRRP).

21.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

- DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
- DNS cache, for saving the positive and negative results of DNS requests.
- Static entries (static hosts), to manually define or prevent assignments of IP addresses to names.
- DNS monitoring (statistics), to provide an overview of DNS requests on your device.

Name server

Under **Local Services->DNS->DNS Servers->New** you enter the IP addresses of name servers that are queried if your device cannot answer requests itself or by forwarding entries. Global name servers and name servers that are attached to an interface can both be entered.

Your device can also receive the global name servers dynamically via PPP or DHCP and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

- (1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.
- (2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.
- (3) Otherwise, if name servers have been entered, taking into account the priority configured and if the relevant interface status is "up", the primary DNS server is queried and then the secondary DNS server. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.
- (4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.
- (5) Otherwise, if overwriting the addresses of the global name servers is allowed in the **WAN->Internet + Dialup** menu (**Interface Mode** = *Dynamic*), a connection is set up – if necessary at extra cost – to the first Internet or dialin connection configured to enable DNS server addresses to be requested from DNS servers (**DNS Negotiation** = *Enabled*), if this has not been already attempted. When the name servers have been negotiated successfully, these name servers are then available for more queries.
- (6) Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with `non-existent domain`, the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of your device.

21.1.1 Global Settings

Global Settings

DNS Servers

Static Hosts

Domain Forwarding

Cache

Statistics

Basic Parameters

Domain Name

WINS Server

Primary

0.0.0.0

Secondary

0.0.0.0

Advanced Settings

Positive Cache

☒ Enabled

Negative Cache

☒ Enabled

Cache Size

100

Entries

Maximum TTL for Positive Cache Entries

86400

Seconds

Maximum TTL for Negative Cache Entries

300

Seconds

Fallback interface to get DNS server

Automatic

IP address to use for DNS/WINS server assignment

As DHCP Server

☐ None

☒ Own IP Address

☐ DNS Setting

As IPCP Server

☐ None

☐ Own IP Address

☒ DNS Setting

OK

Cancel

Fig. 161: Local Services->DNS->Global Settings

The menu **Local Services->DNS->Global Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Domain Name	Enter the standard domain name of your device.
WINS Server	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).
Primary	
Secondary	

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated,

Field	Description
	<p>i.e. successfully resolved names and IP addresses are to be stored in the cache.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Negative Cache	<p>Select whether the negative dynamic cache is to be activated, i.e. whether queried names for which a DNS server has sent a negative response are stored as negative entries in the cache.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Cache Size	<p>Enter the maximum total number of static and dynamic entries.</p> <p>Once this value is reached, the dynamic entry not requested for the longest period of time is deleted when a new entry is added. Cache Size is reduced by the user, dynamic entries are deleted if necessary. Statistical entries are not deleted. Cache Size cannot be set to lower than the current number of static entries.</p> <p>Possible values: <i>0.. 1000</i>.</p> <p>The default value is <i>100</i>.</p>
Maximum TTL for Positive Cache Entries	<p>Enter the value to which the TTL is to be set for a positive dynamic DNS entry in the cache if its TTL is <i>0</i> or its TTL exceeds the value for Maximum TTL for Positive Cache Entries .</p> <p>The default value is <i>86400</i>.</p>
Maximum TTL for Negative Cache Entries	<p>Enter the value set to which the TTL is to be set in the case of a negative dynamic entry in the cache.</p> <p>The default value is <i>86400</i>.</p>
Fallback interface to get DNS server	<p>Select the interface to which a connection is set up for name server negotiation if other name resolution attempts were not successful.</p> <p>The default value is <i>Automatic</i>, i.e. a one-time connection is set up to the first suitable connection partner configured in the system.</p>


Fields in the IP address to use for DNS/WINS server assignment menu.

Field	Description
As DHCP Server	<p>Select which name server addresses are sent to the DHCP client if your device is used as DHCP server.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i>: No name server address is sent.• <i>Own IP Address</i> (default value): The address of your device is transferred as the name server address.• <i>DNS Setting</i>: The addresses of the global name servers entered on your device are sent.
As IPCP Server	<p>Select which name server addresses are to be transmitted by your device in the event of dynamic server name negotiation if your device is used as the IPCP server for PPP connections.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i>: No name server address is sent.• <i>Own IP Address</i>: The address of your device is transferred as the name server address.• <i>DNS Setting</i> (default value): The addresses of the global name servers entered on your device are sent.

21.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services->DNS->DNS Servers** menu.

21.1.2.1 Edit or New

Choose the  icon to edit existing entries. Select the **New** button to set up additional DNS servers.

Here you can configure both global DNS servers and DNS servers that are to be assigned to a particular interface.

Configuring a DNS server for a particular interface can be useful, for example, if accounts with different providers have been set up via different interfaces and load balancing is being used.

Global Settings

DNS Servers

Static Hosts

Domain Forwarding

Cache

Statistics

Basic Parameters

Admin Status

☒ Enabled

Description

Priority

5

Interface Mode

☐ Static ☒ Dynamic

Interface

None

OK

Cancel

Fig. 162: Local Services->DNS->DNS Servers->New

The **Local Services->DNS->DNS Servers->New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Admin Status	<p>Select whether the DNS server should be enabled.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Description	<p>Enter a description for DNS server.</p>
Priority	<p>Assign a priority to the DNS server.</p> <p>You can assign more than one pair of DNS servers (Primary DNS Server and Secondary DNS Server) to an interface (i. e. for example, to an Ethernet port or a PPPoE WAN partner). The pair with the highest priority is used if the interface is "up".</p> <p>Possible values from <i>0</i> (highest priority) to <i>9</i> (lowest priority).</p> <p>The default value is <i>5</i>.</p>
Interface Mode	<p>Select whether the IP addresses of name servers for resolving the names of Internet addresses are to be obtained automatically or whether up to two fixed DNS server addresses are to be entered, depending on the priority.</p> <p>Possible values:</p> <ul style="list-style-type: none"><i>Static</i>

Field	Description
	<ul style="list-style-type: none"><i>Dynamic</i> (default value)
Interface	<p>Select the interface to which the DNS server pair is to be assigned.</p> <p>For Interface Mode = <i>Dynamic</i></p> <p>A global DNS server is created with the setting <i>None</i>.</p> <p>For Interface Mode = <i>Static</i></p> <p>A DNS server is configured for all interfaces with the <i>Any</i> setting.</p>
Primary DNS Server	<p>Only if Interface Mode = <i>Static</i></p> <p>Enter the IP address of the first name server for Internet address name resolution.</p>
Secondary DNS Server	<p>Only if Interface Mode = <i>Static</i></p> <p>Optionally, enter the IP address of an alternative name server.</p>

21.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services->DNS->Static Hosts** menu.

21.1.3.1 New

Choose the **New** button to set up new static hosts.

Global SettingsDNS ServersStatic HostsDomain ForwardingCacheStatistics

Basic Parameters

DNS Hostname

Response

Positive

IP Address

0.0.0.0

TTL

86400

Seconds

OK

Cancel

Fig. 163: Local Services->DNS->Static Hosts->New

The menu **Local Services->DNS->Static Hosts->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
DNS Hostname	<p>Enter the host name to which the IP Address defined in this menu is to be assigned if a positive response is received to a DNS request. If a negative response is received to a DNS request, no address is specified.</p> <p>The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com.</p> <p>If a name is entered without a dot, this is completed with OK "<Name.> " after confirmation.</p> <p>Entries with spaces are not allowed.</p>
Response	<p>In this entry, select the type of response to DNS requests.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Negative</i>: A DNS request for DNS Hostname gets a negative response.• <i>Positive</i> (default value): A DNS request for DNS Hostname is answered with the related IP Address.• <i>None</i>: A DNS request is ignored; no answer is given.
IP Address	<p>Only if Response = <i>Positive</i></p> <p>Enter the IP address assigned to DNS Hostname.</p>
TTL	<p>Enter the validity period of the assignment from DNS Hostname to IP Address in seconds (only relevant for Response = <i>Positive</i>) transmitted to requesting hosts.</p> <p>The default value is <i>86400</i> (= 24 h).</p>

21.1.4 Domain Forwarding

In the **Local Services->DNS->Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

21.1.4.1 New

Choose the **New** button to set up additional forwardings.

Global SettingsDNS ServersStatic HostsDomain ForwardingCacheStatistics

Forwarding Parameters

Forward

☒ Host ☐ Domain

Host

Forward to

☒ Interface ☐ DNS Server

Interface

Automatic

OK

Cancel

Fig. 164: Local Services->DNS->Domain Forwarding->New

The menu **Local Services->DNS->Domain Forwarding->New** consists of the following fields:

Fields in the Forwarding Parameters menu.

Field	Description
Forward	<p>Select whether a host or domain is to be forwarded.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Host</i> (default value)• <i>Domain</i>
Host	<p>Only for Forwarding = <i>Host</i></p> <p>Enter the name of the host to be forwarded.</p> <p>The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If a name is entered without a full stop, you complete with OK " <Default Domain>." " is added.</p>
Domain	<p>Only for Forwarding = <i>Domain</i></p> <p>Enter the name of the domain to be forwarded.</p> <p>The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If a name is entered without a full stop, you complete with OK " <Default Domain>." " is added.</p>

Field	Description
Forward to	<p>Select the forwarding destination requests to the name defined in Host or Domain.</p> <p>Possible values:</p> <ul style="list-style-type: none"><i>Interface</i> (default value): The request is forwarded to the defined Interface.<i>DNS Server</i>: The request is forwarded to the defined DNS Server.
Interface	<p>Only for Forward to = <i>Interface</i></p> <p>Select the interface via which the requests for the defined Domain are to be received and forwarded to the DNS server.</p>
DNS Server	<p>Only for Forward to = <i>DNS Server</i></p> <p>Enter the IP address of the primary and secondary DNS server.</p>

21.1.5 Cache

In the **Local Services->DNS->Cache** menu, a list of all available cache entries is displayed.

Global SettingsDNS ServersStatic HostsDomain ForwardingCacheStatistics

Automatic Refresh Interval60SecondsApply

View20per page<<>>Filter inNoneequalGo

Description	IP Address	Response	TTL	Reference Counter	Select all / Deselect all	Make static
Page: 1						

OKCancel

Fig. 165: Local Services->DNS->Cache

You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button.

A dynamic entry can be converted to a static entry by marking the entry and confirming with **Make static**. This corresponding entry disappears from the list and is displayed in the list in the **Static Hosts** menu. The TTL is transferred.

21.1.6 Statistics

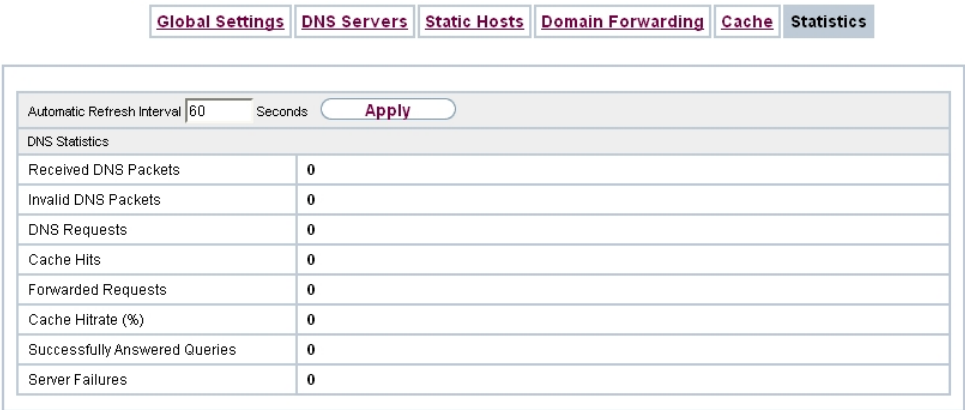


Fig. 166: Local Services->DNS->Statistics

In the **Local Services->DNS->Statistics** menu, the following statistical values are displayed:

Fields in the DNS Statistics menu.

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.
Cache Hitrate (%)	Indicates the number of Cache Hits pro DNS request in percentage.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

21.2 HTTPS

You can operate the user interface of your device from any PC with an up-to-date Web browser via an HTTPS connection.

HTTPS (HyperText Transfer Protocol Secure) is the procedure used to establish an encrypted and authenticated connection by SSL between the browser used for configuration and the device.

21.2.1 HTTPS Server

In the **Local Services->HTTPS->HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

HTTPS Server

HTTPS Parameters

HTTPS TCP Port

443

Local Certificate

Internal

Apply

Cancel

Fig. 167: Local Services->HTTPS->HTTPS Server

The **Local Services->HTTPS->HTTPS Server** menu consists of the following fields:

Fields in the HTTPS Parameters menu.

Field	Description
HTTPS TCP Port	<div>Enter the port via which the HTTPS connection is to be established.</div> <div>Possible values are 0 to 65535.</div> <div>The default value is 443.</div>
Local Certificate	<div>Select a certificate that you want to use for the HTTPS connection.</div> <div>Possible values:</div> <div><ul style="list-style-type: none"><i>Internal</i> (default value): Select this option if you want to use the certificate built into the device.</div>

Field	Description
	<ul style="list-style-type: none">• <i><Certificate name></i>: Under System Management->Certificates->Certificate List select entered certificate.

21.3 DynDNS Client

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. DynDNS ensures that your device can still be reached after a change to the IP address.

The following configuration steps are necessary:

- Registration of a host name at a DynDNS provider
- Configuration of your device

Registration

The registration of a host name means that you define an individual user name for the DynDNS service, e.g. *dyn_client*. The service providers offer various domain names for this, so that a unique host name results for your device , e.g. *dyn_client.provider.com*. The DynDNS provider relieves you of the task of answering all DNS requests concerning the host *dyn_client.provider.com* with the dynamic IP address of your device.

To ensure that the provider always knows the current IP address of your device, your device contacts the provider when setting up a new connection and propagates its present IP address.

21.3.1 DynDNS Update

In the **Local Services->DynDNS Client->DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed

21.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

DynDNS Update

DynDNS Provider

Basic Parameters

Host Name

Interface

Select one

User Name

Password

••••••••

Provider

dyndns

Enable update

☐ Enabled

Advanced Settings

Mail Exchanger (MX)

Wildcard

☐ Enabled

OK

Cancel

Fig. 168: Local Services->DynDNS Client->DynDNS Update->New

The menu **Local Services->DynDNS Client->DynDNS Update->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host Name	Enter the complete host name as registered with the DynDNS provider.
Interface	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.
Provider	<p>Select the DynDNS provider with which the above data is registered.</p> <p>A choice of DynDNS providers is already available in the unconfigured state and their protocols are supported.</p> <p>Other DynDNS providers can be configured in the Local Services->DynDNS Client->DynDNS Provider menu.</p>

Field	Description
	The default value is <i>DynDNS</i> .
Enable update	Select whether the DynDNS entry configured here is to be activated. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether forwarding of all subdomains of the Host Name is to be enabled for the current IP address of the Interface (advanced name resolution). The function is activated by selecting <i>Enabled</i> . The function is disabled by default.

21.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services->DynDNS Client->DynDNS Provider** menu.

21.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

DynDNS Update

DynDNS Provider

Basic Parameters

Provider Name	<input type="text"/>
Server	<input type="text"/>
Update Path	<input type="text"/>
Port	<input type="text" value="80"/>
Protocol	<div>DynDNS</div>
Update Interval	<input type="text" value="300"/> Seconds

OK

Cancel

Fig. 169: Local Services->DynDNS Client->DynDNS Provider->New

The menu **Local Services->DynDNS Client->DynDNS Provider->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is 80.
Protocol	Select one of the protocols implemented. Possible values: <ul style="list-style-type: none">DynDNS (default value)Static DynDNSODS

Field	Description
	<ul style="list-style-type: none">• <i>HN</i>• <i>DYNS</i>• <i>GnuDIP-HTML</i>• <i>GnuDIP-TCP</i>• <i>Custom DynDNS</i>• <i>DnsExit</i>
Update Interval	<p>Enter the minimum time (in seconds) that your device must wait before it is allowed to propagate its current IP address to the DynDNS provider again.</p> <p>The default value is <i>300</i> seconds.</p>

21.4 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool.


If a client requires an IP address for the first time, it sends a DHCP request (with its MAC address) to the available DHCP server as a network broadcast.* The client then receives its IP address from bintec elmeg (as part of a brief exchange).

You therefore do not need to allocate fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which your device assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the domain name server entered statically or by PPP negotiation (DNS), NetBIOS name server (WINS) and default gateway.

21.4.1 IP Pool Configuration

The **Local Services->DHCP Server->IP Pool Configuration** menu displays a list of all the configured IP pools. This list is global and also displays pools configured in other menus.

21.4.1.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

IP Pool Configuration

DHCP Configuration

IP/MAC Binding

DHCP Relay Settings

Basic Parameters

IP Pool Name

IP Address Range

-

DNS Server

Primary

Secondary

OK

Cancel

Fig. 170: Local Services->DHCP Server->IP Pool Configuration->New

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	Primary: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. Secondary: Optionally, enter the IP address of an alternative DNS server.

21.4.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured IP address pools is displayed in the **Local Services->DHCP Server->DHCP Configuration** menu.


In the list, for each entry, you have the possibility under **Status** of enabling or disabling the configured DHCP pools.



Note

In the ex works state the DHCP pool is preconfigured with the IP addresses 192.168.0.10 to 192.168.0.49 and is used if there is no other DHCP server available in the network.

21.4.2.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

IP Pool Configuration

DHCP Configuration

IP/MAC Binding

DHCP Relay Settings

Basic Parameters

Interface

Select one

IP Pool Name

Not yet defined

Pool Usage

Local

Advanced Settings:

Gateway

Use router as gateway

Lease Time

120

Minutes

DHCP Options

Option

Value

Add

OK

Cancel

Fig. 171: Local Services->DHCP Server->DHCP Configuration->New

The **Local Services->DHCP Server->DHCP Configuration->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface over which the addresses defined in IP Address Range are to be assigned to DHCP clients. When a DHCP request is received over this Interface , one of the addresses from the address pool is assigned.
IP Pool Name	Enter any description to uniquely identify the IP pool.

Field	Description
Pool Usage	<p>Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Local</i> (default value): The DHCP pool is only used for DHCP requests in the same subnet.• <i>Relay</i>: The DHCP pool is only used for DHCP requests forwarded from other subnets.• <i>Local/Relay</i>: The DHCP pool is used for DHCP requests in the same subnet and from other subnets.

The menu **Advanced Settings** consists of the following fields:


Fields in the menu **Advanced Settings**

Field	Description
Gateway	<p>Select which IP address is to be transferred to the DHCP client as gateway.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Use router as gateway</i> (default value): Here, the IP address defined for the Interface is transferred.• <i>No gateway</i>: No IP address is sent.• <i>Specify</i>: Enter the corresponding IP address.
Lease Time	<p>Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host.</p> <p>After the Lease Time expires, the address can be reassigned by the server.</p> <p>The default value is <i>120</i>.</p>
DHCP Options	<p>Specify which additional data is forwarded to the DHCP client.</p> <p>Possible values for Option:</p> <ul style="list-style-type: none">• <i>Time Server</i> (default value): Enter the IP address of the time server to be sent to the client.

Field	Description
	<ul style="list-style-type: none">• <i>DNS Server</i>: Enter the IP address of the DNS server to be sent to the client.• <i>DNS Domain Name</i>: Enter the DNS domain to be sent to the client.• <i>WINS/NBNS Server</i>: Enter the IP address of the WINS/NBNS server to be sent to the client.• <i>WINS/NBT Node Type</i>: Select the type of the WINS/NBT node to be sent to the client.• <i>TFTP Server</i>: Enter the IP address of the TFTP server to be sent to the client.• <i>CAPWAP Controller</i>: Enter the IP address of the CAPWAP controller to be sent to the client.• <i>URL (provisioning server)</i>: This option enables you to send a client any URL. Use this option to send querying IP1x0 telephones the URL of the provisioning server if the telephones are to be provisioned automatically. The URL then needs to take the form <i>http://<IP address of the provisioning server>/eg_prov</i>.• <i>Vendor Group</i> (Vendor Specific Information): This enables you to send the client any manufacturer-specific information in any text string. <p>Several entries are possible. Add additional entries with the Add button.</p>

Edit

In the **Local Services->DHCP Server ->DHCP Configuration->Advanced Settings** menu you can edit an entry in the **DHCP Options** field, if **Option** = *Vendor Group* is selected.

Choose the  icon to edit an existing entry. In the popup menu, you configure manufacturer-specific settings in the DHCP server for specific telephones, for example.

Fields in the Basic Parameters menu

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server.

Field	Description
	Possible values: <ul style="list-style-type: none">• <i>Siemens</i> (default value)• <i>Other</i>
Provisioning Server	Only für Select vendor = <i>Siemens</i> Enter which manufacturer value shall be transmitted. For the setting Select vendor = <i>Siemens</i> , the default value <i>sdlp</i> is displayed. You can complete the IP address of the desired server.
Vendor Description	Only für Select vendor = <i>Other</i> Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Custom DHCP Options	Only für Select vendor = <i>Other</i> Use Add to add more entries. You can add custom DHCP options.

21.4.3 IP/MAC Binding

The **Local Services->DHCP Server->IP/MAC Binding** menu displays a list of all clients that received an IP address from your device via DHCP.

You can allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.



Note

You can only create new static IP/MAC bindings if IP address ranges were configured in **Local Services->DHCP Server->DHCP Pool**.

21.4.3.1 New

Choose the **New** button to set up new IP/MAC bindings.

IP Pool Configuration

DHCP Configuration

IP/MAC Binding

DHCP Relay Settings

Basic Parameters

Description

IP Address

MAC Address

OK

Cancel

Fig. 172: Local Services->DHCP Server->IP/MAC Binding->New

The menu **Local Services->DHCP Server->IP/MAC Binding->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the host to which the MAC Address the IP Address is to be bound. A character string of up to 256 characters is possible.
IP Address	Enter the IP address to be assigned to the MAC address specified in MAC Address is to be assigned.
MAC Address	Enter the MAC address to which the IP address specified in IP Address is to be assigned.

21.4.4 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

IP Pool Configuration

DHCP Configuration

IP/MAC Binding

DHCP Relay Settings

Basic Parameters

Primary DHCP Server

0.0.0.0

Secondary DHCP Server

0.0.0.0

OK

Cancel

Fig. 173: Local Services->DHCP Server->DHCP Relay Settings

The menu **Local Services->DHCP Server->DHCP Relay Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded.
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server.

21.5 Web Filter

In the**Local Services->Web Filter** menu, you can configure a URL-based Web Filter service, which during operation accesses the Proventia Web Filter from the company Internet Security Systems (www.iss.net) and checks how a requested Internet page is categorised by the Proventia Web Filter. The action resulting from the classification is configured on your device.

21.5.1 General

This menu contains the configuration of basic parameters for using the Proventia Web Filter.

General

Filter List

Black / White List

History

Web Filter Options

Web Filter Status

☒ Enabled

Filtered Input Interface(s):

Add

Maximum Number of History Entries

64

URL Path Depth

1

Action if server not reachable

☒ Allow all ☐ Block all ☐ Log all

Action if license not registered

☒ Allow all ☐ Block all ☐ Log all

License Information

Licence Key

B1BT

[Activate 30 days demo licence]

Licence Status

License valid until

Not activated

Apply

Fig. 174: Local Services->Web Filter->General

The **Local Services->Web Filter->General** menu consists of the following fields:

Fields in the Web Filter Options menu.

Field	Description
Web Filter Status	Activate or deactivate the filter. The function is activated by selecting <i>Enabled</i> . The function is disabled by default.
Filtered Input Interface(s)	Select for which of the existing Ethernet and WLAN interfaces web filtering is to be activated.

Field	Description
	Press the Add button to add more interfaces. The requests from http Internet pages that reach your device via these interfaces are then monitored by web filtering.
Maximum Number of History Entries	<p>Define the number of entries to be saved in the web filtering history (History menu).</p> <p>Possible values are <i>1</i> to <i>512</i>.</p> <p>The default value is <i>64</i>.</p>
URL Path Depth	Select the path length to which a URL is to be checked by the Cobion Orange Filter.
Action if server not reachable	<p>Select which is to be done with URL requests if the web filtering server cannot be reached.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Allow all</i> (default value): Callup is permitted.• <i>Block all</i>: Callup of the requested page is blocked.• <i>Log all</i>: Callup is permitted, but logged.
Action if license not registered	<p>Select what is to be done with URL requests if the licence key status is <i>Not Valid</i>.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Allow all</i> (default value): Callup is permitted.• <i>Block all</i>: Callup of the requested page is blocked.• <i>Log all</i>: Callup is permitted, but logged.

The menu **License Information** consists of the following fields:

Fields in the License Information menu.

Field	Description
Licence Key	<p>Enter the number of your Proventia Web Filter licence. The pre-set code assigned by ISS designates the device type.</p> <p>In the ex works state, you can activate a 30-day demo version of the Proventia Web Filter. To do this, click the link Activate 30 days demo licence</p>

Field	Description
Licence Status	Shows the result of the last validity check of the licence. The validity of the licence is checked every 23 hours.
License valid until	This shows the expiry date of the licence (relative to the time set on your device) and cannot be edited.

21.5.2 Filter List

In the **Local Services->Web Filter->Filter List** menu, you configure how the various categories of Internet pages are to be handled.

You configure the relevant filters for this purpose. A list of filters already configured is displayed.

There are basically different approaches for configuring the filters:

- First a filter list can be created that only contains entries for those addresses that are to be blocked. In this case it is necessary to make an entry at the end of the filter list that allows all accesses that do not match a filter. (Setting for this: **Category** = *Default behaviour*, **Action** = *Allow* or *Allow and Log*)
- If you only create entries for those addresses that are to be allowed or logged, it is not necessary to change the default behaviour (= all other calls are blocked).

21.5.2.1 New

Choose the **New** button to create additional filters.

GeneralFilter ListBlack / White ListHistory

Filter Parameters

Category	Anonymous Proxies
Day	Everyday
Schedule (Start / Stop Time)	From 00:00 to 23:59
Action	<input type="radio"/> Allow <input type="radio"/> Allow and Log <input checked="" type="radio"/> Block and Log

OKCancel

Fig. 175: Local Services->Web Filter->Filter List->New

The **Local Services->Web Filter->Filter List->New** menu consists of the following fields:

Fields in the Filter Parameters menu.

Field	Description
Category	<p>Select which category of addresses/URLs the filter is to be used on.</p> <p>The options are first the standard categories of the Proventia Web Filter (default value: <i>Anonymous Proxies</i>). Actions can also be defined for the following special cases, e.g.:</p> <ul style="list-style-type: none"> • <i>Default behaviour</i>: This category applies to all Internet addresses. • <i>Other Category</i>: Some addresses are already known to the Proventia Web Filter, but not yet classified. The action associated with this category is used for such addresses. • <i>Unknown URL</i>: If an address is not known to the Proventia Web Filter, the action associated with this category is used.
Day	<p>Select the days on which the filter is to be active.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> • <i>Everyday</i> (default value): The filter is used every day of the week. • <i><Weekday></i>: The filter is used on a certain day of the week. Only one day can be selected per filter; several filters must be configured if several individual days are to be covered. • <i>Monday-Friday</i>: The filter is used from Monday to Friday. <p>The default value is <i>Everyday</i>.</p>
Schedule (Start / Stop Time)	<p>In From, enter the time at which the filter is to be activated. The time is entered in the form hh:mm. Enter the time at which the filter is to be deactivated after the to in the field. The time is entered in the form hh:mm. The default value is 00:00 to 23:59.</p>
Action	<p>Select the action to be executed if the filter matches a call.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Block and Log</i> (default value): The call of the requested page is prevented and logged. • <i>Allow and Log</i>: Callup is permitted, but logged. You can view the logged events in the Local Services->Web Filter->Filter List menu.

Field	Description
	<ul style="list-style-type: none"><i>Allow</i>: Callup is allowed and not logged.

21.5.3 Black / White List

The **Local Services->Web Filter->Black / White List** menu contains a list of URLs or IP addresses, as the case applies. The addresses **on the White List** can also be called if they had been blocked because of filter configuration and classification in the Proventia web filter. The addresses **on the Black List** remain blocked even if they could be called because of filter configuration and classification in the Proventia web filter. In standard configuration neither of the two lists contains entries.

Use the **Add** button to add further URLs or IP addresses to the list.

GeneralFilter ListBlack / White ListHistory

URL / IP Address

BlacklistedWhitelisted

Add

OK

Cancel

Fig. 176: Local Services->Web Filter->Black / White List->Add

The **Local Services->Web Filter->Black / White List->Add** menu consists of the following fields:

Fields in the Black / White List menu.

Field	Description
URL / IP Address	You enter a URL or IP address. The length of the entry is limited to 60 characters.
Blacklisted Whitelisted	<p>You can select whether an URL or IP Address can always (<i>Whitelisted</i>) or never (<i>Blacklisted</i>) be called up.</p> <p><i>Whitelisted</i> is enabled by default.</p> <p>Addresses listed in the White List are allowed automatically. It is not necessary to configure a suitable filter.</p>

21.5.4 History

In the **Local Services->Web Filter->History** menu, you can view the recorded history of the web filter. The history logs all requests that are marked for logging by a relevant filter (**Action** = *Allow and Log*), likewise all rejected requests.

GeneralFilter ListBlack / White ListHistory

View20per page<<>>Filter inNoneequalGo

No.	Date	Time	Source	URL	Category	Result
Page: 1						

Fig. 177: Local Services->Web Filter->History

21.6 Scheduling

Your device has a event scheduler, which enables certain standard actions (for example, activating and deactivating interfaces) to be carried out. Moreover, every existing MIB variable can be configured with any value.

You specify the **Actions** you want and define the **Trigger** that control when and under which conditions the **Actions** are to be carried out. A **Trigger** may be a single event or a sequence of events which are combined into an **Event List**. You also create an event list for a single event, but it only contains one event.

Actions can be initiated on a time-controlled basis. Moreover, the status or accessibility of interfaces or their data traffic may lead to execution of the configured actions, or also the validity of licences. Here also, it is possible to set up every MIB variable as initiator with any value.

To take the event scheduler live, enable the **Schedule Interval** under **Options**. This interval species the time gap in which the system checks whether at least one event has occurred. This event is used as the initiator for a configured action.



Caution

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of bintec elmeg gateways. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.



Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

21.6.1 Trigger

The **Local Services->Scheduling->Trigger** menu displays all the event lists that have been configured. Every event list contains at least one event which is intended to be the initiator for an action.

21.6.1.1 New

Choose the **New** button to create more event lists.

TriggerActionsOptions

Basic Parameters

Event List

New

Description

Event Type

Time

Select time interval

Time Condition

Condition Type

Weekday

Periods

Day of Month

Condition Settings

Monday

Daily

1

Start Time

Hour

Minute

Stop Time

Hour

Minute

OK

Cancel

Fig. 178: Local Services->Scheduling->Trigger->New

The menu **Local Services->Scheduling->Trigger->New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Event List	You can create a new event list with <i>New</i> (default value). You give this list a name with Description . You use the remaining parameters to create the first event in the list.

430

bintec RV Series

Field	Description
	<p>If you want to add to an existing event list, select the event list you want and add at least one more event to it.</p> <p>You can use event lists to create complex conditions for initiating an action. The events are processed in the same order in which they are created in the list.</p>
Description	<p>Only for Event List = <i>New</i></p> <p>Enter your chosen designation for the event list.</p>
Event Type	<p>Select the type of event.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Time</i> (default value): The operations configured and assigned in Actions are initiated at specific points in time.• <i>MIB/SNMP</i>: The actions configured and assigned in Actions are initiated when the defined MIB variables assumes the assigned values.• <i>Interface Status</i>: Operations configured and assigned in Actions are initiated, when the defined interfaces take on a specified status.• <i>Interface Traffic</i>: The operations configured and assigned in Actions are triggered if the data traffic on the specified interfaces falls below or exceed the defined value.• <i>Ping Test</i>: the operations configured and assigned in Actions are triggered if the defined IP address is accessible or not accessible.• <i>Certificate Lifetime</i>: Operations configured and assigned in Actions are initiated when the defined period of validity is reached.• <i>GEO Zone Status</i> : Operations configured and assigned in Actions are initiated, when the defined GEO Zones take on a specified status.
Monitored GEO Zone	<p>Only for Event Type <i>GEO Zone Status</i></p> <p>Select a GEO zone configured in the Physical Interfaces menu.</p>
GEO Zone Status	<p>Only for Event Type <i>GEO Zone Status</i></p>

Field	Description
	<p>Select the GEO Zone Status.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>True</i>: The current position lies within the defined zone.• <i>False</i>: The current position lies outside the defined zone.
Monitored Variable	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Select the MIB variable whose defined value is to be configured as initiator. First, select the System in which the MIB variable is saved, then the MIB Table and finally the MIB Variable itself. Only the MIB tables and MIB variables present in the respective area are displayed.</p>
Compare Condition	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Select whether the MIB variable <i>Greater</i> (default value), <i>Equal</i>, <i>Less</i>, <i>Not Equal</i>, must have the value given in <i>Compare Value</i> or must lie within <i>Range</i> to initiate the operation.</p>
Compare Value	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Enter the value of the MIB variable.</p>
Index Variables	<p>Only for Event Type <i>MIB/SNMP</i></p> <p>Where required, select MIB variables to uniquely identify a specific data set in the MIB Table, e.g. <i>ConnIfIndex</i>. The unique identification of a particular table entry is derived from the combination of Index Variable (usually an index variable which is flagged with *) and Index Value.</p> <p>Use Index Variables to create more entries with Add.</p>
Monitored Interface	<p>Only for Event Type <i>Interface Status</i> and <i>Interface Traffic</i></p> <p>Select the interface whose defined status shall trigger an operation.</p>
Interface Status	<p>Only for Event Type <i>Interface Status</i></p> <p>Select the status that the interface must have in order to initiate</p>

Field	Description
	<p>the intended operation.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Up</i> (default value): The function is enabled.• <i>Down</i>: The interface is disabled.
Traffic Direction	<p>Only for Event Type <i>Interface Traffic</i></p> <p>Select the direction of the data traffic whose values should be monitored as initiating an operation.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>RX</i> (default value): Incoming data traffic is monitored.• <i>TX</i>: Outgoing data traffic is monitored.
Interface Traffic Condition	<p>Only for Event Type <i>Interface Traffic</i></p> <p>Select whether the value for data traffic must be <i>Greater</i> (default value) or <i>Less</i> the value specified in <i>Transferred Traffic</i> in order to initiate the operation.</p>
Transferred Traffic	<p>Only for Event Type <i>Interface Traffic</i></p> <p>Enter the desired value in kBytes for the data traffic to serve as comparison.</p> <p>The default value is <i>0</i>.</p>
Destination IP Address	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter the IP address whose accessibility is to be checked.</p>
Source IP Address	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter an IP address to be used as sender address for the ping test.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Automatic</i> (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address.• <i>Specific</i>: Enter the desired IP address in the input field.

Field	Description
Status	<p>Only for Event Type <i>Ping Test</i></p> <p>Select whether Destination IP Address <i>Reacheable</i> must be (default value) or <i>Unreacheable</i> in order to initiate the operation.</p>
Interval	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter the time in Seconds after which a ping must be resent.</p> <p>The default value is <i>60</i> seconds.</p>
Trials	<p>Only for Event Type <i>Ping Test</i></p> <p>Enter the number of ping tests to be performed until Destination IP Address as <i>Unreacheable</i> applies.</p> <p>The default value is <i>3</i>.</p>
Monitored Certificate	<p>Only for Event Type <i>Certificate Lifetime</i></p> <p>Select the certificate whose validity should be checked.</p>
Remaining Validity	<p>Only for Event Type <i>Certificate Lifetime</i></p> <p>Enter the desired value for the remaining validity of the certificate in percentage.</p>

Fields in the menu **Select time interval**

Field	Description
Time Condition	<p>For Event Type <i>Time</i> only</p> <p>First select the type of time entry in Condition Type.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Weekday</i>: Select a weekday in Condition Settings.• <i>Periods</i> (default value): In Condition Settings, select a particular period.• <i>Day of Month</i>: Select a specific day of the month in Condition Settings. <p>Possible values for Condition Settings in Condition Type =</p>

Field	Description
	<p><i>Weekday:</i></p> <p><i>Monday (default value) ... Sunday.</i></p> <p>Possible values for Condition Settings in Condition Type = Periods:</p> <ul style="list-style-type: none">• <i>Daily:</i> The initiator becomes active daily (default value).• <i>Monday-Friday:</i> The initiator becomes active daily from Monday to Friday.• <i>Monday - Saturday:</i> The initiator becomes active daily from Monday to Saturday.• <i>Saturday - Sunday:</i> The initiator becomes active on Saturdays and Sundays. <p>Possible values for Condition Settings in Condition Type = Day of Month:</p> <p><i>1... 31.</i></p>
Start Time	Enter the time from which the initiator is to be activated. Activation is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Enter the time from which the initiator is to be deactivated. Deactivation is carried on the next scheduling interval. If you do not enter a Stop Time or set a Stop Time = Start Time , the initiator is activated, and deactivated after 10 seconds.

21.6.2 Actions

In the **Local Services->Scheduling->Actions** menu is displayed a list of all operations to be initiated by events or event chains configured in **Local Services->Scheduling->Trigger**.

21.6.2.1 New

Choose the **New** button to configure additional operations.

Trigger

Actions

Options

Basic Parameters

Description

Command Type

Reboot

Event List

Select one

Event List Condition

All

Reboot device after

60

Seconds

OK

Cancel

Fig. 179: Local Services->Scheduling->Actions->New

The menu **Local Services->Scheduling->Actions->New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter your chosen designation for the action.
Command Type	<div>Select the desired action.</div> <div>Possible values:</div> <ul style="list-style-type: none">• <i>Reboot</i> (default value): Your device is rebooted.• <i>MIB/SNMP</i>: The desired value is entered for a MIB variable.• <i>Interface Status</i>: The status of an interface is modified.• <i>Wlan Status</i>: Only for devices with a wireless LAN. The status of a WLAN-SSID is modified.• <i>Software Update</i>: A software update is initiated.• <i>Configuration Management</i>: A configuration file is loaded onto your device or backed up by your device.• <i>Ping Test</i>: Accessibility of an IP address is checked.• <i>Certificate Management</i>: A certificate is to be renewed, deleted or entered.• <i>5 GHz WLAN Bandscan</i>: Only for devices with a wireless LAN. A scan of the 5 GHz frequency band is performed.• <i>5.8 GHz WLAN Bandscan</i>: Only for devices with a wireless LAN. A scan of the 5.8 GHz frequency range is performed.• <i>WLC: New Neighbor Scan</i>: Only for devices with a WLAN controller. A Neighbor Scan is initiated by the WLAN network

Field	Description
	<p>controlled by the WLAN controller.</p> <ul style="list-style-type: none">• <i>WLC: VSS State</i>: Only for devices with a WLAN controller. The status of a wireless network is modified.• <i>WLAN: Operation Mode</i>: The operating mode of a WLAN radio module is modified.
Event List	Select the event list you want which has been created in Local Services->Scheduling->Trigger .
Event List Condition	<p>For the selected chains of events, select how many of the configured events must occur for the operation to be initiated.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>All</i> (default value): The operation is initiated if all events occur.• <i>One</i>: The operation is initiated if a single event occurs.• <i>None</i>: The operation is triggered if no event occurs.• <i>One not</i>: The operation is triggered if one of the events does not occur.
Reboot device after	<p>Only if Command Type = <i>Reboot</i></p> <p>Enter the timespan in seconds that must elapse after occurrence of the event until the device is restarted.</p> <p>The default value is <i>60</i> seconds.</p>
MIB/SNMP Variable to add/edit	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select the MIB table in which the MIB variable whose value shall be changed is saved. First, select the System, then the MIB Table. Only the MIB tables present in the respective area are displayed.</p>
Command Mode	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select how the MIB entry is to be manipulated.</p> <p>Possible settings:</p> <ul style="list-style-type: none">• <i>Change existing entry</i> (default value): An existing entry shall be modified.

Field	Description
	<ul style="list-style-type: none">• <i>Create new MIB entry</i>: A new entry shall be created.
Index Variables	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Where required, select MIB variables to uniquely identify a specific data set in MIB Table, e.g. <i>ConnIfIndex</i>. The unique identification of a particular table entry is derived from the combination of Index Variable (usually an index variable which is flagged with *) and Index Value.</p> <p>Use Index Variables to create more entries with Add.</p>
Trigger Status	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select what status the event must have in order to modify the MIB variable as defined.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Active</i> (default value): The value of the MIB variable is modified if the initiator is active.• <i>Inactive</i>: The value of the MIB variable is modified if the initiator is inactive.• <i>Both</i>: The value of the MIB variable is differentially modified if the initiator status changes.
MIB Variables	<p>Only if Command Type = <i>MIB/SNMP</i></p> <p>Select the MIB variable whose value is to be configured as dependent upon initiator status.</p> <p>If the initiator is active (Trigger Status <i>Active</i>), the MIB variable is described with the value entered in Active Value.</p> <p>If the initiator is inactive (Trigger Status <i>Inactive</i>), the MIB variable is described with the value entered in Inactive Value.</p> <p>If the MIB variable is to be modified, depending on whether the initiator is active or inactive (Trigger Status <i>Both</i>), it is described with an active initiator with the value entered in Active Value and with an inactive initiator with the value in Inactive Value.</p> <p>Use Add to create more entries.</p>

Field	Description
Interface	<p>Only if Command Type = <i>Interface Status</i></p> <p>Select the interface whose status should be changed.</p>
Set interface status	<p>Only if Command Type = <i>Interface Status</i></p> <p>Select the status to be set for the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Up</i> (default value)• <i>Down</i>• <i>Reset</i>
Local WLAN SSID	<p>Only if Command Type = <i>Wlan Status</i></p> <p>Select the desired wireless network whose status shall be changed.</p>
Set status	<p>Only if Command Type = <i>Wlan Status</i> or <i>WLC: VSS State</i></p> <p>Select the status for the wireless network.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Activate</i> (default value)• <i>Deactivate</i>
Source Location	<p>Only if Command Type = <i>Software Update</i></p> <p>Select the source for the software update.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Current Software from Update Server</i> (default value): The latest software will be downloaded from the update server.• <i>HTTP Server</i>: The latest software will be downloaded from an HTTP server that you define in <i>Server URL</i>.• <i>HTTPS Server</i>: The latest software will be downloaded from an HTTPS server that you define in <i>Server URL</i>.• <i>TFTP Server</i>: The latest software will be downloaded from an TFTP server that you define in <i>Server URL</i>.

Field	Description
Server URL	<p>Where Command Type = <i>Software Update</i> if Source Location not <i>Current Software from Update Server</i></p> <p>Enter the URL of the server from which the desired software version is to be retrieved.</p> <p>Where Command Type = <i>Configuration Management</i> with Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Enter the URL of the server from which a configuration file is to be retrieved, or on which the configuration file is to be backed up.</p>
File Name	<p>For Command Type = <i>Software Update</i></p> <p>Enter the file name of the software version.</p> <p>Where Command Type = <i>Certificate Management</i> with Action = <i>Import certificate</i></p> <p>Enter the file name of the certificate file.</p>
Action	<p>For Command Type = <i>Configuration Management</i></p> <p>Select which operation is to be performed on a configuration file.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Import configuration</i> (default value)• <i>Export configuration</i>• <i>Rename configuration</i>• <i>Delete configuration</i>• <i>Copy configuration</i> <p>For Command Type = <i>Certificate Management</i></p> <p>Select which operation you wish to perform on a certificate file.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Import certificate</i> (default value)• <i>Delete certificate</i>

Field	Description
	<ul style="list-style-type: none">• <i>SCEP</i>
Protocol	<p>Only for Command Type = <i>Certificate Management</i> and <i>Configuration Management</i> if Action = <i>Import configuration</i></p> <p>Select the protocol for the data transfer.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>HTTP</i> (default value)• <i>HTTPS</i>• <i>TFTP</i>
CSV File Format	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Select whether the file is to be sent in the CSV format.</p> <p>The CSV format can easily be read and modified. In addition, you can view the corresponding file clearly using Microsoft Excel for example.</p> <p>The function is enabled by default.</p>
Remote File Name	<p>Only if Command Type = <i>Configuration Management</i></p> <p>For Action = <i>Import configuration</i></p> <p>Enter the name of the file under which it is saved on the server from which it is to be retrieved.</p> <p>For Action = <i>Export configuration</i></p> <p>Enter the file name under which it should be saved on the server.</p>
Local File Name	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i>, <i>Rename configuration</i> or <i>Copy configuration</i></p> <p>At import, renaming or copying enter a name for the configuration file under which to save it locally on the device.</p>

Field	Description
File Name in Flash	<p>Where Command Type = <i>Configuration Management</i> and Action = <i>Export configuration</i></p> <p>Select the file to be exported.</p> <p>Where Command Type = <i>Configuration Management</i> and Action = <i>Rename configuration</i></p> <p>Select the file to be renamed.</p> <p>Where Command Type = <i>Configuration Management</i> and Action = <i>Delete configuration</i></p> <p>Select the file to be deleted.</p> <p>Where Command Type = <i>Configuration Management</i> and Action = <i>Copy configuration</i></p> <p>Select the file to be copied.</p>
Configuration contains certificates/keys	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Select whether the certificates and keys contained in the configuration are to be imported or exported.</p> <p>The function is disabled by default.</p>
Encrypt configuration	<p>Only where Command Type = <i>Configuration Management</i> and Action = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Define whether the data of the selected Action are to be encrypted..</p> <p>The function is disabled by default.</p>
Reboot after execution	<p>Only if Command Type = <i>Configuration Management</i></p> <p>Select whether your device should restart after the intended Action.</p> <p>The function is disabled by default.</p>
Version Check	<p>Only where Command Type = <i>Configuration</i></p>

Field	Description
	<p>and Action = <i>Import configuration</i></p> <p>Select whether, when importing a configuration file, to check on the server for the presence of a more current version of the already loaded configuration. If not, the file import is interrupted.</p> <p>The function is disabled by default.</p>
Destination IP Address	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter the IP address whose accessibility is to be checked.</p>
Source IP Address	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter an IP address to be used as sender address for the ping test.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Automatic</i> (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address.• <i>Specific</i>: Enter the desired IP address in the input field.
Interval	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter the time in Seconds after which a ping must be resent.</p> <p>The default value is <i>1</i> second.</p>
Count	<p>Only if Command Type = <i>Ping Test</i></p> <p>Enter the number of ping tests to be performed until Destination IP Address is considered unreachable.</p> <p>The default value is <i>3</i>.</p>
Server Address	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Enter the URL of the server from which a certificate file is to be retrieved.</p>
Local Certificate Description	<p>Where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p>

Field	Description
	<p>Enter a description for the certificate under which to save it on the device.</p> <p>Where Command Type = <i>Certificate Management</i> and Action = <i>Delete certificate</i></p> <p>Select the certificate to be deleted.</p>
Password for protected Certificate	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Select whether to use a secure certificate requiring a password and enter it into the entry field.</p> <p>The function is disabled by default.</p>
Overwrite similar certificate	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Select whether to overwrite a certificate already present on the your device with the new one.</p> <p>The function is disabled by default.</p>
Write certificate in configuration	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>Import certificate</i></p> <p>Select whether to integrate the certificate in a configuration file; and if so, select the desired configuration file.</p> <p>The function is disabled by default.</p>
Certificate Request Description	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter a description under which the SCEP certificate on your device is to be saved.</p>
URL SCEP Server URL	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter the URL of the SCEP server, e.g. <i>http://scep.bintec-elmeg.com:8080/scep/scep.dll</i></p> <p>Your CA administrator can provide you with the necessary data.</p>

Field	Description
Subject Name	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter a subject name with attributes.</p> <p>Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE"</p>
CA Name	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. <i>cawindows</i>. Your CA administrator can provide you with the necessary data.</p>
Password	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>To obtain certificates, you may need a password from the certification authority. Enter the password you received from the certification authority here.</p>
Key Size	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Select the length of the key to be created. Possible values are <i>1024</i> (default value), <i>2048</i> and <i>4096</i>.</p>
Autosave Mode	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p> <p>Select whether your device automatically stores the various steps of the enrolment internally. This is an advantage if enrolment cannot be concluded immediately. If the status has not been saved, the incomplete registration cannot be completed. As soon as the enrolment is completed and the certificate has been downloaded from the CA server, it is automatically saved in the device configuration.</p> <p>The function is enabled by default.</p>
Use CRL	<p>Only where Command Type = <i>Certificate Management</i> and Action = <i>SCEP</i></p>

Field	Description
	<p>Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Auto</i> (default value): In case there is an entry for a CDP, CRL distribution point this should be evaluated in addition to the CRLs globally configured in the device.• <i>Yes</i>: CRLs are always checked.• <i>No</i>: No checking of CRLs.
Select radio	<p>Only where Command Type = <i>5 GHz WLAN Bandscan, 5.8 GHz WLAN Bandscan</i> or <i>WLAN: Operation Mode</i></p> <p>Select the WLAN module on which to perform the frequency band scan.</p>
WLC SSID	<p>Only where Command Type = <i>WLC: VSS State</i></p> <p>Select the wireless network administered over the WLAN controller whose status should be changed.</p>
Operation Mode (Active)	<p>Only where Command Type = <i>WLAN: Operation Mode</i></p> <p>Select the required operating mode for the selected radio module if it currently has the status <i>Active</i>. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.</p>
Operation Mode (Inactive)	<p>Only where Command Type = <i>WLAN: Operation Mode</i></p> <p>Select the required operating mode for the selected radio module if it currently has the status <i>Down</i>. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.</p>

21.6.3 Options

You configure the schedule interval in the **Local Services->Scheduling->Options**.

Trigger

Actions

Options

Scheduling Options

Schedule Interval

0

sec

☒ Enabled

OK

Cancel

Fig. 180: Local Services->Scheduling->Options

The **Local Services->Scheduling->Options** menu consists of the following fields:

Fields in the Scheduling Options menu.

Field	Description
Schedule Interval	<p>Select whether the schedule interval is to be enabled for the interface.</p> <p>Enter the period of time in seconds after which the system checks whether configured events have occurred.</p> <p>Possible values are 0 to 65535.</p> <p>The value 300 is recommended (5 minute accuracy).</p>

21.7 Surveillance

In this menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

You can monitor temperature with devices from the **bintec WI** series.




Note

This function cannot be configured on your device for connections that are authenticated via a RADIUS server.

21.7.1 Hosts

A list of all monitored hosts is displayed in the **Local Services->Surveillance->Hosts** menu.

21.7.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional monitoring tasks.

Hosts

Interfaces

Ping Generator

Host Parameters

Group ID

New ID

Trigger

Monitored IP Address

Default Gateway

Source IP Address

Automatic

Interval

10

Seconds

Successful Trials

3

Unsuccessful Trials

3

Action to be performed

Action

Interface

Disable

Select one

Add

OK

Cancel

Fig. 181: Local Services->Surveillance->Hosts->New

The menu **Local Services->Surveillance->Hosts->New** consists of the following fields:

Fields in the Host Parameters menu

Field	Description
Group ID	<p>If the availability of a group of hosts or the default gateway is to be monitored by your device, select an ID for the group or the default gateway.</p> <p>The group IDs are automatically created from 0 to 255. If an entry has not yet been created, a new group is created using the <i>New ID</i> option. If entries have been created, you can select one from the list of created groups.</p> <p>Each host to be monitored must be assigned to a group.</p> <p>The operation configured in Interface is only executed if no group member can be reached.</p>

Fields in the Trigger menu.


Field	Description
Monitored IP Address	<p>Enter the IP address of the host to be monitored.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Default Gateway</i> (default value): The default gateway is monitored.• <i>Specific</i>: Enter the IP address of the host to be monitored manually in the adjacent input field.
Source IP Address	<p>Select how the IP address is to be determined that your device uses as the source address of the packet sent to the host to be monitored.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Automatic</i> (default value): The IP address is determined automatically.• <i>Specific</i>; Enter the IP address in the adjacent input field.
Interval	<p>Enter the time interval (in seconds) to be used for checking the availability of hosts.</p> <p>Possible values are 1 to 65536.</p> <p>The default value is 10.</p> <p>Within a group, the smallest Interval of the group members is used.</p>
Successful Trials	<p>Specify how many pings need to be answered for the host to be regarded as accessible.</p> <p>You can use this setting to specify, for example, when a host is deemed to be accessible once more, and used again, instead of a backup device.</p> <p>Possible values are 1 to 65536.</p> <p>The default value is 3.</p>
Unsuccessful Trials	<p>Specify how many pings need to be unanswered for the host to be regarded as inaccessible.</p> <p>You can use this setting to specify, for example, when a host is deemed to be inaccessible, and that a backup device should be</p>

Field	Description
	<p>used.</p> <p>Possible values are <i>1</i> to <i>65536</i>.</p> <p>The default value is <i>3</i>.</p>
Action to be performed	<p>Select which Action should be run. For most actions, you select an Interface to which the Action relates.</p> <p>All physical and virtual interfaces can be selected.</p> <p>For each interface, select whether it is to be enabled (<i>Enable</i>), disabled (<i>Disable</i> default value), reset (<i>Reset</i>), or the connection reestablished (<i>Redial</i>).</p> <p>With Action = <i>Monitor</i> you can monitor the IP address that is specified under Monitored IP Address. This information can be used for other functions, such as the Tracking IP Address.</p>

21.7.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services->Surveillance->Interfaces** menu.

21.7.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to set up monitoring for other interfaces.

Hosts

Interfaces

Ping Generator

Basic Parameters

Monitored Interface

Select one

Trigger

Interface goes up

Interface Action

Enable

Interface

Select one

OK

Cancel

Fig. 182: **Local Services->Surveillance->Interfaces->New**

The menu **Local Services->Surveillance->Interfaces->New** consists of the following fields:


Fields in the Basic Parameters menu.

Field	Description
Monitored Interface	Select the interface on your device that is to be monitored.
Trigger	<p>Select the state or state transition of Monitored Interface that is to trigger a particular Interface Action.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Interface goes up</i> (default value)• <i>Interface goes down</i>
Interface Action	<p>Select the action that is to follow the state or state transition defined in Trigger.</p> <p>The action is applied to the Interface(s) selected in Interface.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Enable</i> (default value): Activation of interface(s)• <i>Disable</i>: Deactivation of interface(s)
Interface	<p>Select the interface(s) for which the action defined in Interface is to be performed.</p> <p>You can choose all physical and virtual interfaces as well as options <i>All PPP Interfaces</i> and <i>All IPSec Interfaces</i>.</p>

21.7.3 Ping Generator

In the **Local Services->Surveillance->Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

21.7.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional pings.

Hosts

Interfaces

Ping Generator

Basic Parameters

Destination IP Address

Source IP Address

Specific

Interval

10

Seconds

Trials

3

OK

Cancel

Fig. 183: Local Services->Surveillance->Ping Generator->New

The menu **Local Services->Surveillance->Ping Generator->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.
Source IP Address	<div>Enter the source IP address of the outgoing ICMP echo request packets.</div> <div>Possible values:</div> <div><ul style="list-style-type: none">• <i>Automatic</i>: The IP address is determined automatically.• <i>Specific</i> (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.</div>
Interval	<div>Enter the interval in seconds during which the ping is sent to the address specified in Remote IP Address.</div> <div>Possible values are 1 to 65536.</div> <div>The default value is 10.</div>
Trials	<div>Enter the number of ping tests to be performed until Destination IP Address as <i>Unreachable</i> applies.</div> <div>The default value is 3.</div>

21.8 UPnP

Universal Plug and Play (UPnP) makes it possible to use current messenger services (e.g. real time video/audio conferencing) as peer-to-peer communication where one of the peers lies behind a NAT-enabled gateway.

UPnP enables (mostly) Windows-based operating systems to take control of other devices with UPnP functionality on the local network. These include gateways, access points and print servers. No special device drivers are needed as known common protocols are used, such as TCP/IP, HTTP and XML.

Your gateway makes it possible to use the subsystem of the Internet Gateway Device (IGD) from the UPnP function range.

In a network behind a NAT-enabled gateway, the UPnP-configured computers act as LAN UPnP clients. To do this, the UPnP function on the PC must be enabled.

The pre-configured port used for UPnP communication between LAN UPnP clients and the gateway is `5678`. The LAN UPnP client acts as a so-called service control point, i.e. it recognizes and controls the UPnP devices on the network.

The ports assigned dynamically by, for example, MSN Messenger, lie in the range from `5004` to `65535`. The ports are released internally to the gateway on demand, i.e. when an audio/video transfer is started in Messenger. When the application is closed, the ports are immediately closed again.

The peer-to-peer-communication is initiated via public SIP servers with only the information from the two clients being forwarded. The clients then communicate directly with one another.

For further information about UPnP, see www.upnp.org.

21.8.1 Interfaces

In this menu, you configure the UPnP settings individually for each interface of your gateway.

You can determine whether UPnP requests from clients are accepted by each interface (for requests from the local network) and/or whether the interface can be controlled via UPnP requests.

Interfaces

General

View 20 per page << >> Filter in None equal Go

Interface	Answer to client request	Interface is UPnP controlled
en1-0	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
en1-4	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

Page: 1, Items: 1 - 2

OK

Cancel

Fig. 184: Local Services->UPnP->Interfaces

The menu **Local Services->UPnP->Interfaces** consists of the following fields:

Fields in the Interfaces menu.

Field	Description
Interface	Shows the name of the interface for which the UPnP settings are to be made. The entry cannot be changed.
Answer to client request	Determine whether UPnP requests from clients are to be answered via the particular interface (from the local network). The function is enabled with <i>Enabled</i> . The function is disabled by default.
Interface is UPnP controlled	Determine whether the NAT configuration of this interface is controlled by UPnP. The function is enabled with <i>Enabled</i> . The function is disabled by default.

21.8.2 General

In this menu, you make the basic UPnP settings.

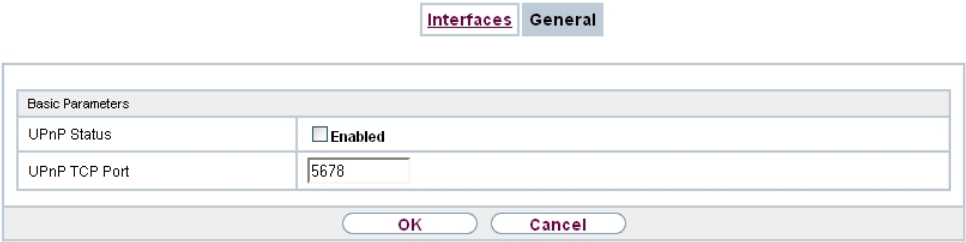


Fig. 185: Local Services->UPnP->General

The **Local Services->UPnP->General** menu consists of the following fields:

Fields in the General menu.

Field	Description
UPnP Status	<p>Decide how the gateway processes UPnP requests from the LAN.</p> <p>The function is enabled with <i>Enabled</i>. The gateway proceeds with UPnP releases in accordance with the parameters contained in the request from the LAN UPnP client, independently of the IP address of the requesting LAN UPnP client.</p> <p>The function is disabled by default. The gateway rejects UPnP requests, NAT releases are not made.</p>
UPnP TCP Port	<p>Enter the number of the port on which the gateway listens for UPnP requests.</p> <p>The possible values are <i>1</i> to <i>65535</i>, the default value is <i>5678</i>.</p>

21.9 HotSpot Gateway

The **HotSpot Solution** allows provision of public Internet accesses (using WLAN or wired Ethernet). The solution is adapted to setup of smaller and larger Hotspot solutions for cafes, hotels, companies, communal residences, campgrounds, etc.

The **HotSpot Solution** consists of a bintec elmeg gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hot-spot server, centrally located at a computing centre. The operator account is administered on the server via an administration terminal (e.g., a hotel reception PC); this includes functions such as registration entry, generating tickets, statistical analysis, etc.

Login sequence at the Hotspot server

- When a new user connects with the Hotspot, he/she is automatically assigned an IP address via DHCP.
- As soon as he attempts to access any Internet site with a browser, the user is redirected to the home/login page.
- After the user has entered the registration data (user/password), these are sent to the central RADIUS server (Hotspot server) as RADIUS registration.
- Following successful registration, the gateway opens Internet access.
- For each user, the gateway sends regular additional information to the RADIUS server for recording accounting data.
- When the ticket expires, the user is automatically logged off and again redirected to the home/login page.

Requirements

To operate a Hotspot, the customer requires:

- a bintec elmeg device as hotspot gateway with active Internet access and configured hotspot server entries for login and accounting (see menu **System Management->Remote Authentication->RADIUS->New** with **Group Description** *default group 0*)
- bintec elmeg Hotspot hosting (article number 5510000198)
- Access data
- Documentation
- Software licensing

Please note that you must first activate the licence.

Go to www.bintec-elmeg.com then **Service/Support -> Services -> Online Services**.

- Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

- You then receive the Hotspot server's login data.



Note

Activation may require 2-3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Set by bintec elmeg GmbH
Domain	Individually set for customers by customer/dealer
Walled Garden Network	Individually set for customers by customer/dealer
Walled Garden Server URL	Individually set for customers by customer/dealer
Terms & Conditions URL	Individually set for customers by customer/dealer

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Individually set by bintec elmeg
Password	Individually set by bintec elmeg



Note

Also refer to the WLAN Hotspot Workshop that is available to download from www.bintec-elmeg.com

21.9.1 HotSpot Gateway

In the **HotSpot Gateway** menu, you can configure the bintec elmeg gateway installed onsite for the **Hotspot Solution**.

A list of all configured hotspot networks is displayed in the **Local Services->HotSpot Gateway->HotSpot Gateway** menu.

HotSpot GatewayOptions


Interface	Domain	Status		
LAN_EN1-0	hotspot.domain.de	<input checked="" type="checkbox"/> Enabled		

NewOKCancel

Fig. 186: Local Services->HotSpot Gateway->HotSpot Gateway

You can use the **Enabled** option to enable or disable the corresponding entry.

21.9.1.1 Edit or New

You configure the hotspot networks in the **Local Services->HotSpot Gateway->HotSpot Gateway->** menu. Choose the **New** button to set up additional Hotspot networks.

HotSpot Gateway

Options

Basic Parameters

Interface

LAN_EN1-0

Domain at the HotSpot Server

Walled Garden

☐ Enabled

Post Login URL

Language for login window

English

Advanced Settings

Ticket Type

Username/Password

Allowed HotSpot Client

All

Login Frameset

☒ Active

Pop-Up window for status indication

☒ Active

Default Idle Timeout

☒ Enabled

600

Seconds

OK


Cancel

Fig. 187: Local Services->HotSpot Gateway->HotSpot Gateway->

The **Local Services->HotSpot Gateway->HotSpot Gateway->** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Choose the interface to which the Hotspot LAN or WLAN is connected. When operating over LAN, enter the Ethernet interface here (e. g. en1-0). If operating over WLAN, the WLAN interface to which the access point is connected must be selected.

Field	Description
	<p>Caution</p> <p>For security reasons you cannot configure your device over an interface that is configured for the Hotspot. Therefore take care when selecting the interface you want to use for the Hotspot.</p> <p>If you select the interface over which the current configuration session is running, the current connection will be lost. You must then log in again over a reachable interface that is not configured for the Hotspot to configure your device.</p>
Domain at the HotSpot Server	Enter the domain name that you used when setting up the HotSpot server for this customer. The domain name is required so that the Hotspot server can distinguish between the different clients (customers).
Walled Garden	<p>Enable this function if you want to define a limited and free area of websites (intranet).</p> <p>The function is not activated by default.</p>
Walled Network / Netmask	<p>Only if Walled Garden is enabled.</p> <p>Enter the network address of the Walled Network and the corresponding Netmask of the intranet server.</p> <p>For the address range resulting from Walled Network / Netmask, clients require no authentication.</p> <p>Example: Enter 192.168.0.0 / 255.255.255.0, if all IP addresses from 192.168.0.0 to 19.168.0.255 are free. Enter 192.168.0.1 / 255.255.255.255, if only the IP address 192.168.0.1 is free.</p>
Walled Garden URL	<p>Only if Walled Garden is enabled.</p> <p>Enter the Walled Garden URL of the intranet server. Freely accessible websites must be reachable over this address.</p>
Terms &Conditions	<p>Only if Walled Garden is enabled.</p> <p>In the Terms &Conditions input field, enter the address of the general terms and conditions on the intranet server, or public server, e.g., http://www.webserver.de/agb.htm. The page must</p>

Field	Description
	lie within the address range of the walled garden network.
Additional freely accessible Domain Names	<p>Only if Walled Garden is enabled.</p> <p>Add further URLs or IP addresses with Add. The web pages can be accessed via these additional freely accessible addresses.</p>
Post Login URL	Here you can specify the URL a user is redirected to after logging in to the Hotspot Solution.
Language for login window	<p>Here you can choose the language for the start/login page.</p> <p>The following languages are supported: <i>English, Deutsch, Italiano, Français, Español, Português</i> and <i>Netherlands</i>.</p> <p>The language can be changed on the start/login page at any time.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu **Advanced Settings**

Field	Description
Ticket Type	<p>Select the ticket type.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Voucher</i>: Only the user name must be entered. Define a default password in the input field.• <i>Username/Password</i> (default value): User name and password must be entered.
Allowed HotSpot Client	<p>Here you can define which type of users can log in to the Hotspot.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>All</i>: All clients are approved.• <i>DHCP Client</i>: Prevents users who have not received an IP address from DHCP from logging in.
Login Frameset	Enable or disable the login window.

Field	Description
	<p>The login window on the HTML homepage consists of two frames.</p> <p>When the function is enabled, the login form displays on the left-hand side.</p> <p>When the function is disabled, only the website with information, advertising and/or links to freely accessible websites is displayed.</p> <p>The function is enabled by default.</p>
Pop-Up window for status indication	<p>Specify whether the device uses pop-up windows to display the status.</p> <p>The function is enabled by default.</p>
Default Idle Timeout	<p>Enable or disable the Default Idle Timeout. If a hotspot user does not trigger any data traffic for a configurable length of time, they are logged out of the hotspot.</p> <p>The function is enabled by default.</p> <p>The default value is 600 seconds.</p>

21.9.2 Options

In the **Local Services->HotSpot Gateway->Options** menu, general settings are performed for the hotspot.

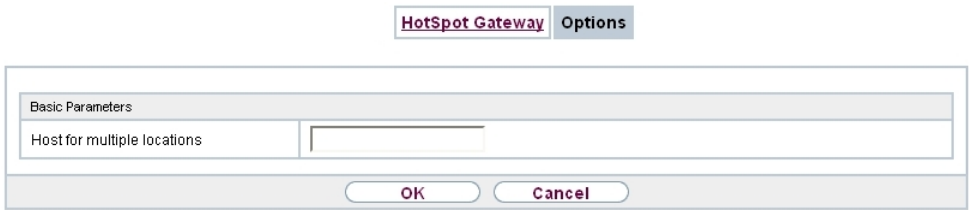


Fig. 188: Local Services->HotSpot Gateway->Options

The **Local Services->HotSpot Gateway->Options** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host for multiple locations	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.


21.10 Wake-On-LAN

With the function **Wake-On-LAN (WOL)** you can start network devices that are switched off via an integrated network card. The network card also needs a power supply, even when the computer is switched off. You can use filters and rule chains to define the conditions that need to be met to send the so-called magic packet, and select the interfaces that are to be monitored for the defined rule chains. Configuring the filters and rule chains is largely like configuring filters and rule chains in the menu **Access Rules**.

21.10.1 Wake-On-LAN Filter

The menu **Local Services->Wake-On-LAN->Wake-On-LAN Filter** displays a list of all the WOL filters that have been configured.

21.10.1.1 Edit or New






Choose the  icon to edit existing entries. Choose the **New** button to enter additional filters.

Wake-On-LAN Filter

WOL Rules

Interface Assignment

Basic Parameters

Description	<input type="text"/>
Service	any 
Destination IP Address/Netmask	Any 
Source IP Address/Netmask	Any 
DSCP/TOS Filter (Layer 3)	Ignore 
COS Filter (802.1p/Layer 2)	Ignore 

OK

Cancel

Fig. 189: Local Services->Wake-On-LAN->Wake-On-LAN Filter->New

The **Local Services->Wake-On-LAN->Wake-On-LAN Filter->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter the name of the filter.
Service	<p>Select one of the preconfigured services. The extensive range of services configured ex works includes the following:</p> <ul style="list-style-type: none">• <i>activity</i>• <i>apple-qt</i>• <i>auth</i>• <i>charge</i>• <i>clients_1</i>• <i>daytime</i>• <i>dhcp</i>• <i>discard</i> <p>The default value is <i>Any</i>.</p>
Protocol	<p>Select a protocol.</p> <p>The option <i>Any</i> (default value) matches any protocol.</p>
Type	<p>Only for Protocol = <i>ICMP</i></p> <p>Select the type.</p> <p>Possible values: <i>Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply.</i></p> <p>See RFC 792.</p> <p>The default value is <i>Any</i>.</p>
Connection State	<p>With Protocol = <i>TCP</i>, you can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.• <i>Any</i> (default value): All TCP packets match the filter.
Destination IP Ad-	Enter the destination IP address of the data packets and the


Field	Description
dress/Netmask	corresponding netmask.
Destination Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a destination port number or a range of destination port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The destination port is not specified.• <i>Specify port</i>: Enter a destination port.• <i>Specify port range</i>: Enter a destination port range.
Source IP Address/Netmask	Enter the source IP address of the data packets and the corresponding netmask.
Source Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a source port number or a range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>-All-</i> (default value): The destination port is not specified.• <i>Specify port</i>: Enter a destination port.• <i>Specify port range</i>: Enter a destination port range.
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Ignore</i> (default value): The type of service is ignored.• <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit).• <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).• <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format).• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.

Field	Description
	<ul style="list-style-type: none"><i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.<i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Possible values are whole numbers between 0 and 7. Value range 0 to 7.</p> <p>The default value is <i>Ignore</i>.</p>

21.10.2 WOL Rules

The menu **Local Services->Wake-On-LAN->WOL Rules** displays a list of all the WOL rules that have been configured.

21.10.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional rules.

Wake-On-LAN FilterWOL RulesInterface Assignment

Basic Parameters

Wake-On-LAN Rule Chain

New

Description

Wake-On-LAN Filter

Select one

Action

Invoke WOL if filter matches

Type

Ethernet

Send WOL packet over Interface

Select one

Target MAC-Address

Password

OK

Cancel

Fig. 190: Local Services->Wake-On-LAN->WOL Rules->New

The **Local Services->Wake-On-LAN->WOL Rules->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Wake-On-LAN Rule Chain	<p>Select whether to create a new rule chain or to edit an existing one.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>New</i> (default value): You can create a new rule chain with this setting.• <i><Name of the rule chain></i>: Shows a rule chain that has already been created, which you can select and edit.
Description	<p>Only where Wake-On-LAN Rule Chain = <i>New</i></p> <p>Enter the name of the rule chain.</p>
Wake-On-LAN Filter	<p>Select a WOL filter.</p> <p>If the rule chain is new, select the filter to be set at the first point of the rule chain.</p> <p>If the rule chain already exists, select the filter to be attached to the rule chain.</p> <p>To select a filter, at least one filter must be configured in the Local Services->Wake-On-LAN->WOL Rules menu.</p>
Action	<p>Define the action to be taken for a filtered data packet.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Invoke WOL if filter matches</i>: Run WOL if the filter matches.• <i>Invoke if filter does not match</i>: Run WOL if the filter does not match.• <i>Deny WOL if filter matches</i>: Do not run WOL if the filter matches.• <i>Deny WOL if filter does not match</i>: Do not run WOL if the filter does not match.• <i>Ignore rule and skip to next rule</i>: This rule is ignored and the next one in the chain is examined.
Type	<p>Select whether the Wake on LAN magic packet is to be sent as a UDP packet or as an Ethernet frame via the interface spe-</p>


Field	Description
	cified in Send WOL packet via interface .
Send WOL packet over Interface	Select the interface which is to be used to send the Wake on LAN magic packet.
Target MAC-Address	<p>Only where Action = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p> <p>Enter the MAC address of the network device that is to be enabled using WOL.</p>
Password	<p>Only where Action = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p> <p>If the network device that is to be enabled supports the "SecureOn" function, enter the corresponding password for this device here. The device is only enabled if the MAC address and password are correct.</p>

21.10.3 Interface Assignment

In this menu, the configured rule chains are assigned to individual interfaces which are then monitored for these rule chains.

A list of all configured interface assignments is displayed in the **Local Services->Wake-On-LAN->Interface Assignment** menu.

21.10.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create other entries.

Wake-On-LAN FilterWOL RulesInterface Assignment

Basic Parameters

Interface

Select one

Rule Chain

Select one

OK

Cancel

Fig. 191: Local Services->Wake-On-LAN->Interface Assignment->New

The **Local Services->Wake-On-LAN->Interface Assignment->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.

21.11 BRRP

In the **BRRP** menu you can configure the redundancy of your gateway.



Note

You require a licence for devices in the R23x series and RS series.

BRRP (Bintec Router Redundancy Protocol) is a bintec elmeg-specific implementation of the VRRP (Virtual Router Redundancy Protocol). A router redundancy procedure is used mainly to safeguard the availability of a physical gateway in a LAN or WAN.

Terms and Definitions

A number of special terms are used to describe the function. The following terms are defined in the relevant RFC and in the Internet draft.

BRRP terms

Field	Description
VRRP router	“A router that uses the Virtual Router Redundancy Protocol. It can be integrated into one or more “virtual routers””
Virtual Router	“An abstract object controlled by the VRRP, which is used as default router for the hosts of a LAN. It comprises a Virtual Router Identifier (Virtual Router ID) and an IP address or a group of associated IP addresses in a common LAN. A VRRP router can protect the data traffic of one or more virtual routers.”
IP Address Owner	“The VRRP router that possesses the IP address(es) of the virtual router as real interface address(es). This is the router that – if active - answers packets for ICMP pings, TCP connections, etc. to one of these IP addresses.”
Primary IP Address	“An IP address that is selected from the group of real interface

Field	Description
	addresses. A possible algorithm option is the selection of the first address. VRRP advertisements are always sent with the primary IP address as source of the IP packet.”
VRRP Advertisement	A keepalive that sends the master to the backup gateway to indicate his reachability.
Virtual Router Master	“The VRRP router that takes over forwarding the packets that have been sent to the IP addresses associated with the “virtual router”. It is also responsible for answering ARP (Address Resolution Protocol) requests for these IP addresses.”
Virtual Router Backup	“The group of VRRP routers that take over responsibility for forwarding the packets if the master fails.” In backup status these VRRP routers are inactive, i.e. they do not respond to any ARP requests.”

21.11.1 Virtual Routers

When using a route redundancy protocol, multiple routers are combined into a logical unit. The router redundancy protocol BRRP manages the routes involved and organises these as follows:

It ensures that only one routers within the logical connection is active.

It guarantees that if the active route fails, another router takes over the function of the failed device. The time that each router is active is determined by the priority assigned to the router.

Let us take the example of a simple scenario, in which gateway A provides Internet access for the hosts in a LAN. If this gateway fails, all hosts cannot access the Internet and their routes are configured statically. To allow the hosts continued access to the Internet, gateway B offers all hosts in the LAN the service that gateway A previously performed. All the tasks of a “virtual router” and the switching of services from one gateway to the other are controlled by the BRRP redundancy procedure.

The BRRP conforms to the specifications in RFC 2338 and the relevant Internet draft (see www.ietf.org).

The configuration of the router redundancy procedure is carried out in the following steps:

- Configuration of the interface via which the BRRP advertisement data packets are sent.

**Note**

This interface is used to transmit the BRRP advertisement data packets and possibly to transmit keepalive monitoring data packets. Another interface must be configured in the next step to transmit the usage data.

Configuration of the advertisement interface is performed in the **Local Services->BRRP->Virtual Router->New** menu under **BRRP Advertisement Interface**.

Only the active router in the router group sends advertisement data packets. The IPv4 multicast address 224.0.0.18 is used as the destination address for all routers in the group. All passive routers in the group must monitor this address so that if the advertisement data packets are not received that can react according to their priority and BRRP configuration.

- Configuration of the interface for transmitting usage data (configuration of the virtual interface).

A virtual interface is activated and deactivated by assigning it to a virtual router over the BRRP router redundancy protocol.

Configuration is performed in the **Local Services->BRRP->Virtual Router->New->Ethernet Interface** menu.

In this step, you configure the IP address settings and assign the interface to a virtual router. The properties of the virtual router (e.g. the priority) are also defined here.

**Note**

The system automatically assigns the MAC address of the virtual interface according to the following model: 00:00:5E:00:01:<ID of the virtual router>. The ID of the virtual router therefore determines the MAC address of the interface, which is used to transmit the usage data.

The configuration of the virtual interface (MAC address, IP address) and the configuration of the virtual router (sending interval for advertisement, master down trials) must be identical on all routers with the same virtual router ID within the logical group.

You must use IP addresses from different subnets for the advertisement interface and for the virtual interface.

All virtual interfaces on a physical router should normally have the same priority.

- Configuration of the synchronisation between the virtual router and configuration of the

events, which result in a switching of the operating status of the virtual router.

Controlling the operating status of a virtual router implicitly also controls the operating status of the interface to which the virtual router is linked. If an error occurs, all interfaces on a device have to be deactivated. Consequently, the operating status of all interfaces on a device must be synchronised. This synchronisation is required if multiple interfaces are monitored on a single device. This configuration is performed in the **Local Services->BRRP->VR Synchronisation->New** menu.

- Switching on the redundancy procedure. This configuration is performed in the **Local Services->BRRP->Options** menu.

You configure the advertisement interface and the virtual interface(s) in the **Local Services->BRRP->Virtual Router->New** menu. You must configure the same virtual routers with the same interfaces on all physical routers involved in the redundancy procedure. (However, the virtual routers have different priorities on the various physical routers.)

21.11.1.1 New

Choose the **New** button to configure other virtual routers.

Virtual Routers

VR Synchronisation

Options

BRRP Advertisement Interface

Ethernet Interface

Select one

IP Address

IP Address

Netmask

BRRP Monitored Interface

Virtual Router Interface

Advertisement interface not selected!

Virtual Router IP Address

IP Address

Netmask

255.255.255.0

Add

Virtual Router ID

1

Virtual Router Priority

100

Advanced Settings

Advertisement send interval

1

Master down trials

10

Pre-empt mode (go back into master state)

☒ Enabled

Enable authentication

☐

OK

Cancel


Fig. 192: Local Services->BRRP->Virtual Routers->New

The **Local Services->BRRP->Virtual Routers->New** menu consists of the following fields:

Fields in the BRRP Advertisement Interface menu.

Field	Description
Ethernet Interface	<p>Choose the interface via which BRRP advertisement packets are sent and expected.</p> <p>If you edit a Virtual Router, the Ethernet interface is displayed and cannot be changed.</p> <p>Please note: The Ethernet interface for sending the advertisements is always up and running and cannot therefore be used as the Virtual Router Interface.</p>
IP Address	Shows the IP address(es) of the interface via which BRRP advertisement packets are sent and expected.

Fields in the BRRP Monitored Interface menu.

Field	Description
Virtual Router Interface	<p>Indicates on which physical interface the virtual interface is based, if a new virtual interface is created. The name of the virtual interface is assigned automatically when it is created.</p> <p>Shows the name of the virtual interface, if a virtual interface that has already been created is edited.</p>
Virtual Router IP Address	<p>Enter the IP address and the netmask of the virtual router. Here enter the IP address that you want to use in the local network as the actual gateway IP address.</p>
	<div>Note<p>To avoid problems in the LAN, the IP Address for advertisements and the Virtual Router IP Address cannot originate from the same subnet.</p></div>
Virtual Router ID	<p>Select the ID of the virtual router.</p> <p>This ID identifies the “virtual router” in the LAN and is part of every BRRP advertisement packet that is sent by the current master.</p> <p>Possible values are whole numbers between 1 and 255.</p>

Field	Description
Virtual Interface Priority	<p>Define the transmitted BRRP priority of the interface for the virtual router. Higher priorities determine the master interfaces during the initialization pahse as well as with active Pre-Empt-Mode.Possible values are between 1 and 255. The higher the value, the higher the priority. The value 255 defines that this virtual router always functions as master as soon as it is active.</p> <p>The default value is 100.</p> <p>A priority of 255 is used for routers the IP address of which is idential with the IP address of the virtual router.</p>

In the **Advanced Settings** menu you must configure all of the parameters for all virtual routers identically on all devices in the group. We recommend leaving the preset values.

The menu **Advanced Settings** consists of the following fields:

Fields in the Advanced Settings menu.

Field	Description
Advertisement send interval	<p>Determine how often a BRRP advertisement packet is sent if the virtual router is defined as master. Only the current master sends via multicast BRRP advertisements, which also contain the ID and the priority of the master.</p> <p>Possible values are whole numbers between 1 and 255. The value is indicated in seconds and the default value is 1. 1.</p> <p>An advertisement timer based on the sending interval for advertisements runs in the router and an advertisement packet is sent when the timer expires.</p>
Master down trials	<p>Define the number of BRRP advertisements that must fail before the backup router with the lowest priority assumes that the master is inactive and takes over the role of master.</p> <p>A master down timer based on the Master down trials parameter runs in the router; when this timer expires, the backup assumes that the master is not reachable if no advertisement has been received.</p> <p>The effective master down interval is the time calculated from the number of expected but omitted BRRP advertisements, the advertisement interval and the skew time, which adds a minim-</p>

Field	Description
	<p>um period depending on the priority. The higher the priority, the shorter the time added. Consequently, a backup router with a higher priority responds more quickly than a router with lower priority).</p> <p>Possible values are whole numbers between <i>1</i> and <i>255</i> and the default value is <i>10</i>.</p>
Pre-empt mode (go back into master state)	<p>Define whether a backup router with higher priority has priority over a master router with low priority.</p> <p>Pre-empt mode is used to prevent unnecessary switching.</p> <p>The function is enabled with <i>Enabled</i>. The router with the higher priority always has priority. This means that when the actual master router is accessible once more, it is always enabled. If the function is not enabled, the currently enabled backup router continues to be enabled even when the actual master router is accessible once more, although the priority of the master router is higher than the priority of the backup router which is currently enabled.</p> <p>The function is enabled by default.</p> <p>Note the following exception: If Virtual Interface Priority <i>255</i> is selected, the gateway with this priority certainly takes over the master role, i.e. the setting in Pre-empt mode (go back into master state) is ignored. You should therefore select a Virtual Interface Priority lower than <i>255</i> if you wish to use Pre-empt Mode.</p>
Enable authentication	<p>Enable or disable authentication.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>If the function is active, an input field is displayed. Enter the authentication key here.</p> <p>Please note: Note that the authentication key must be the same for all virtual routers in the group.</p> <p>The function is disabled by default.</p>

21.11.2 VR Synchronisation

The watchdog daemon is configured in the **Local Services->BRRP->VR Synchronisation** menu, i.e. you define how state changes are handled.

After opening the menu **Local Services->BRRP->VR Synchronisation** a list of all synchronisations is displayed. You can either synchronise virtual interfaces or interfaces. New synchronisations can be added in the **New** menu.

For example, you can synchronise both virtual routers R1 and R2 over BRRP. To do this, you must create two entries. For the first entry, as **Monitoring VR / Interface** R1 and as **Synchronisation VR / Interface** you must use R2. For the second entry, as **Monitoring VR / Interface** R2 and as **Synchronisation VR / Interface** you must use R1.

21.11.2.1 New

Select the **New** button to create new synchronisations.

Virtual Routers

VR Synchronisation

Options

Basic Parameters

Monitoring VR / Interface

Monitoring Mode

BRRP

Virtual Router ID

Select one

Synchronisation VR / Interface

Synchronisation Mode

BRRP

Virtual Router ID

Select one

OK

Cancel

Fig. 193: **Local Services->BRRP->VR Synchronisation->New**

The **Local Services->BRRP->VR Synchronisation->New** menu consists of the following fields:

Fields in the Monitoring VR / Interface menu.

Field	Description
Monitoring Mode	<div>Shows which mechanism is used for monitoring a virtual router.</div> <div>Possible values:</div> <div><ul style="list-style-type: none">BRRP:The BRRP-specific state advertisements are used for determining the state of the master. (The master sends ad-</div>

Field	Description
	vertisements as per its configuration in the Local Services->BRRP->Virtual Routers->New->Advanced Settings menu.)
Virtual Router ID	Select a virtual router using the Virtual Router ID and define which interface is to be checked. You can choose previously defined IDs (see Virtual Router ID in the Local Services->BRRP->Virtual Router->New menu under BRRP Monitored Interface). The watchdog daemon requests detailed information entered in the Virtual Routers .

Fields in the Synchronisation VR / Interface menu.

Field	Description
Synchronisation Mode	Indicates the mechanism with which virtual routers or interfaces are synchronised: Possible values: <ul style="list-style-type: none">• <i>BRRP</i>: BRRP is used to synchronise the virtual router.
Virtual Router ID	Select the ID of the virtual router to be synchronised. Synchronising the virtual router implicitly synchronises the virtual interface associated with the virtual router.

21.11.3 Options

In the **Local Services->BRRP->Options** menu,you can enable or disable the BRRP function.



Fig. 194: Local Services->BRRP->Options

The **Local Services->BRRP->Options**menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Enable BRRP	<p>Enable or disable the BRRP function.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Chapter 22 Maintenance

This menu provides you with numerous functions for maintaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you need other languages for the configuration interface, you can import these. You can also trigger a system reboot in this menu.

22.1 Diagnostics

In the **Maintenance->Diagnostics** menu, you can test the availability of individual hosts, the resolution of domain names and certain routes.

22.1.1 Ping Test

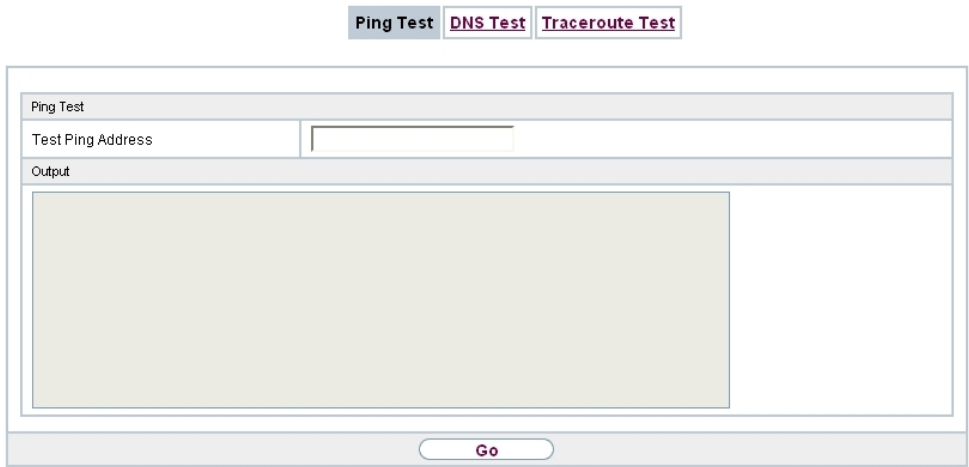


Fig. 195: Maintenance->Diagnostics->Ping Test

You can use the ping test to check whether a certain host in the LAN or an internet address can be reached. The **Output**field displays the ping test messages. The ping test is launched by entering the IP address to be tested in **Test Ping Address** and clicking the **Go** button.

22.1.2 DNS Test

Ping TestDNS TestTraceroute Test

DNS Test

DNS Address

Output

Go

Fig. 196: Maintenance->Diagnostics->DNS Test

The DNS test is used to check whether the domain name of a particular host is correctly re-solved. The **Output**field displays the DSN test messages. The ping test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

22.1.3 Traceroute Test

Ping TestDNS TestTraceroute Test

Traceroute Test

Traceroute Address

Output

Go

Fig. 197: Maintenance->Diagnostics->Traceroute Test

You use the traceroute test to display the route to a particular address (IP address or domain name), if this can be reached. The **Output** field displays the traceroute test messages. The ping test is launched by entering the IP address to be tested in **Traceroute Address** and clicking the **Go** button.

22.2 Software & Configuration

You can use this menu to manage the software version of your device, your configuration files and the language of the **GUI**.

22.2.1 Options

Your device contains the version of the system software available at the time of production. More recent versions may have since been released. You may therefore need to carry out a software update.

Every new system software includes new features, better performance and any necessary bugfixes from the previous version. You can find the current system software at www.bintec-elmeg.com. The current documentation is also available here.



Important

If you want to update your software, make sure you consider the corresponding release notes. These describe the changes implemented in the new system software.

The result of an interrupted update (e.g. power failure during the update) could be that your gateway no longer boots. Do not turn your device off during the update.

An update of BOOTmonitor and/or Logic is recommended in a few cases. In this case, the release notes refer expressly to this fact. Only update BOOTmonitor or Logic if bintec elmeg GmbH explicitly recommends this.

Flash

Your device saves its configuration in configuration files in the flash EEPROM (Electrically Erasable Programmable Read Only Memory). The data even remains stored in the flash when your device is switched off.

RAM

The current configuration and all changes you set on your device during operation are

stored in the working memory (RAM). The contents of the RAM are lost if the device is switched off. So if you modify your configuration and want to keep these changes for the next time you start your device, you must save the modified configuration in the flash memory before switching off: The **Save configuration** button over the navigation area of the **GUI**. This configuration is then saved in the flash in a file with the name *boot*. When you start your device, the *boot* configuration file is used by default.

Actions

The files in the flash memory can be copied, moved, erased and newly created. It is also possible to transfer configuration files between your device and a host via HTTP.

Configuration file format

The file format of the configuration file allows encryption and ensures compatibility when restoring the configuration on the gateway in various system software versions. This is a CSV format, which can be read and modified easily. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The administrator can store encrypted backup files for the configuration. When the configuration is sent by e-mail (e.g for support purposes) confidential configuration data can be protected fully if required. You can save or import files with the actions "Export configuration", "Export configuration with status information" and "Load configuration". If you want to save a configuration file with the action ""Export configuration" or "Export configuration with status information", you can choose whether the configuration file is saved encrypted or without encryption.



Caution

If you have saved a configuration file in an old format via the SNMP shell with the `put` command, there is no guarantee that it can be reloaded to the device. As a result, the old format is no longer recommended.

Options

Currently Installed Software	
BOSS	V.9.1 Rev. 1 IPSec from 2012/06/29 00:00:00
System Logic	1.1
Software and Configuration Options	
Action	No Action

Go

Fig. 198: Maintenance->Software & Configuration ->Options

The **Maintenance->Software & Configuration->Options** menu consists of the following fields:

Fields in the Currently Installed Software menu.

Field	Description
BOSS	Shows the current software version loaded on your device.
System Logic	Shows the current system logic loaded on your device.
ADSL Logic	Shows the current version of the ADSL logic loaded on your device.

Fields in the Software and Configuration Options menu.

Field	Description
Action	<p>Select the action you wish to execute.</p> <p>After each task, a window is displayed showing the other steps that are required.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>No Action</i> (default value):• <i>Export configuration</i>: The configuration file Current File Name in Flash is transferred to your local host. If you click the Go button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name.• <i>Import configuration</i>: Under Filename select a configuration file you want to import. Please note: Click Go to first load the file under the name <i>boot</i> in the flash memory for the device. You must restart the device to enable it. <p>Please note: The files to be imported must be in CSV format!</p> <ul style="list-style-type: none">• <i>Copy configuration</i>: The configuration file in the Source File Name field is saved as Destination File Name.• <i>Delete configuration</i>: The configuration in the Select file field is deleted.• <i>Rename configuration</i>: The configuration file in the Select file field is renamed to New File Name.• <i>Restore backup configuration</i>: Only if, under Save configuration with the setting <i>Save configuration and</i>

Field	Description
	<p><i>back up previous boot configuration</i> the current configuration was saved as boot configuration and the previous boot configuration was also archived.</p> <p>You can load back the archived boot configuration.</p> <ul style="list-style-type: none">• <i>Delete software/firmware</i>: The file in the Select file field is deleted.• <i>Import language</i>: You can import additional language versions of the GUI into your device. You can download the files to your PC from the download area at www.bintec-elmeg.com and from there import them to your device• <i>Update system software</i>: You can launch an update of the system software, the ADSL logic and the BOOTmonitor.• <i>Import Voice Mail Wave Files</i>: (Only displayed if an SD card is inserted.) In file name, select the <i>vms_wavfiles.zip</i> file that you wish to import.• <i>Export configuration with state information</i>: The active configuration from the RAM is transferred to your local host. If you click the Go button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name.
Configuration Encryption	<p>Only for Action = <i>Import configuration, Export configuration, Export configuration with state information</i>. Define whether the data of the selected Action are to be encrypted.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>If the function is enabled, you can enter the Password in the text field.</p>
Filename	<p>Only for Action = <i>Import configuration, Import language Update system software</i>.</p> <p>Enter the path and name of the file or select the file with Browse... via the explorer/finder.</p>
Source Location	<p>Only for Action = <i>Update system software</i></p>

Field	Description
	<p>Select the source of the update.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Local File</i> (default value): The system software file is stored locally on your PC.• <i>HTTP Server</i>: The file is stored on a remote server specified in the URL.• <i>Current Software from Update Server</i>: The file is on the official update server.
URL	<p>Only for Source Location = <i>HTTP Server</i></p> <p>Enter the URL of the update server from which the system software file is loaded.</p>
Current File Name in Flash	<p>For Action = <i>Export configuration</i></p> <p>Select the configuration file to be exported.</p>
Include certificates and keys	<p>For Action = <i>Export configuration, Export configuration with state information</i></p> <p>Define whether the selected Action should also be applied for certificates and keys.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Source File Name	<p>Only for Action = <i>Copy configuration</i></p> <p>Select the source file to be copied.</p>
Destination File Name	<p>Only for Action = <i>Copy configuration</i></p> <p>Enter the name of the copy.</p>
Select file	<p>Only for Action = <i>Rename configuration, Delete configuration or Delete software/firmware</i></p> <p>Select the file or configuration to be renamed or deleted.</p>
New File Name	<p>Only for Action = <i>Rename configuration</i></p>

Field	Description
	Enter the new name of the configuration file.

22.3 Reboot

22.3.1 System Reboot

In this menu, you can trigger an immediate reboot of your device. Once your system has restarted, you must call the **GUI** again and log in.

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** chapter of the manual.



Note

Before a reboot, make sure you confirm your configuration changes by clicking the **Save configuration** button, so that these are not lost when you reboot.

System Reboot

Do you really want to reboot the system now?

OK

Fig. 199: **Maintenance->Reboot->System Reboot**

If you wish to restart your device, click the **OK** button. The device will reboot.

Chapter 23 External Reporting

In this system menu, you define what system protocol messages are saved on which computers, and whether the system administrator should receive an e-mail for certain events. Information on IP data traffic can also be saved--depending on the individual interfaces. In addition, SNMP traps can be sent to specific hosts in case of error. Moreover, you can prepare your device for monitoring with the activity monitor.

23.1 Syslog

Events in various subsystems of your device (e.g. PPP) are logged in the form of syslog messages (system logging messages). The number of messages visible depends on the level set (eight steps from *Emergency* over *Information* to *Debug*).

In addition to the data logged internally on your device, all information can and should be transmitted to one or more external PCs for storage and processing, e.g. to the system administrator's PC. The syslog messages saved internally on your device are lost when you reboot.



Warning

Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon

All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at www.bintec-elmeg.com).

23.1.1 Syslog Servers

Configure your device as a syslog server so that defined system messages can be sent to suitable hosts in the LAN.

In this menu, you define which messages are sent to which hosts and with which conditions.

A list of all configured system log servers displayed in the **External Reporting->Syslog->Syslog Servers** menu.

23.1.1.1 New

Select the **New** button to set up additional syslog servers.

Syslog Servers

Basic Parameters

IP Address

Level

Information

Facility

local0

Timestamp

☒ None ☐ Time ☐ Date & Time

Protocol

☒ UDP ☐ TCP

Type of Messages

☐ System ☐ Accounting ☒ System & Accounting

OK

Cancel

Fig. 200: **External Reporting->Syslog->Syslog Servers->New**

The menu **External Reporting->Syslog->Syslog Servers->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the host to which syslog messages are passed.
Level	<div>Select the priority of the syslog messages that are to be sent to the host.</div> <div>Possible values:</div> <div><ul style="list-style-type: none">Emergency (highest priority)AlertCriticalErrorWarningNoticeInformation (default value)</div>

Field	Description
	<ul style="list-style-type: none">• <i>Debug</i> (lowest priority) <p>Syslog messages are only sent to the host if they have a higher or identical priority to that indicated, i.e. at syslog level <i>Debug</i> all messages generated are forwarded to the host.</p>
Facility	<p>Enter the syslog facility on the host.</p> <p>This is only required if the Log Host is a Unix computer.</p> <p>Possible values: <i>local0</i> - 7</p> <p>.</p> <p>The default value is <i>local0</i>.</p>
Timestamp	<p>Select the format of the time stamp in the syslog.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): No system time indicated.• <i>Time</i>: System time without date.• <i>Date &Time</i>: System time with date.
Protocol	<p>Select the protocol for the transfer of syslog messages. Note that the syslog server must support the protocol.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>UDP</i> (default value)• <i>TCP</i>
Type of Messages	<p>Select the message type.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>System &Accounting</i> (default value)• <i>System</i>• <i>Accounting</i>

23.2 IP Accounting

In modern networks, information about the type and number of data packets sent and received over the network connections is often collected for commercial reasons. This information is extremely important for Internet Service Providers that bill their customers by data volume.

However, there are also non-commercial reasons for detailed network accounting. If, for example, you manage a server that provides different kinds of network services, it is useful for you to know how much data is generated by the individual services.

Your device contains the IP Accounting function, which enables you to collect a lot of useful information about the IP network traffic (each individual IP session).

23.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

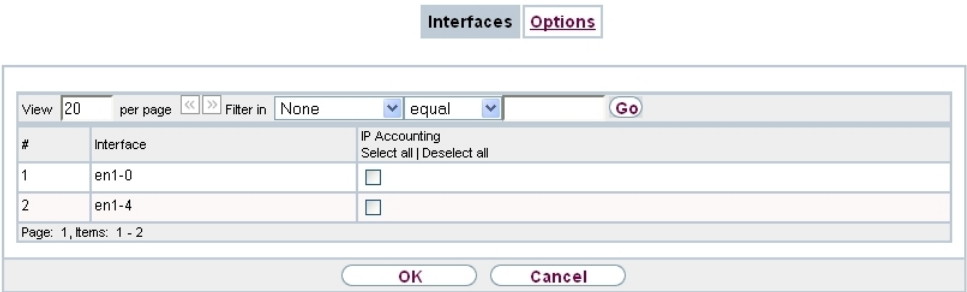


Fig. 201: External Reporting->IP Accounting->Interfaces

In the **External Reporting->IP Accounting->Interfaces** menu, a list of all interfaces configured on your device is shown. For each entry, you can activate IP Accounting by setting the checkmark. In the **IP Accounting** column, you do not need to click each entry individually. Using the options **Select all** or **Deselect all** you can enable or disable the IP accounting function for all interfaces simultaneously.

23.2.2 Options

In this menu, you configure general settings for IP Accounting.

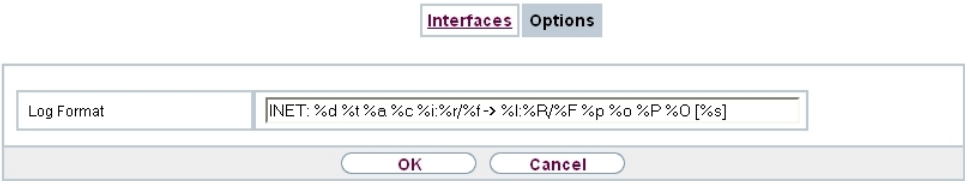


Fig. 202: External Reporting->IP Accounting->Options

In the **External Reporting->IP Accounting->Options** menu, you can define the **Log Format** of the IP accounting messages. The messages can contain character strings in any order, sequences separated by a slash, e.g. `\t` or `\n` or defined tags.

Possible format tags:

Format tags for IP Accounting messages

Field	Description
%d	Date of the session start in the format DD.MM.YY
%t	Time of the session start in the format HH:MM:SS
%a	Duration of the session in seconds
%c	Protocol
%i	Source IP Address
%r	Source Port
%f	Source interface index
%l	Destination IP Address
%R	Destination Port
%F	Destination interface index
%p	Packets sent
%o	Octets sent
%P	Packets received
%O	Octets received
%s	Serial number for accounting message
%%	%

By default, the following format instructions are entered in the **Log Format** field: `INET: %d %t %a %c %i:%r/%f -> %l:%R/%F %p %o %P %O [%s]`

23.3 Alert Service

It was previously possible to send syslog messages from the router to any syslog host. Depending on the configuration, e-mail alerts are sent to the administrator as soon as relevant syslog messages appear.

23.3.1 Alert Recipient

A list of Syslog messages is displayed in the **Alert Recipient** menu.

23.3.1.1 New

Select the **New** to create additional alert recipients.

Alert Recipient

Alert Settings

Add / Edit Alert Recipient

Alert Service	E-mail
Recipient	<input type="text"/>
Message Compression	<input checked="" type="checkbox"/> Enabled
Subject	<input type="text"/>
Event	Syslog contains string <input type="button" value="v"/>
Matching String	<input type="text"/> (Wildcards allowed)
Severity	Emergency <input type="button" value="v"/>
Monitored Subsystems	<div>Subsystem <input type="button" value="Add"/></div>
Message Timeout	<input type="text" value="60"/>
Number of Messages	<input type="text" value="1"/>

OK

Cancel

Fig. 203: External Reporting->Alert Service->Alert Recipient->New

The menu **External Reporting->Alert Service->Alert Recipient->New** consists of the following fields:

Fields in the Add / Edit Alert Recipient menu.

Field	Description
Alert Service	Displays the alert service. You can select an alert service for devices with UMTS.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• E-mail• SMS
Recipient	<p>Enter the recipient's e-mail address. The entry is limited to 40 characters.</p>
Message Compression	<p>Select whether the text in the alert E-mail is to be shortened. The e-mail then contains the syslog message only once plus the number of relevant events.</p> <p>Enable or disable the field.</p> <p>The function is enabled by default.</p>
Subject	<p>You can enter a subject.</p>
Event	<p>This feature is available only for devices with Wireless LAN Controller.</p> <p>Select the event to trigger an email notification.</p> <p>Possible values:</p> <ul style="list-style-type: none">• <i>Syslog contains string</i> (default value): A Syslog message includes a specific string.• <i>New Neighbor AP found</i>: A new adjacent AP has been found.• <i>New Rogue AP found</i>: A new Rough AP has been found, i.e. an AP using an SSID of its own network, yet is not a component of this network.• <i>New Slave AP (WTP) found</i>: A new unconfigured AP has reported to the WLAN.• <i>Managed AP offline</i>: A managed AP is no longer accessible.
Matching String	<p>You must enter a "Matching String". This must occur in a syslog message as a necessary condition for triggering an alert.</p> <p>The entry is limited to 55 characters. Bear in mind that without the use of wildcards (e.g. "*"), only those strings that correspond exactly to the entry fulfil the condition. The "Matching String"</p>

Field	Description
	entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter "".
Severity	<p>Select the severity level which the string configured in the Matching String field must reach to trigger an e-mail alert.</p> <p>Possible values:</p> <p><i>Emergency (default value), Alert, Critical, Error, Warning, Notice, Information, Debug</i></p>
Monitored Subsystems	<p>Select the subsystems to be monitored.</p> <p>Add new subsystems with Add.</p>
Message Timeout	<p>Enter how long the router must wait after a relevant event before it is forced to send the alert mail.</p> <p>Possible values are 0 to 86400. The value 0 disables the timeout. The default value is 60.</p>
Number of Messages	<p>Enter the number of syslog messages that must be reached before an E-mail can be sent for this case. If timeout is configured, the mail is sent when this expires, even if the number of messages has not been reached.</p> <p>Possible values are 0 to 99; the default value is 1.</p>

23.3.2 Alert Settings

Alert Recipient

Alert Settings

Basic Parameters

Alert Service

☒ Enabled

Maximum E-mails per Minute

6

E-mail Parameters

Sender E-mail Address

SMTP Server

SMTP Authentication

☒ None ☐ ESMTP ☐ SMTP after POP

OK

Cancel

Fig. 204: External Reporting->Alert Service->Alert Settings

The menu **External Reporting->Alert Service->Alert Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Alert Service	<p>Select whether the alert service is to be enabled for the interface.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
Maximum E-mails per Minute	<p>Limit the number of outgoing mails per minute. Possible values are <i>1</i> to <i>15</i>, the default value is <i>6</i>.</p>

Fields in the E-mail Parameters menu.

Field	Description
Sender E-mail Address	<p>Enter the mail address to be entered in the sender field of the E-mail.</p>
SMTP Server	<p>Enter the address (IP address or valid DNS name) of the mail server to be used for sending the mails.</p> <p>The entry is limited to 40 characters.</p>
SMTP Authentication	<p>Authentication expected by the SMTP server.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none">• <i>None</i> (default value): The server accepts and send emails without further authentication.• <i>ESMTP</i>: The server only accepts e-mails if the router logs in with the correct user name and password.• <i>SMTP after POP</i>: The server requires that e-mails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an e-mail.
User Name	<p>Only if SMTP Authentication = <i>ESMTP</i> or <i>SMTP after POP</i></p> <p>Enter the user name for the POP3 or SMTP server.</p>
Password	<p>Only if SMTP Authentication = <i>ESMTP</i> or <i>SMTP after POP</i></p> <p>Enter the password of this user.</p>
POP3 Server	<p>Only if SMTP Authentication = <i>SMTP after POP</i></p> <p>Enter the address of the server from which the e-mails are to be retrieved.</p>
POP3 Timeout	<p>Only if SMTP Authentication = <i>SMTP after POP</i></p> <p>Enter how long the router must wait after the POP3 call before it is forced to send the alert mail.</p> <p>The default value is <i>600</i> seconds.</p>

Fields in the SMS Parameters menu (for devices with UMTS only)

Field	Description
SMS Device	<p>You can receive notification of system alerts in text messages. Select the device to be used to send the text message.</p>
Maximum SMS per Day	<p>Limit the maximum number of SMS sent during a single day.</p> <p>Activating <i>No Limitation</i> allows any number of SMS to be sent.</p> <p>The default value is 10 SMS per day.</p> <p>Note: Entering a value of <i>0</i> is equivalent to activating <i>No Limitation</i>.</p>

23.4 SNMP

SNMP (Simple Network Management Protocol) is a protocol from the IP protocol family for transporting management information about network components.

Every SNMP management system contains an MIB. SNMP can be used to configure, control and administrate various network components from one system. Such an SNMP tool is included on your device: the Configuration Manager. As SNMP is a standard protocol, you can use any other SNMP managers, e.g. HPOpenView.

For more information on the SNMP versions, see the relevant RFCs and drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

23.4.1 SNMP Trap Options

In the event of errors, a message - known as a trap packet - is sent unrequested to monitor the system.

In the **External Reporting->SNMP->SNMP Trap Options** menu, you can configure the sending of traps.

SNMP Trap Options [SNMP Trap Hosts](#)

Basic Parameters

SNMP Trap Broadcasting	<input checked="" type="checkbox"/> Enabled
SNMP Trap UDP Port	162
SNMP Trap Community	snmp-trap

OK

Cancel

Fig. 205: **External Reporting->SNMP->SNMP Trap Options**

The menu **External Reporting->SNMP->SNMP Trap Options** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
SNMP Trap Broadcast-	Select whether the transfer of SNMP traps is to be activated.

Field	Description
ing	<p>Your device then sends SNMP traps to the LAN's broadcast address.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
SNMP Trap UDP Port	<p>Only if SNMP Trap Broadcasting is enabled.</p> <p>Enter the number of the UDP port to which your device is to send SNMP traps.</p> <p>Any whole number is possible.</p> <p>The default value is <i>162</i>.</p>
SNMP Trap Community	<p>Only if SNMP Trap Broadcasting is enabled.</p> <p>Enter a new SNMP code. This must be sent by the SNMP Manager with every SNMP request so that this is accepted by your device.</p> <p>A character string of between <i>0</i> and <i>255</i> characters is possible.</p> <p>The default value is <i>SNMP Trap</i>.</p>

23.4.2 SNMP Trap Hosts

In this menu, you specify the IP addresses to which your device is to send the SNMP traps.

In the **External Reporting->SNMP->SNMP Trap Hosts** menu, a list of all configured SNMP trap hosts is displayed.

23.4.2.1 New

Select the **New** button to create additional SNMP trap hosts.

SNMP Trap Options

SNMP Trap Hosts

Basic Parameters

IP Address

OK

Cancel

Fig. 206: External Reporting->SNMP->SNMP Trap Hosts->New

The menu **External Reporting->SNMP->SNMP Trap Hosts->New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the SNMP trap host.

Field	Description
Subsystem	Displays which subsystem of the device generated the message.
Message	Displays the message text.

24.2 IPSec

24.2.1 IPSec Tunnels

A list of all configured IPSec tunnel providers is displayed in the **Monitoring->IPSec->IPSec Tunnels** menu.

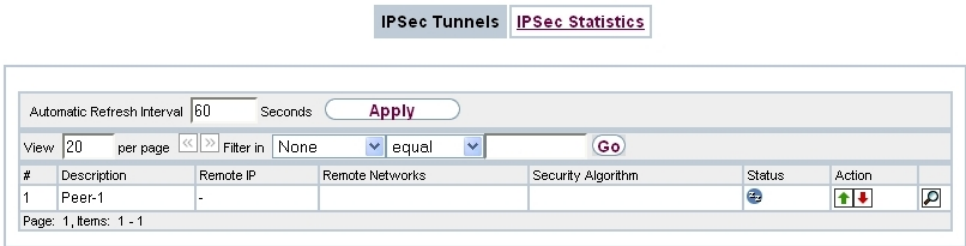





Fig. 208: **Monitoring->IPSec->IPSec Tunnels**

Values in the IPSec Tunnels list

Field	Description
Description	Displays the name of the IPSec tunnel.
Remote IP	Displays the IP address of the remote IPSec Peers.
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by clicking the  button or the  button in the **Action** column.

By clicking the  button, you display detailed statistics on the IPSec connection.

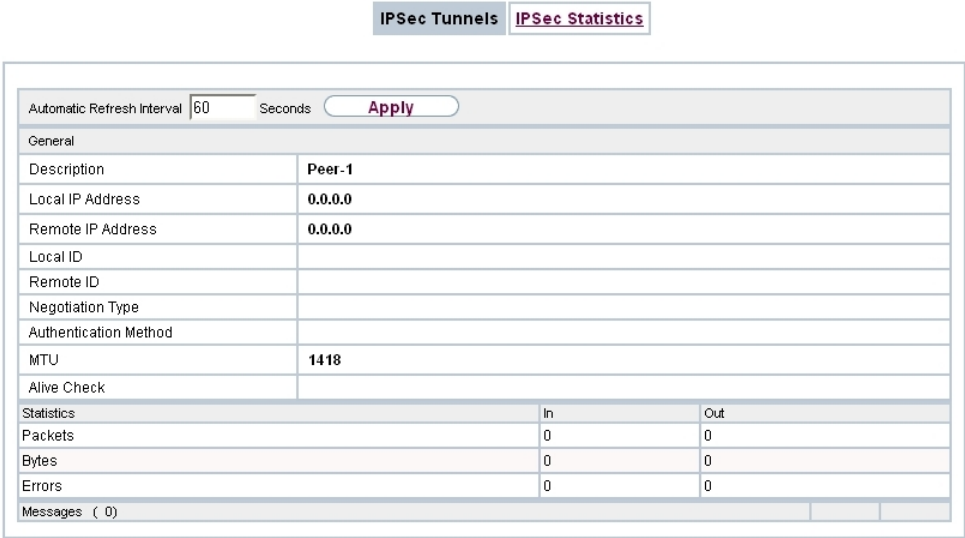


Fig. 209: Monitoring->IPSec->IPSec Tunnels->

Values in the IPSec Tunnels list

Field	Description
Description	Shows the description of the peer.
Local IP Address	Shows the WAN IP address of your device.
Remote IP Address	Shows the WAN IP address of the connection partner.
Local ID	Shows the ID of your device for this IPSec tunnel.
Remote ID	Shows the ID of the peer.
Negotiation Type	Shows the exchange type.
Authentication Method	Shows the authentication method.
MTU	Shows the current MTU (Maximum Transfer Unit).
Alive Check	Shows the method for checking that the peer is reachable.
NAT Detection	Displays the NAT detection method.
Local Port	Shows the local port.
Remote Port	Shows the remote port.
Packets	Shows the total number of incoming and outgoing packets.
Bytes	Shows the total number of incoming and outgoing bytes.
Errors	Shows the total number of errors.
IKE (Phase-1) SAs (x)	The parameters of the IKE (Phase 1) SAs are displayed here.

Field	Description
Role / Algorithm / Life-time remaining / Status	
IPSec (Phase-2) SAs (x)	Shows the parameters of the IPSec (Phase 2) SAs.
Role / Algorithm / Life-time remaining / Status	
Messages	The system messages for this IPSec tunnel are displayed here.

24.2.2 IPSec Statistics

In the **Monitoring->IPSec->IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

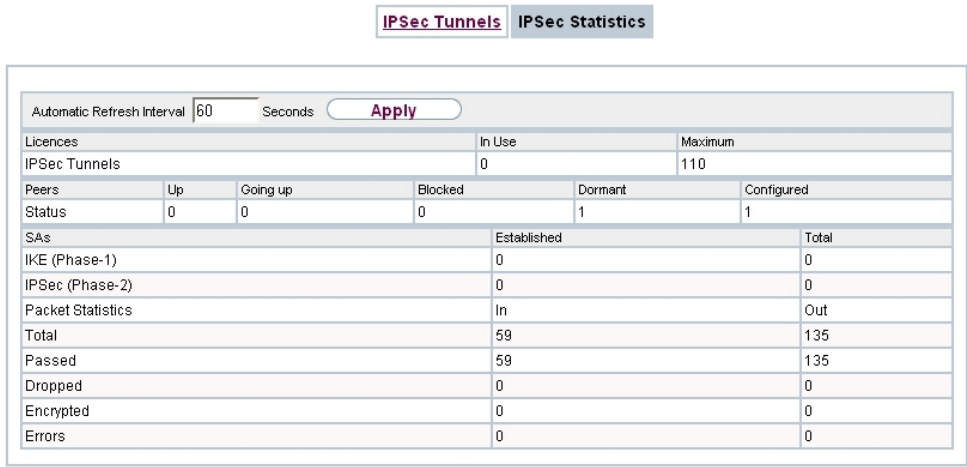


Fig. 210: Monitoring->IPSec->IPSec Statistics

The **Monitoring->IPSec->IPSec Statistics** menu consists of the following fields:

Fields in the Licences menu

Field	Description
IPSec Tunnels	Shows the IPSec licences currently in use (In Use) and the maximum number of licenses usable (Maximum).

Fields in the Peers menu

Field	Description
Status	<p>Displays the number of IPSec tunnels by their current status.</p> <ul style="list-style-type: none">• Up: Currently active IPSec tunnels.• Going up: IPSec tunnels currently in the tunnel setup phase.• Blocked: IPSec tunnels that are blocked.• Dormant: Currently inactive IPSec tunnels.• Configured: Configured IPSec tunnels.

Fields in the SAs menu.

Field	Description
IKE (Phase-1)	Shows the number of active phase 1 SAs (Established) from the total number of phase 1 SAs (Total).
IPSec (Phase-2)	Shows the number of active phase 2 SAs (Established) from the total number of phase 2 SAs (Total).

Fields in the Packet Statistics menu.

Field	Description
Total	Shows the number of all processed incoming (In) or outgoing (Out) packets.
Passed	Shows the number of incoming (In) or outgoing (Out) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (In) or outgoing (Out) packets.
Encrypted	Shows the number of all incoming (In) or outgoing (Out) packets protected by IPSec.
Errors	Shows the number of incoming (In) or outgoing (Out) packets for which processing led to errors.

24.3 Interfaces

24.3.1 Statistics

In the **Monitoring->Interfaces->Statistics** menu, current values and activities of all device interfaces are displayed.

With the filter bar, you can select whether to display **Transfer Totals** or **Transfer Throughput**. The values per second are shown on the **Transfer Throughput** display.

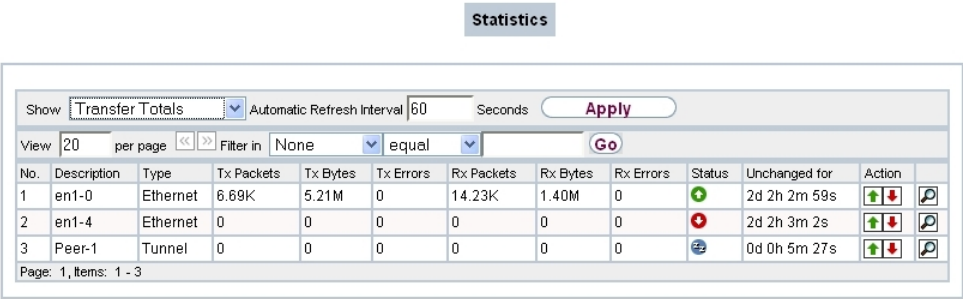


Fig. 211: Monitoring->Interfaces->Statistics

Change the status of the interface by clicking the or the button in the **Action** column.

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Click the button to display the statistical data for the individual interfaces in detail.

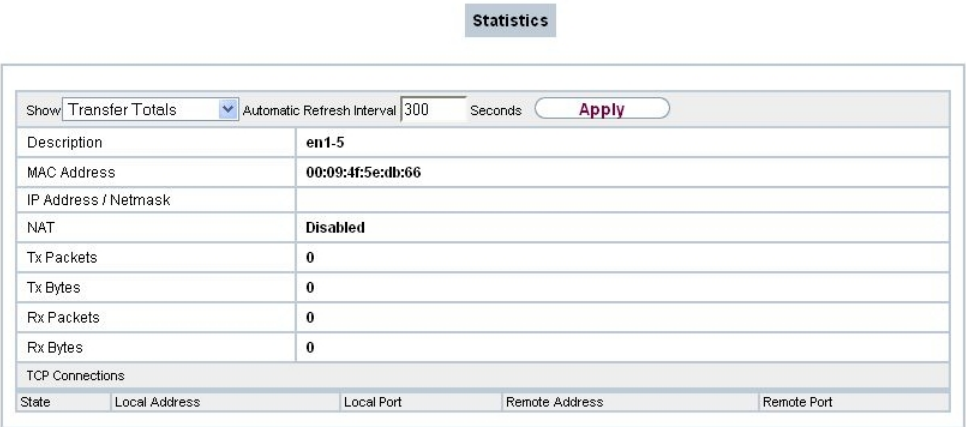


Fig. 212: Monitoring->Interfaces->Statistics->

Values in the Statistics list

Field	Description
Description	Displays the name of the interface.
MAC Address	Displays the interface text.
IP Address / Netmask	Shows the IP address and the netmask.
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections menu

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.
Remote Port	Displays the port to which an active TCP connection exists.

24.4 WLAN

24.4.1 WLANx

In the **Monitoring->WLAN->WLAN** menu, current values and activities of the WLAN interface are displayed. The values for wireless mode 802.11n are listed separately.

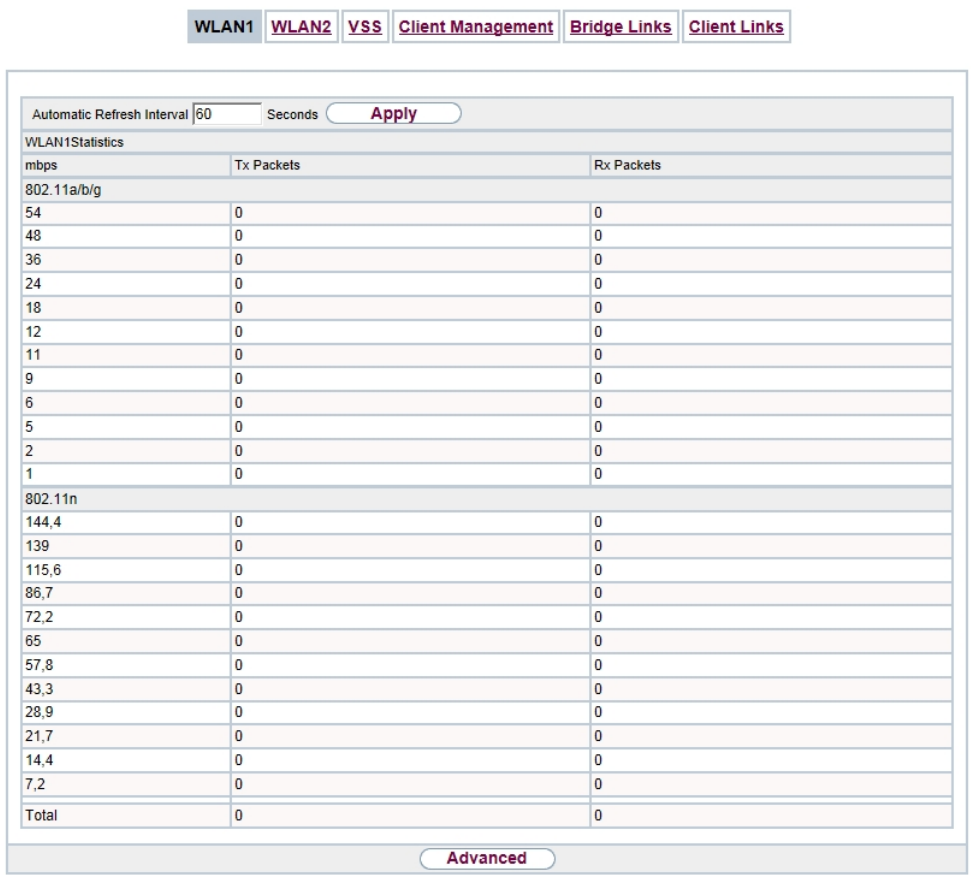


Fig. 213: Monitoring->WLAN->WLAN

Values in the WLAN list

Field	Description
mbps	Displays the possible data rates on this wireless module.
Tx Packets	Shows the total number of packets sent for the data rate shown in mbps.

Field	Description
Rx Packets	Shows the total number of received packets for the data rate shown in mbps .

You can choose the **Advanced** button to go to an overview of more details.

WLAN1

WLAN2

VSS

Client Management

Bridge Links

Client Links

Automatic Refresh Interval

300

Seconds

Apply

#	Description	Value
1	Unicast MSDUs transmitted successfully	0
2	Multicast MSDUs transmitted successfully	0
3	Transmitted MPDUs	0
4	Multicast MSDUs received successfully	0
5	Unicast MPDUs received successfully	0
6	MSDUs that could not be transmitted	0
7	Frame transmissions without ACK received	0
8	Duplicate received MSDUs	0
9	CTS frames received in response to an RTS	0
10	Received MPDUs that couldn't be decrypted	0
11	RTS frames with no CTS received	0
12	Corrupt Frames Received	0

Back

Fig. 214: Monitoring->WLAN->WLAN->Advanced

Values in the Advanced list

Field	Description
Description	Displays the description of the displayed value.
Value	Displays the statistical value.

Meaning of the list entries

Description	Meaning
Unicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to unicast addresses since the last reset. An acknowledgement was received for each of these packets.
Multicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to multicast addresses (including the broadcast MAC address).
Transmitted MPDUs	Displays the number of MPDUs received successfully.
Multicast MSDUs received successfully	Displays the number of successfully received MSDUs that were sent with a multicast address.
Unicast MPDUs re-	Displays the number of successfully received MSDUs that were

Description	Meaning
ceived successfully	sent with a unicast address.
MSDUs that could not be transmitted	Displays the number of MSDUs that could not be sent.
Frame transmissions without ACK received	Displays the number of sent framesfor which an acknowledge-ment frame was not received.
Duplicate received MS-DUs	Displays the number of MSDUs received in duplicate.
CTS frames received in response to an RTS	Displays the number of received CTS (clear to send) frames that were received as a response to RTS (request to send).
Received MPDUs that couldn't be decrypted	Displays the number of received MSDUs that could not be en-crypted. One reason for this could be that a suitable key was not entered.
RTS frames with no CTS received	Displays the number of RTS frames for which no CTS was re-ceived.
Corrupt Frames Re-ceived	Displays the number of frames received incompletely or with er-rors.

24.4.2 VSS

In the **Monitoring->WLAN->VSS** menu, current values and activities of the configured wireless networks are displayed.

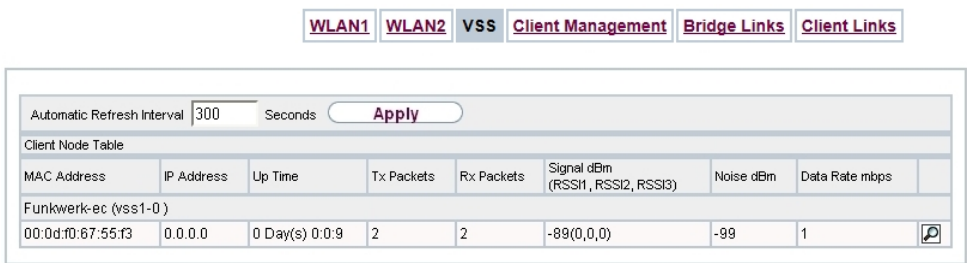



Fig. 215: Monitoring->WLAN->VSS

Values in the VSS list

Field	Description
MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the cli-ent is logged in.

Field	Description
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	<div>Shows the current transmission rate of data received by this client in mbps.</div> <div>The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24, 18, 12, 9, 6 mbps.</div> <div>If the 5 GHz frequency band is used, the indication of 11, 5.5, 2 and 1 mbps is suppressed for IEEE 802.11b.</div>

VSS - Details for Connected Clients

In the **Monitoring->WLAN->VSS-><Connected Client>** -> menu, the current values and activities of a connected client are shown. The values for wireless mode 802.11n are listed separately.

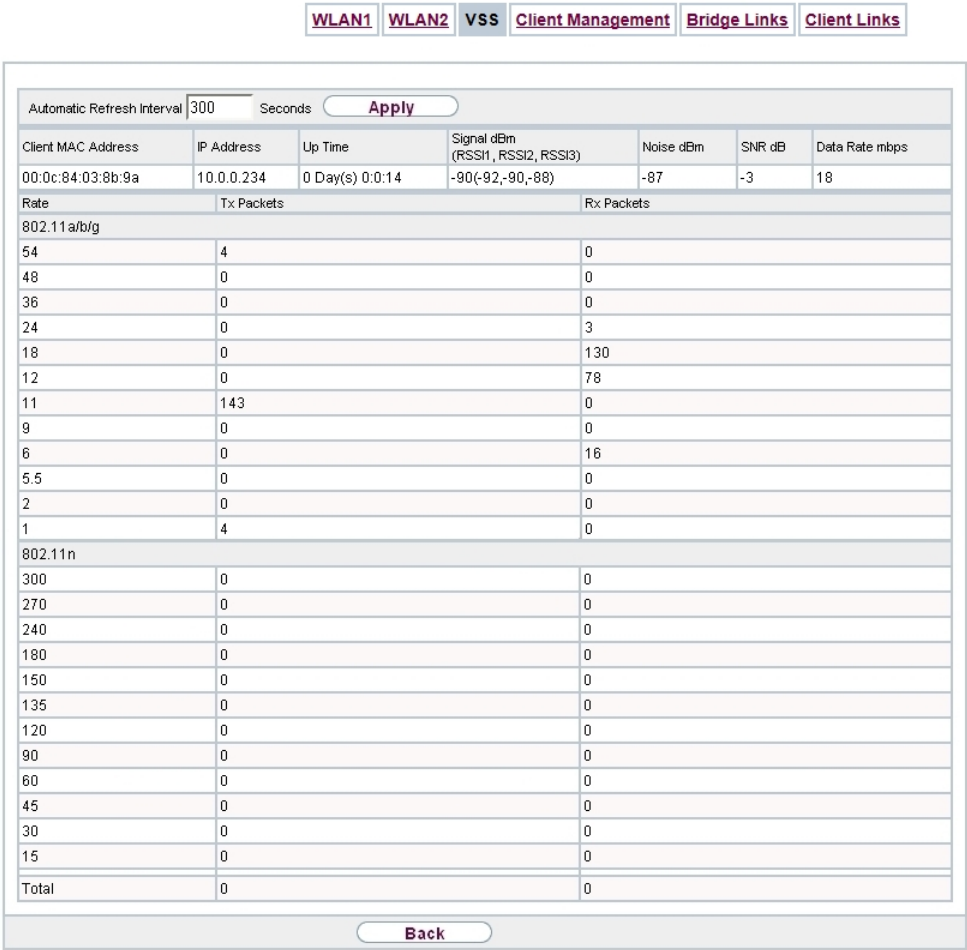


Fig. 216: Monitoring->WLAN->VSS-><connected client>->

Values in the list <Connected Client>

Field	Description
Client MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the client is logged in.
Signal dBm(RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Signal-to-Noise Ratio in dB is an indicator of the quality of the

Field	Description
	wireless connection. Values: <ul style="list-style-type: none">• > 25 dB excellent• 15 – 25 dB good• 2 – 15 dB borderline• 0 – 2 dB bad.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24, 18, 12, 9.6 Mbps. If the 5-GHz frequency band is used, the indication of 11, 5.5, 2 and 1 Mbps is suppressed for IEEE 802.11b.
Rate	Displays the possible data rates on the wireless module.
Tx Packets	Shows the number of sent packets for the data rate.
Rx Packets	Shows the number of received packets for the data rate.

24.5 Bridges

24.5.1 br<x>

In the **Monitoring->Bridges-> br<x>** menu, the current values of the configured bridges are shown.



Fig. 217: Monitoring->Bridges

Values in the br<x> list

Field	Description
MAC Address	Shows the MAC addresses of the associated bridge.

Field	Description
Port	Shows the port on which the bridge is active.

24.6 HotSpot Gateway

24.6.1 HotSpot Gateway

A list of all linked hotspot users is displayed in the **Monitoring->HotSpot Gateway->HotSpot Gateway** menu.

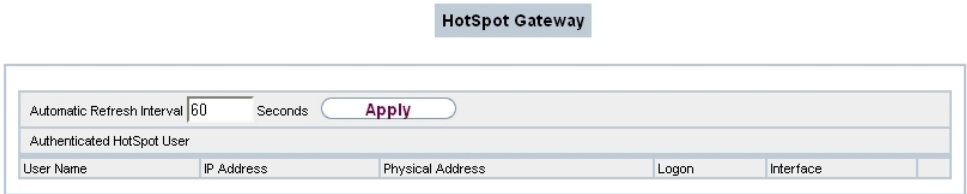


Fig. 218: **Monitoring->HotSpot Gateway->HotSpot Gateway**

Values in the HotSpot Gateway list

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Displays the time of the notification.
Interface	Shows the interface used.

24.7 QoS

In the **Monitoring->QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

24.7.1 QoS

A list of all interfaces for which QoS was configured is displayed in the **Monitoring->QoS->QoS** menu.

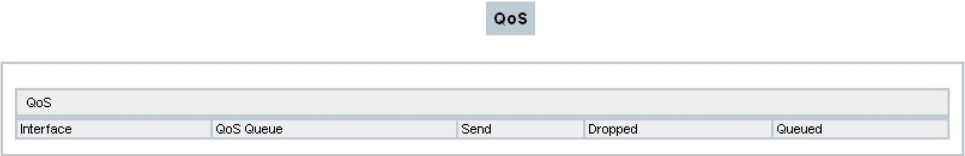


Fig. 219: **Monitoring->QoS->QoS**

Values in the QoS list

Field	Description
Interface	Shows the interface for which QoS has been configured.
QoS Queue	Shows the QoS queue, which has been configured for this interface.
Send	Shows the number of sent packets with the corresponding packet class.
Dropped	Shows the number of rejected packets with the corresponding packet class in case of overloading.
Queued	Shows the number of waiting packets with the corresponding packet class in case of overloading.

24.8 OSPF

In the **Monitoring->OSPF** menu information on OSPF is monitored . The OSPF monitor is arranged horizontally in three sections and shows information about OSPF interfaces, the detected neighbor and the LinkStateDatabase entries.

24.8.1 Status

In the **Monitoring->OSPF->Status** menu, a list of all interfaces configured for OSPF is displayed.

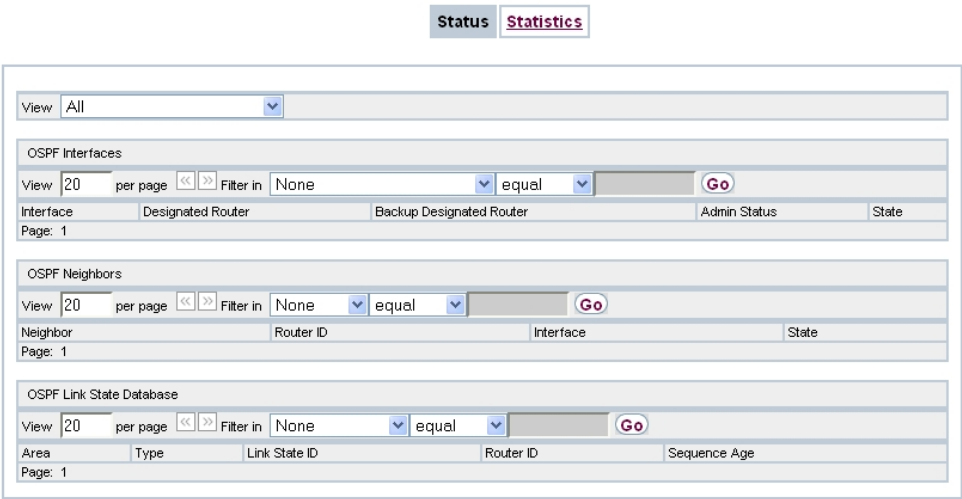


Fig. 220: Monitoring->OSPF->Status

Values in the Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: <i>All</i> , <i>OSPF Interfaces</i> , <i>OSPF Neighbors</i> and <i>OSPF Link State Database</i>

In the **OSPF Interfaces** area all enabled OSPF interfaces are listed:

Values in the OSPF Interfaces list

Field	Description
Interface	Shows the interface for which OSPF has been configured.
Designated Router	Shows the IP address of the designated router. The designated router generates network links and distributes these to all gateways within the BMA network (BMA = Broadcast Multi Access Network, e.g. Ethernet, FDDI, Tokenring). A designated router is not shown for non-BMA networks, e.g. X.25, Frame Relay, ATM.
Backup Designated Router	Shows the IP address of the backup designated router.
Admin Status	Shows the OSPF Admin Status (<i>active</i> or <i>passive</i>) of the interface.

Field	Description
State	<p>The OSPF status of the interface displayed here can take on the following values:</p> <ul style="list-style-type: none">• <i>Down</i>: OSPF is not running on this interface.• <i>Waiting</i>: The initial phase of the OSPF, in which the DR and BDR are determined.• <i>Point-to-point</i>: The interface is a point-to-point interface. DR or BDR are not shown.• <i>Designated Router</i>: The gateway is the designated router within the BMA network.• <i>Designated Router Backup</i>: The gateway is the backup designated router within the BMA network.• <i>Other Designated Router</i>: Another gateway is designated router or backup designated router within the BMA network.

The **Neighbor** section lists the neighbor gateways that have been identified via the HELLO protocol.

Values in the OSPF Neighbors list

Field	Description
Neighbor	Shows the IP address of the neighbor gateway.
Router ID	Shows the system-wide router ID of the neighbor gateway.
Interface	Indicates the interface over which the neighbor gateway was identified.
State	<p>The OSPF status with this neighbor gateway can have the following values:</p> <ul style="list-style-type: none">• <i>Down</i>: The connection to this OSPF neighbor is inactive.• <i>Init</i>: The initial phase. A HELLO packet is received from the neighbor.• <i>Bidirectional</i>: Bidirectional communication with the neighbor. The HELLO packets sent are accepted by the neighbor gateway (with correct parameters).• <i>Start Exchange</i>: The exchange of Database Description packets between the gateways has started.• <i>Exchange</i>: Active exchange of Database Description packets with the neighbor.

Field	Description
	<ul style="list-style-type: none">• <i>Loading</i>: The gateway now exchanges Link State Advertisements with the neighbor.• <i>Complete</i>: The Link State Databases of the gateway and its neighbor are now synchronized.

The headers of all Link State Advertisements (LSA) are listed in the section for the Link State Database.

Values in the OSPF Link State Database list

Field	Description
Area	Indicates the area database to which the LSA is assigned.
Type	Indicates the LSA type. There are five LSA types: Router Link, Network Link, Summary Link, Summary ASBR, and AS External.
Link State ID	The Link State ID of the LSA. The meaning of the Link State ID depends on the type of advertisement.
Router ID	Identifies the gateway that has generated this LSA.
Sequence Age	The age of the LSA (in seconds)

24.8.2 Statistics

In the **Monitoring->OSPF->Statistics** menu, current values and activities are displayed.

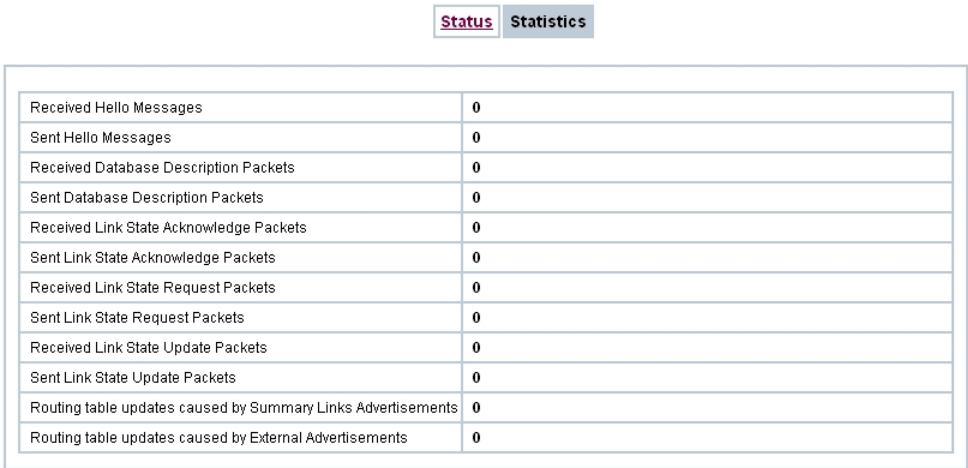


Fig. 221: Monitoring->OSPF->Statistics

Values in the Statistics list

Field	Description
Received Hello Messages	Displays the number of Hello packets received.
Sent Hello Messages	Displays the number of Hello packets sent.
Received Database Description Packets	Displays the number of received databank entries.
Sent Database Description Packets	Displays the number of sent databank entries.
Received Link State Acknowledge Packets	Displays the number of Link State Acknowledge packets received.
Sent Link State Acknowledge Packets	Displays the number of Link State Acknowledge packets sent.
Received Link State Request Packets	Displays the number of Link State Request packets received.
Sent Link State Request Packets	Displays the number of Link State Request packets sent.
Received Link State Update Packets	Displays the number of Link State Update packets received.
Sent Link State Update Packets	Displays the number of Link State Update packets sent.
Routing table updates caused by Summary Links Advertisements	Displays the number of incremental routing table updates performed when new Summary Link Advertisements have been received.
Routing table updates caused by External Advertisements	Displays the number of incremental routing table updates performed when new external Advertisements have been received.

24.9 PIM

24.9.1 Global Status

The status of all configured PIM components is displayed in the **Monitoring->PIM->Global Status** menu.

Global Status

Not Interface-Specific Status

Interface-Specific States

View

All

PIM Interfaces

View

20

per page

<<

>>

Filter in

None

<

equal

>

Go

Interface

IP Address

Designated Router

Page: 1

PIM Neighbors

View

20

per page

<<

>>

Filter in

None

<

equal

>

Go

Interface

Generation ID

IP Address

Uptime

Expiry Timer

Page: 1

Multicast Group / RP Mappings

View

20

per page

<<

>>

Filter in

None

<

equal

>

Go

Multicast Group Address

Multicast Group Prefix Length

Rendevous Point IP Address

Page: 1

Fig. 222: Monitoring->PIM->Global Status

Values in the Global Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: <i>All</i> , <i>PIM Interfaces</i> , <i>PIM Neighbors</i> and <i>Multicast Group / RP Mappings</i>

Values in the PIM Interfaces list

Field	Description
Interface	Displays the name of the PIM interface.
IP Address	Displays the primary IP address of the PIM interface.
Designated Router	Displays the primary IP address of the designated router on this PIM interface.

Values in the PIM Neighbors list

Field	Description
Interface	Displays the interface via which the PIM Neighbor is reached.
Generation ID	Displays the ID of the neighbor gateway.
IP Address	Displays the primary IP address of the PIM Neighbor.
Uptime	Indicates how long the last PIM Neighbor is a neighbor of the local router.

Field	Description
Expiry Timer	Indicates when the PIM Neighbor is no longer entered as neighbor. If the value 0 is displayed, the PIM Neighbor always remains entered as neighbor.

Values in the Multicast Group / RP Mappings list

Field	Description
Multicast Group Address	Displays the multicast group address.
Multicast Group Prefix Length	Displays the related network mask.
Rendezvous Point IP Address	Displays the IP address of the Rendezvous point.

24.9.2 Not Interface-Specific Status

The menu **Monitoring->PIM->Not Interface-Specific Status** includes status information for all PIM interfaces.

Global Status

Not Interface-Specific Status

Interface-Specific States

View All

(*,*_RP) States

View 20 per page<<>>Filter in NoneequalGo

Rendezvous Point IP AddressUpstream Join StateUpstream Neighbor IP AddressUptimeUpstream Join Timer

Page: 1

(*_G) States

View 20 per page<<>>Filter in NoneequalGo

Multicast Group AddressUpstream Neighbor IP AddressReverse-Path-Forwarding (RPF)Upstream Join StateUptimeUpstream Join Timer

Page: 1

(S,G) States

View 20 per page<<>>Filter in NoneequalGo

Multicast Group AddressSource IP AddressUpstream Neighbor IP AddressUpstream Join StateUptimeUpstream Join TimerShortest Path Tree

Page: 1

(S,G,RPT) States

View 20 per page<<>>Filter in NoneequalGo

Multicast Group AddressSource IP AddressReverse-Path-Forwarding (RPF)UptimeUpstream Override Timer

Page: 1

Fig. 223: Monitoring->PIM->Not Interface-Specific Status

Values in the Not Interface-Specific Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: <i>All, (*,*,RP) States, (*,G) States, (S,G) States</i> and <i>(S,G,RPT) States</i>

Values in the (*,*,RP) States list

Field	Description
Rendezvous Point IP Address	Displays the IP address of the Rendezvous Point (RP) for the group.
Upstream Join State	The Upstream (*,*,RP) Join/Prune Status indicates the status of the Upstream (*,*,RP) State Machine in the PIM-SM Specification.
Upstream Neighbor IP Address	Displays the primary IP address of the Upstream Neighbors, or unknown (0) if the Upstream Neighbor IP address is not known, or if it is not a PIM Neighbor.
Uptime	Indicates the timespan of the RP's existence.
Upstream Join Timer	Join/Prune Timer is used to periodically send Join(*,*,RP) messages, and to correct Prune(*,*,RP) messages from peers on an Upstream LAN interface.

Values in the (*,G) States list

Field	Description
Multicast Group Address	Displays the multicast group address.
Upstream Neighbor IP Address	Displays the primary IP address of the Neighbor on pimStarGRPFIIndex, to which the local router periodically (*,G) sends Join messages. The InetAddressType is defined through the pimStarGUpstreamNeighborType. In the PIM-SM specification, this address is named RPF'(*,G).
Reverse-Path-Forwarding (RPF)	Indicates the address type of the RPF Next Hop to the RP, or unknown(0), if the Next Hop is not known.
Upstream Join State	Indicates whether the local router should join the group's RP Tree. This corresponds to the status of the Upstream (*,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Join Timer	Indicates the remaining time until the local router sends out the

Field	Description
	next periodic (*,G) Join message on pimStarGRPFIflIndex. In the PIM-SM specification, this address is named (*,G) Upstream Join Timer. If the timer is deactivated, it has the value 0.

Values in the (S,G) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimSGAddressType object.
Source IP Address	Displays the source IP address. InetAddressType is defined in the pimSGAddressType object.
Upstream Neighbor IP Address	Displays the primary IP address of the Neighbor on pimSGRPFflIndex, to which the router periodically (S,G) sends Join messages. The value is 0, if the RPF Next Hop is unknown or is no PM Neighbor. InetAddressType is defined in the pimSGAddressType object. In the PIM-SM specification, this address is named RPF'(S,G).
Upstream Join State	Indicates whether the local router should join the Shortest-Path-Tree for the source and the group represented by this entry. This corresponds to the status of the Upstream (S,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Join Timer	Indicates the remaining time until the local router sends out the next periodic (S,G) Join message on pimSGRPFflIndex. In the PIM-SM specification, this timer is named (S,G) Upstream Join Timer. If the timer is deactivated, it has the value 0.
Shortest Path Tree	Indicates whether the Shortest Path Tree Bit is set, i.e. whether forwarding via the Shortest Path Tree should take place.

Values in the (S,G,RPT) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimStarGAddressType object.
Source IP Address	Displays the source IP address. InetAddressType is defined in the pimStarGAddressType object.
Reverse-Path-Forwarding (RPF)	Indicates the address type of the RPF Next Hop to the RP, or unknown(0), if the RPF Next Hop is not known.
Uptime	Indicates the timespan since the entry was generated by the local router.

Field	Description
Upstream Override Timer	Indicates the remaining time until the local router sends out the next Triggered (S,G, rpt) Join message on pimSGRPFIIndex. In the PIM-SM specification, this timer is named (S,G, rpt) Upstream Override Join Timer. If the timer is deactivated, it has the value 0.

24.9.3 Interface-Specific States

The menu **Monitoring->PIM->Interface-Specific States** includes interface-specific status information.

Global Status

Not Interface-Specific Status

Interface-Specific States

View -All-

(*,G,I) States

View 20 per page

Filter in None

equal

Go

Multicast Group Address

Interface

Join/Prune State

Uptime

Expiry Timer

Assert State

Assert Winner IP Address

Page: 1

(S,G,I) States

View 20 per page

Filter in None

equal

Go

Multicast Group Address

Source IP Address

Interface

Join/Prune State

Uptime

Expiry Timer

Assert State

Assert Winner IP Address

Page: 1

(S,G,Rpt,I) States

View 20 per page

Filter in None

equal

Go

Multicast Group Address

Source IP Address

Interface

Uptime

Join/Prune State

Expiry Timer

Page: 1

Fig. 224: Monitoring->PIM->Interface-Specific States

Values in the Interface-Specific States list

Field	Description
View	Select the desired view from the dropdown menu. Are available: <i>All</i> , <i>(*,G,I) States</i> , <i>(S,G,I) States</i> and <i>(S,G,RPT) States</i>

Values in the (*,G,I) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimStarGAddressType object.
Interface	Displays the name of the interface.

Field	Description
Join/Prune State	Indicates the status that results from the (*,G) Join/Prune messages received on this interface. This corresponds to the status of the Downstream Per-Interface (*,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Expiry Timer	Displays the remaining time until the (*,G) Join State becomes invalid for this interface. In the PIM-SM specification, this address is named (*,G) Join Expiry Timer. If the timer is deactivated, it has the value 0. The value 'FFFFFFFF'h stands for infinite.
Assert State	Displays the (*,G) Assert State for this interface. This corresponds to the status of the Per-Interface (*,G) Assert State Machine in the PIM-SM specification. If pimStarGPimMode is 'bidir', this object must 'noInfo' be.
Assert Winner IP Address	Indicates the address of Assert Winner, if pimStarGIAAssertState runs 'iAmAssertLoser'. InetAddressType is defined through the object pimStarGIAAssertWinnerAddressType.

Values in the (S,G) States list

Field	Description
Multicast Group Address	Displays the multicast IP address. InetAddressType is defined through the object pimSGAddressType.
Source IP Address	Displays the source IP address. InetAddressType is defined through the object pimSGAddressType.
Interface	Displays the name of the interface.
Join/Prune State	Indicates the status that results from the (S,G) Join/Prune messages received on this interface. This corresponds to the status of the Downstream Per-Interface (S,G) State Machine in the PIM-SM and PIM-DM.
Uptime	Indicates the time remaining before the local router reacts to an (S,G) Prune message received on this interface. The router waits this period to check whether another downstream router corrects the Prune message. In the PIM-SM specification, this timer is named (S,G) Prune-Pending Timer. If the timer is deactivated, it has the value 0.
Expiry Timer	Displays the remaining time until the (S,G) Join State becomes invalid for this interface. In the PIM-SM specification, this timer is named (S,G) Join Expiry Timer . If the timer is deactivated, it

Field	Description
	has the value 0. The value 'FFFFFFFF'h stands for infinite. In the PIM-DM specification, this timer is named (S,G) Prune Timer.
Assert State	Displays the (S,G) Assert State for this interface. This corresponds to the status of the Per-Interface (S,G) Assert State Machine in der PIM-SM Specification See "I-D.ietf-pim-sm-v2-new section 4.6.1"
Assert Winner IP Address	Indicates the address of Assert Winner, if pimStarGIAAssertState runs 'iAmAssertLoser. InetAddressType is defined through the object pimSGIAAssertWinnerAddressType.

Values in the (S,G,RPT) States list

Field	Description
Multicast Group Address	Displays the multicast IP address. InetAddressType is defined through the object pimSGAddressType.
Source IP Address	Displays the source IP address. InetAddressType is defined through the object pimStarGAddressType.
Interface	Displays the name of the interface.
Uptime	Indicates the timespan since the entry was generated by the local router.
Join/Prune State	Indicates whether the local router should sever the source of the RP tree. This corresponds in the PIM-SM specification to the status of the Upstream (S,G,rpt) State Machine for Triggered Messages.
Expiry Timer	Displays the remaining time until the (S,G, rpt) Prune State becomes invalid for this interface. In the PIM-SM specification, this timer is named (S,G, rpt) Prune Expiry Timer. If the timer is deactivated, it has the value 0. The value 'FFFFFFFF'h stands for infinite. In the PIM-DM specification, this timer is named (S,G) Prune Timer.

Glossary

2G	See GSM.
3DES	See DES.
3G	See UMTS.
4G	See LTE.
802.11	The 802.11 norm describes wireless LAN (WLAN). There are a variety of amendments: 802.11a: Gross data transfer rates: 54 Mbit/s, frequency band: 5 GHz, 802.11b/g: Gross data transfer rates: 11 Mbit/s, frequency band: 2.4 GHz, 802.11g: Gross data transfer rates: 54 Mbit/s, frequency band: 2.4 GHz, 802.11n: Gross data transfer rates: 600 Mbit/s, frequency band: 2.4 GHz (optional: 5 GHz)
Access client	Client mode is an operating mode of a wireless access point (AP) in which the latter behaves like a wireless adapter vis-a-vis the higher level AP. With an AP run in client mode, individual computers or entire sub-networks can be connected to higher level networks.
Access point	An access point (AP) is a device for wirelessly connecting clients (computers). The AP thus serves to create a wireless network (WLAN) and connect that WLAN to a wired Ethernet network (bridging).
Accounting	Accounting refers to the recording of connection data, e.g. date, time, connection duration, charging information and number of data packets transferred.
Activity monitor	The activity monitor is used to oversee the status of physical and virtual device interfaces.
Ad-hoc network	In an ad-hoc network, individual clients connect to an independent wireless LAN via a wireless adapter. Ad-hoc networks work independently, with no access point on a peer-to-peer basis. The ad-hoc mode is also referred to as IBSS (Independent Basic Service Set) mode and is useful in very small networks, e. g. when linking two notebooks with no access point.
ADSL	Asymmetric digital subscriber line. See DSL.
AES	Advanced Encryption Standard (AES, Rijndael) is an encryption method (see Cipher). AES uses a fixed block length of 128 bits. The

	key length is 128, 192 or 256 bits. AES is a very fast and secure algorithm.
Aggressive mode	When an IPSec connection is being established, aggressive mode is used to implement a phase 1 exchange. Aggressive mode offers no identity protection for negotiating nodes, since they have to transmit their identity before they can establish a secure channel. See also Main mode.
AH	The authentication header (AH) is used with IPSec to ensure the authenticity and integrity of the packets transmitted and to authenticate the sender.
Annex A	Annex A is a DSL variant which occurs in connection with analogue telephone connections, e. g. in France.
Annex B	Annex B is a DSL variant which occurs in connection with ISDN, e. g. in Germany.
Annex J	Annex J is a DSL variant purely for data transmission, with no voice data (unbundled connection). Annex J is an extension of specification G.992. These DSL connections require no splitter and have a greater range and faster transmission speed.
Annex L	Annex L is an extension of Annex A. The range is increased at the expense of the data transmission rate.
Annex M	Annex M is an extension of Annex A. The upstream is increased at the expense of the downstream.
ANSI T1.413	ANSI T1.413 is an ADSL variant.
ARP	The Address Resolution Protocol (ARP) supplies the associated MAC addresses to IPv4 addresses. The information required is shared between the network nodes, stored in the device's cache, and deleted again after the ARP lifetime has expired. For IPv6 this functionality is provided by the Neighbor Discovery Protocol (NDP).
ATM	Asynchronous Transfer Mode (ATM) is a data transmission technology in which the data traffic is coded in small packets – called cells or slots – with a fixed length and is transmitted via asynchronous time multiplexing.
Authentication	Check on the user's identity.
Authorisation	Based on their identity (authentication), the user can access certain services and resources.

AUX	AUX is a signal input for external devices, e. g. analogue or GSM modems.
B channel	See Basic Rate Interface and Primary Rate Interface.
Back Route Verify	If a Back Route Verify is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface.
Backbone area	The core area of a network which connects all the sub-networks (areas) with one another is known as the backbone.
Basic Rate Interface	The Basic Rate Interface is a network connection to the ISDN. This type of connection is often abbreviated to BRI. A basic rate interface includes two basic channels (B channels) each with 64 kbps and one control and signalling channel (D channel) with 16 kbps. There are two operating modes for the Basic Rate Interface: Point-to-point ISDN and Point-to-multipoint The Primary Rate Interface (PRI) is used with larger installations.
Beacon	The central access point sends beacons to create a wireless LAN in infrastructure mode. These messages contain the network name (SSID), a list of the supported transmission rates and the type of encryption.
Bit	A binary digit (bit) is the smallest unit of data in computing technology. Signals are represented in the logical states "0" and "1".
Black / White List	Entries in the Black List are blocked, entries in the White List are allowed through. (Example: Any telephone number beginning with 01234 is blocked in the Black List. The number 01234987 can nonetheless be approved in the White List.)
Blowfish	Blowfish is an encryption method (see Cipher). Blowfish uses a fixed block length of 64 bits. The key length can be between 32 and 448 bits.
BootP	The Bootstrap Protocol (BootP) is used to automatically issue an IP address.
Bps	Bits per second. A unit of measure for the transmission rate.
BRI	See Basic Rate Interface
Bridge	A bridge is a network component for connecting the same types of network at Level 2 of the OSI model. Data packets are transmitted using MAC addresses. The use of bridges divides up the network

	and reduces the load.
Broadcast	In a broadcast, data packets are sent from one point to all the subscribers in a network, e. g. if the recipient is not yet known. Examples of this are the ARP and DHCP protocols. The communication is via broadcast addresses: MAC networks: FF:FF:FF:FF:FF:FF, IPv4 networks: 255.255.255.255, IPv6 networks: ff00::/8
BRRP	BRRP is an implementation of the Virtual Router Redundancy Protocol (VRRP). The aim of the method is to compensate for the failure of the default gateway. Multiple routers are combined to form one virtual router. If one of these routers falls over, the others are able to replace it.
CA	Certificate Authority. See Certificate.
Cache	The device temporarily stores data used in name resolution in the cache. See also ARP.
Called party number	The number of the party being phoned.
Calling party number	The number of the calling terminal.
CAPI	The Common ISDN Application Programming Interface (CAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also TAPI.
CAPWAP	Control And Provisioning of Wireless Access Points Protocol (CAPWAP) is used to have wireless access points (slaves) monitored by a WLAN controller (master). It uses UDP port 5246 for monitoring and 5247 to send data.
CAST	CAST is an encryption method (see Cipher). CAST uses a fixed block length of 64 bits. The key length can be between 40 and 128 bits. Alternative names are CAST-128 and CAST5.
Certificate	A certificate identifies a person, an institution, a device or an application. A public key certificate is a digital certificate and it creates a connection between the identity and a public key. Certificates with public keys are issued by a certification authority (CA). Certificates that can no longer be trusted may be revoked using certificate revocation lists (CRLs)
Channel	A wireless channel is a frequency band used for wireless LAN. Devices that send on adjacent channels disrupt one another.

Channel bundling	When channels are bundled, the B channels in an ISDN connection are combined to increase data throughput.
CHAP	The Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol for PPP connections. As well as the standard CHAP, Microsoft also has the variants MS-CHAPv1 and MS-CHAPv2. You dial into a network via PPP and you authenticate yourself with a username and password. The username and password are transmitted encrypted. See also PAP.
Cipher	A block cipher is an encryption algorithm. In this encryption method, a data block of a fixed size (normally 64 bit) is rewritten to a block of the same size using a so-called key. The longer the key, the more secure the algorithm.
Client	A client uses the services provided by a server. Clients are usually workstations.
Configuration	The configuration refers to all of a device's settings. It is stored internally, in MIB tables. This data can be backed up, loaded and deleted externally. The configuration is edited using the HTTP(S) user interface, an SNMP client or connected telephones.
CoS	The term Class of Service (CoS) means different things depending on the area in which it is applied. In telecommunications CoS refers to the permission class assigned to the user. The permission class defines the user's rights, e. g. exchange access right, features that can be used, access to applications, ... In network technology CoS refers to the classification of certain services as per IEEE 802.1p. CoS enables priorities to be set in a targeted way, while Quality of Service (QoS) is used to set up explicit bandwidth guarantees or restrictions. Data packets are classified using a DSCP (Differentiated Services Code Point) value.
CRC	Cyclic Redundancy Check (CRC) is a method of detecting errors in the data transmission.
CRL	See Certificate.
D channel	See Basic Rate Interface and Primary Rate Interface.
Daemon	A daemon refers to a program that runs in the background and provides certain services.
Data compression	Data compression is a method of reducing the data volume transmitted. See STAC and MPPC.

Datagram	A datagram is a self-contained data entity with user and control data. It generally stands for the terms data frame, data packet and data segment.
DCN	DCN stands for data communication network.
Dead Peer Detection	In IPSec, Dead Peer Detection is used to identify IKE peers that can no longer be accessed.
Default gateway	All the data traffic which is not intended for one's own network is sent to the default gateway (default router).
Default route	See Standard route
Default route	The default route is used when no other suitable route is available.
Default router	See Default gateway.
Deffie-Hellman	Diffie-Hellman is a public key algorithm for negotiating and establishing keys. Because data is neither encrypted nor signed, the method is only secure if the connecting partners authenticate themselves using other mechanisms such as RSA and DSA.
Denial-Of-Service Attack	In a Denial-Of-Service Attack (DoS), a network component is flooded with queries so that it becomes totally overloaded. As a result, the system or a particular service can no longer function.
DES	The Data Encryption Standard (DES) is an encryption method (see Cipher). DES uses a fixed block length of 64 bits. The key length is 56 bits. Triple DES or 3DES is based on using DES three times (three different, independent keys).
DHCP	The Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be assigned dynamically. A DHCP server allocates each client in a network an IP address from a defined address pool. The clients need to be configured accordingly.
Dialup connection	When required, a dialup connection is established by dialling a phone number, in contrast to a fixed connection (see Leased line) which is permanently enabled.
DIME	Desktop Internetworking Management Environment (DIME) is used to configure and monitor gateways.
Direct dial exception	See Point-to-point ISDN access and Direct dial-in (VoIP).
Direct dial-in (VoIP)	Direct dial-in is a VoIP connection that is also known as point-

to-point. It is used to connect a PBX. A main phone number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Main number 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, ...)

Direct dialling range	See number block in Point-to-point ISDN access and Direct dial-in (VoIP)
DNS	The Domain Name System (DNS) is used to convert the domain name (e. g. www.example.org) to an IP address (name resolution).
Domain	A domain is a contiguous sub-set of the DNS (e. g. example.org).
Downstream	The gateway receives the data from a higher-level network and forwards it to its connected network.
DSA	The Digital Signature Algorithm (DSA) is used to create digital signatures and encrypt data packets. Signatures can be used to verify changes made to the information in the data packet. DSA is used for public-key cryptography (IPSec). See also RSA. Key generation is quicker with DSA than with RSA, but key processing is slower.
DSCP	Data packets can be marked with a Differentiated Services Code-point (DSCP). DSCP values classify data packets in such a way that important packets can be routed through the network more quickly. See also QoS.
DSL modem	See Modem.
DSS1	Digital Subscriber Signalling System No. 1 (DSS1) is a signalling protocol for the D channel in the ISDN. It is also known as Euro ISDN.
DTIM	A Delivery Traffic Indication Message informs the clients that multicast or broadcast data is available at the access point.
Dynamic IP address	In contrast to a static IP address, a dynamic IP address is assigned temporarily by DHCP. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.
DynDNS	A DynDNS provider can be used to link a domain name with a dynamically changing IP address.
Encapsulation	Encapsulation of data packets is a particular protocol to transmit the data packets in a network. See also VPN.

Encryption	Refers to the encryption of data, e.g. using MPPE.
ESP	Encapsulating Security Payload (ESP) is a protocol for IPSec. It uses protocol number 50 and supports data encryption and authentication.
Ethernet	Ethernet is a specification for cable data networks. Ethernet works on the first and second layer of the OSI model.
Euro ISDN	Standard ISDN in Europe, based on the DSS1 signalling protocol.
Eurofile transfer	Eurofile transfer (EFT) is a protocol for sharing files over ISDN.
Extension number	See Point-to-point ISDN access and Direct dial-in (VoIP).
Filter	A filter comprises a number of criteria (e.g. protocol, port number, source and destination address). If these criteria match a data packet, the data packet can be subjected to a particular action (forward, reject, ...). This creates a filter rule.
Filter rule	A rule that defines which data packets should or should not be transmitted by the gateway.
Firmware	The firmware (system software) is programming code that is permanently embedded in the device. It provides the device's functions.
Fragmentation	If the overall length of the data packet is greater than the Maximum Transmission Unit (MTU) of the network interface, the data packet has to be broken down into multiple physical data blocks using IP fragmentation. The reverse process is known as reassembly.
Frame	A data frame is an information unit (Protocol Data Unit) in the data link layer in the OSI model.
Frame relay	Frame relay is a data transmission technology and upgrade of X.25 (smaller packets, less error checking). Frame relay is primarily used for GSM networks.
FTP	The File Transfer Protocol (FTP) regulates data transmission in IP networks. It regulates the exchange between FTP server and client.
Full-duplex	With full-duplex, data can be sent and received simultaneously over a line.
G.991.1	Data transmission recommendation for HDSL.
G.991.2	Data transmission recommendation for SHDSL.

G.992.1	Data transmission recommendation for ADSL. There are two country-specific versions: G.992.1 Annex A and G.992.1 Annex B. Data transfer rates: 12 Mbit/s (downstream), 1.3 Mbit/s (upstream)
G.992.2	Data transmission recommendation for ADSL (G.LITE / ADSL-Lite). There are two versions: G.992.2 Annex A and G.992.2 Annex B. Data transfer rates: 12 Mbit/s (downstream), 1.3 Mbit/s (upstream)
G.992.3	Data transmission recommendation for xDSL2. There are three variants: G.992.3 Annex A/B (G.DMT to ADSL2) with data transmission rates of 12 Mbit/s in the downstream and 1.0 Mbit/s in the upstream, G.992.3 Annex L (RE-ADSL2) with data transmission rates of 5 Mbit/s in the downstream and 0.8 Mbit/s in the upstream and G.992.3 Annex M (ADSL2) with data transmission rates of 12 Mbit/s in the downstream and 2.5 Mbit/s in the upstream.
G.992.4	Data transmission recommendation for ADSL2 with Annex A/B. Data transmission rates: 12 Mbit/s (downstream), 1.0 Mbit/s (upstream)
G.992.5	Data transmission recommendation for xDSL2+. There are three variants: G.992.5 Annex A/B (ADSL2+) with data transmission rates of 25 Mbit/s in the downstream and 1.0 Mbit/s in the upstream, G.992.5 Annex L (RE-ADSL2+) with data transmission rates of 25 Mbit/s in the downstream and 1.0 Mbit/s in the upstream and G.992.5 Annex M (ADSL2+) with data transmission rates of 25 Mbit/s in the downstream and 3.5 Mbit/s in the upstream.
G.993.1	Data transmission recommendation for VDSL. Data transmission rates: 52 Mbit/s (downstream), 16 Mbit/s (upstream)
G.993.2	Data transmission recommendation for VDSL2. Data transmission rates: 200 Mbit/s (downstream), 200 Mbit/s (upstream)
G.DMT	See F.992.1.
G.Lite	See F.992.2.
G.SHDSL	See G.991.2.
Gateway	The gateway is a network component for connecting different types of network.
GPRS	General Packet Radio Service (GPRS) is the name for the packet-oriented service for transmitting data in GSM networks.
GRE	Generic Routing Encapsulation (GRE) is a network protocol for en-

	<p>capsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). GRE uses protocol number 47.</p>
GSM	<p>The Global System for Mobile Communications (GSM), also known as 2G, is a mobile communications standard. It achieves, along with GPRS, a specified max. data transmission rate of 171.2 kbit/s.</p>
Half-duplex	<p>With half-duplex, data can only be sent and received back-to-back over a line.</p>
Hash	<p>To ensure data integrity, the information needs to be protected from unauthorised manipulation while it is being transmitted. To ensure that this happens, every item of communication received has to match the information originally sent. Therefore erratic mathematical value functions (hash functions) are used to calculate checksums (hash values). These are encrypted and sent as a digital signature with the message. The recipient, in turn, checks the signature before opening the packet. If the signature and, thus, the content of the data packet has changed, the packet is discarded. The hash algorithms used most frequently are Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA1).</p>
HDSL	<p>High Data Rate Digital Subscriber Line. See DSL.</p>
Heartbeat	<p>A network's subscribers use heartbeats to signal that they are ready to receive.</p>
Hop	<p>Hop is the term for the connection from one network node to the next.</p>
Host	<p>A host is a computer system that provides its services to the network.</p>
Host name	<p>The domain name of a host. See DNS.</p>
Host route	<p>A host route is the name for the route to a single host.</p>
Hotspot	<p>A hotspot is a public internet access point via WLAN or wired Ethernet.</p>
HSDPA	<p>High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ or UMTS broadband) is a data transmission method in the UMTS mobile communications standard.</p>
HTTP	<p>The HyperText Transfer Protocol (HTTP) is a protocol for transmitting HTML pages (web pages) between server and client. By default</p>

it uses port 80.

HTTPS

The HyperText Transfer Protocol Secure (HTTPS) is a protocol which protects against eavesdropping when transmitting HTML pages (web pages) between server and client. HTTPS is schematically identical to HTTP. SSL / TLS is used for additional data encryption. The standard port for HTTPS connections is 443.

Hyperchannel

With a hyperchannel, multiple subscribers have access to the transmission medium. A subscriber can only transmit their data if no other subscriber is using the medium. A hyperchannel network is mainly used for short-range operation with top data rates.

ICMP

The Internet Control Message Protocol (ICMP) is used to exchange information and error messages over IPv4. The version ICMPv6 exists for IPv6.

IGMP

The Internet Group Management Protocol (IGMP) is used in IPv4 networks to organise multicast groups.

IKE

The Internet Key Exchange Protocol (IKE) is used for automatic key management with IPSec connections. The IKE process runs in two phases. During phase 1, the IKE subscribers authenticate themselves to one another and establish a secure channel. In phase 2, the two IPSec subscribers negotiate the SAs. There are two versions of the IKE mechanism.

Infrastructure network

In an infrastructure network the individual terminals (clients) form a wireless LAN via a central access point. This central access point may also be an agent in other networks.

IP

The Internet Protocol (IP) is a network protocol and it is the basis for the Internet. It works on the network layer of the OSI model. The TCP and UDP protocols are based on IP. There are two versions, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

IP address

IP addresses are used to navigate in an IP network, to unambiguously identify the source and destination. IPv4 addresses consist of 32 bits, IPv6 addresses of 128 bits. So, with IPv4 $2^{32} = 4.294.967.296$ addresses can be represented, with IPv6 $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$ addresses. Dotted decimal notation, e. g. 192.168.0.250, is used for IPv4. Hexadecimal notation, e. g. 2001:db8:85a3::8a2e:370:7344, is used for IPv6. See also netmask.

IPCP	The Internet Protocol Control Protocol (IPCP) is used, in a similar way to DHCP, to configure a host with an IP address, gateway and DNS server, when a PPP network connection is being used. With the extension Robust Header Compression over PPP, the header can be compressed for faster data transmission. Similarly, in IPv6 networks, the functionality is provided by the Internet Protocol version 6 Control Protocol (IPV6CP).
IPSec	IPSec (Internet Protocol Security) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). The protocol number for IPSec depends on the protocol used. The Authentication Header (AH) uses protocol number 51, while the Encapsulating Security Payload (ESP) uses number 50.
IPv6	See IP.
ISDN	Integrated Services Digital Network (ISDN) is a data transmission standard that includes telephony, fax and data transmission. There are two ISDN connection variants: Basic Rate Interface and Primary Rate Interface.
ISDN address	The ISDN address of an ISDN device comprises an ISDN number followed by other numbers that relate to the specific terminal.
ISDN login	The ISDN login is used to remotely configure the device via SNMP. To do so, it needs to have a configured ISDN or wireless connection.
ISDN number	The ISDN number is the network address of the ISDN interface.
ISDN router	See Router.
ISP	Internet Service Providers (ISPs) supply technical services for using the Internet.
ITU	The International Telecommunication Union (ITU) coordinates the setting up and operating of telecommunications networks and services.
Keepalive	Keepalive packets are used to check that the communication partner can be contacted.
Keepalive	Keepalive is a mechanism for maintaining the network connection and for checking that the communication partner can be reached. Specific packets are usually sent to the network for this purpose.

L2TP	The Layer 2 Tunneling Protocol (L2TP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). By default, L2TP uses protocol number 1701. The architecture in an L2TP network consists of an L2TP access concentrator (LAC) which may also be permanently integrated into the client, and the L2TP network server (LNS). The LAC establishes the connections to the LNS and manages them. The authorisation is regulated using a network access server (NAS), which can be implemented in the LAC or LNS. The LNS is responsible for routing and controlling the packets received from the LAC. The user data itself is exchanged unencrypted, while control messages for maintaining the accessibility of the tunnel end-points are transmitted securely.
LAC	See L2TP.
LAN	A Local Area Network (LAN) refers to a network that is geographically very limited and normally spans one building or a company head office.
Layer	A layer refers to a layer in the OSI model.
LCP	The Link Control Protocol (LCP) is used in PPP connections to automatically negotiate encapsulation, process limits for varying packet sizes, authenticate the connection partner, determine faulty links, identify connection faults and terminate the connection.
LDAP	The Lightweight Directory Access Protocol (LDAP) regulates the communication between a client and the directory server. LDAP is used for sharing and updating directories, e. g. a phone book.
Lease time	The lease time refers to the validity period of a dynamic IP address that a client has been given by a DHCP server.
Leased line	See Leased line
Leased line	A leased line is a permanent connection of two communication partners via telecommunications network.
LLC	The Link Layer Control (LLC) regulates the media allocation at MAC level.
LNS	See L2TP.
Load balancing	With load balancing, data is sent via different interfaces in order to increase the overall bandwidth available. In contrast to Multilink, load balancing also functions with accounts with different providers.

Loopback	In a loopback switch the sender and recipient are identical.
LTE	Long Term Evolution (LTE), also known as 4G, is a mobile communications standard with a standardised maximum data transmission rate of 300 Mbit/s.
MAC address	The Media Access Control address (MAC address) is the hardware address of the network adapter and is used to identify the device at the hardware level.
Main Mode	When establishing an IPSec connection, main mode is used to implement a phase 1 exchange by setting up a secure channel. See also Aggressive mode.
Man-in-the-Middle attack	In a Man-in-the-Middle attack, the attacker is physically or logically between the two communication partners and so is able to view, and even manipulate, the data traffic.
MD5	Message Digest Algorithm 5 (MD5) is a hash function that generates a 128 bit hash value (checksum). See also Hash.
Media gateway	A media gateway converts the network type of digital voice, audio or image information. For example, the signals from an ISDN network can be converted to an IP network.
Metric	The metric is a measure for the properties of the route. The fastest route has the lowest metric (costs). Simplified, this is connecting with the smallest number of node points (routers).
MIB	The Management Information Base (MIB) describes the data that can be queried or modified via a network management protocol (e. g. SNMP). The MIB is a database that describes all the devices and functions in the network.
MLP	The Multicast Listener Discovery (MLD) is used in IPv6 networks to organise multicast groups.
Modem	A modem is an electronic device that converts digital signals to frequency signals in order to distribute data in a wired or wireless network.
MPDU	The MAC Protocol Data Unit (MPDU) refers to a data packet, including management frames and fragmented MSDUs, exchanged wirelessly.
MPPC	Microsoft Point-to-Point Compression (MPPC) is a method of data compression.

MPPE	Microsoft Point-To-Point Encryption (MPPE) is used to encrypt data transmitted via PPP. It was developed by Microsoft and Cisco and specified as RFC 3078.
MS-CHAP	The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a method of authentication. MS-CHAPv1 is intended for authenticating DCN connections and is largely the same as the standard CHAP. MS-CHAPv2 is an authentication method for PPTP connections (VPN).
MSDU	A MAC Service Data Unit (MSDU) is a data packet that is exchanged at LLC level.
MSN	See Multiple subscriber number
MSS	The Maximum Segment Size (MSS) defines the maximum number of bytes that can be used as user data in a TCP segment. The MSS must be smaller than the Maximum Transmission Unit (MTU) to avoid fragmenting the IP packets.
MSS clamping	MSS clamping reduces the Maximum Segment Size (MSS) in order to connect networks with different Maximum Transmission Units (MTU).
MTU	The Maximum Transmission Unit (MTU) is the largest possible data unit that can be transmitted over a physical line.
Multicast	With a multicast, data packets are sent from one point to particular subscribers in a network. In IPv4 this is controlled via the address range 224.0.0.0 to 239.255.255.255 and the IGMP protocol, while in IPv6 it is controlled by ff00::/8 addresses and ICMPv6.
Multilink	With multilink, multiple interfaces (PPP, PPPoE, ...) are combined into a single virtual connection in order to increase the total bandwidth available.
Multiple subscriber number	Multiple subscriber numbers are the individual phone numbers in the ISDN point-to-multipoint connection.
NAPT	Network Address Port Translation (NAPT) is another term for PAT. See PAT.
NAT	Network Address Translation (NAT) is used to replace the source and destination IP addresses of a data packet with others. This enables different networks to be connected to one another. See also PAT.

NBNS	Like DNS, NetBIOS Name Service (NBSN) is used in centralised name resolution. See also WINS and DNS.
Netmask	With IPv4 in connection with the IP address, the netmask, also network mask and subnet mask, defines the network by dividing the IP address into network and device parts and thus determining which addresses need to be routed. Example of a netmask: 255.255.255.0. With IPv6 one refers to prefix length.
Network address	A network address is the address of the network as a whole. The network mask and prefix length divide the IP address into the network address and host address (device address). Example of a network address: 192.168.0.250/24
Network route	The network route refers to the route to a particular network.
Network termination	Network termination (NT) refers to a connection or operating type. A terminal is given access to a communication network at the NT interface (connection socket). The connector is called a TAE with an analogue connection, an NTBA with the basic ISDN connection, and NTPMGF with the ISDN Primary Rate Interface. In the NT operation, the gateway is connected to the PABX's external S0 and is an external exchange connection for it. See also TE.
NT	See Network termination.
NTP	The Network Time Protocol (NTP) is used to synchronise the time of day.
OAM	OAM is a service for monitoring ATM connections.
OSI model	The OSI model divides the flow of communication between the physical medium and the user level into layers. The requirements at each layer are met by relevant protocols.
OSPF	OSPF is a dynamic routing protocol which is usually used in larger network installations as an alternative to RIP.
PAP	The Password Authentication Protocol (PAP) is an authentication method for connections via PPP. Unlike with CHAP, the username and password are not sent encrypted.
PAT	Port and Address Translation (NAT) is used to replace the source and destination IP addresses and source and destination ports of a data packet with others. This enables different networks to be connected to one another. See also NAT.

Peer	A peer is the endpoint of a communication in the network.
Phase 1/2	See IKE.
PIM	The Protocol Independent Multicast (PIM) enables the dynamic routing of multicast packets on the Internet.
Ping	Ping is a diagnostic tool that can be used to check whether a particular host in an IP network can be contacted. A measurement is taken of the time interval between sending a data packet (ICMP(v6) echo request packet) and receiving a response packet sent back immediately. This enables the connection quality to be determined.
PKCS	The Public-Key Cryptography Standards (PKCS) are standards for public key cryptography. The PKCS are designed for binary and ASCII data and are compatible with the X.509 standard. The public standards are PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12 and #15. PKCS #10 describes the syntax for certification inquiries.
PKI	A public key infrastructure (PKI) is used to issue, distribute and verify digital certificates for an encryption procedure.
PMTU	The Path MTU (PMTU) describes the maximum packet size that can be transmitted along the entire connection route without needing to be fragmented.
Point-to-multipoint	Point-to-multipoint connection is an ISDN connection. It is used to connect ISDN terminals. Multiple subscriber numbers (MSNs) are provided. See also Point-to-point ISDN access
Point-to-multipoint	See Single phone number (VoIP).
Point-to-point	See Point-to-point ISDN access and Direct dial-in (VoIP).
Point-to-point connection number:	See Point-to-point ISDN access
Point-to-point ISDN access	Point-to-point ISDN access refers to an ISDN connection that is also called point-to-point. It is used to connect a PBX. A point-to-point number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Point-to-point connection number: 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, ...) See also Point-to-multipoint connection.
Pool	An address pool is a collection of IP addresses that can be assigned to the connected clients, e. g. by DHCP.

POP3	The Post Office Protocol Version 3 (POP3) is a transmission protocol which controls how a client accesses emails from an email server.
Port	The port number is used to decide the service (telnet, FTP, ...) to which an incoming data packet should be sent.
PPP	The Point-to-Point Protocol (PPP) is a standardised technology for setting up a direct connection between the network nodes via dial-up lines.
PPPoA	The Point-to-Point-over-ATM Protocol (PPPoA) enables PPP data packets to be transported directly over an ATM network.
PPPoE	The Point-to-Point-over-Ethernet Protocol (PPPoE) enables PPP data packets to be transported directly over an Ethernet network.
PPTP	The Point-to-Point Tunneling Protocol (PPTP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). PPTP uses protocol number 1723. The PPTP architecture is divided into two logical systems. The PPTP Access Concentrator (PAC) and the PPTP Network Server (PNS). The PAC is usually integrated into the Windows client. It establishes the connection to the PNS and manages it. The PNS is responsible for routing and controlling the packets received by the PNS.
Pre-shared key	A pre-shared key (PSK) is a key for an encryption procedure. The parties shared the key's value beforehand.
Prefix	See Network address
Prefix delegation	In IPv6 networks, prefix delegation is used to assign the network address (prefix) to the router.
Prefix length	See netmask.
PRI	See Primary Rate Interface.
Primary Rate Interface	The Primary Rate Interface is a network connection to the ISDN. This type of connection is often also called a PRI or S2Minterface. A Primary Rate Interface offers 30 user channels (B channels), each with 64 kbits/s, in Europe and 23 in the USA, one control channel (D channel) with 64 kbits/s and one synchronisation channel with 64 kbits/s in Europe and 8 64 kbits/s in the USA. See also Basic Rate Interface.

Proposal	When an IPSec connection is being established, the initiator of the connection makes proposals with relation to the authentication and encryption methods to be used.
Protocol	Protocols regulate the flow of a data communication on different levels of the OSI model. Protocols control addressing, coding, authentication, formatting, etc. Examples: Ethernet, IP, TCP, HTTP
Proxy	A proxy is a network component. The proxy is an agent. It routes a query from the source with its own IP address to the destination.
PVID	The Port VLAN Identifier (PVID) is the standard VLAN ID for the port concerned. A packet that reaches this port without a VLAN tag is assigned this ID.
Q-SIG	Q-Interface Signalling Protocol (Q-SIG) is an ISDN-based signalling protocol for linking PABX systems.
QoS	Quality of Service (QoS) describes the properties of the communication service. It is defined using bandwidth, delay, packet losses and jitter. To transmit time-critical data packets for VoIP or video streaming as quickly as possible, QoS is used to sort all the data packets into groups and forward them on in the network either more quickly or slowly, depending on their priority.
Queue	The data packets accumulate in a queue before they are sent.
RADIUS	Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol for authenticating, authorising and accounting for users with dial-in connections. The RADIUS server authenticates the client, e. g. by checking the username and password. See also TACACS+.
RE-ADSL2	See G.992.5.
Real Time Jitter Control	Real Time Jitter Control is used, where necessary, to reduce the size of data packets during a telephone conversation so that voice packets are not blocked.
Registrar	The SIP server (registrar) needs to be used in case the subscribers to a VoIP call are not using static IP addresses. The SIP server registers the clients' IP addresses and sends this data to the SIP proxy, which connects the calls. The SIP proxy and SIP registrar are usually identical.
Repeater	A repeater is a device that strengthens electric or optical signals and thus increases the range of the network.

Reset	This returns the device to its unconfigured state.
RFC	A Request For Comments (RFC) is a document that describes the standards and guidelines for the Internet.
Rijndael	See AES.
RIP	The Routing Information Protocol (RIP) is a routing protocol. It is restricted to small networks. See also OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) is a hash function that generates a 160 bit hash value (checksum). See also Hash.
RJ45	RJ45 refers to a jack or connector with a maximum of eight wires to the digital terminals' connection.
Roaming	With roaming, a client moves through a WLAN logging on and off at different access points in the same network.
Router	A router is a network component for connecting different types of network at the network layer of the OSI model. Data packets are transmitted using IP addresses. Routing tables are used to identify the best routes through the network. In order to keep the routing tables up to date, the routers exchange information via routing protocols (e.g. OSPF, RIP).
Router advertisement	Router advertisements are messages that the router sends to the network. They announce the presence of the router in the network. Router announcements are also used to issue prefixes, organise the autoconfiguration and specify the standard router.
Routing	Routing refers to the identifying of routes for sending messages.
RSA	The RSA algorithm (named after its inventors, Rivest, Shamir and Adleman) is used to create digital signatures and encrypt data packets. The signature can be used to verify changes made to the information in the data packet. RSA is used for public-key cryptography (IPSec). See also DSA. Key generation is slower with RSA than with DSA, but key processing is faster.
RTP	The Real-Time Transport Protocol (RTP) is used to transmit audio and video data (streams) via IP-based networks.
RTS threshold	Once the number of frames in the data packet exceeds the RTS threshold, a connection check (RTS/CTS handshake) is run before a data packet is sent.

RTSP	The Real-Time Streaming Protocol (RTSP) controls the transmission of audio and video data (streams) via IP-based networks. While the Real-Time Transport Protocol (RTP) is used to transmit user data, the main function of RTSP lies in controlling the data streams.
Rule chain	A rule chain contains a combination of different filter rules. A filter rule selects part of the data traffic based on particular features, e. g. the source IP address, and applies an action, e. g. block, on this part.
S2M interface	See Primary Rate Interface.
SA	So-called security associations (SA) receive information about the measures to secure the communication connection. One SA, at least, is a prerequisite for establishing a secure connection. An SA receives the subscriber's IP address, the authentication protocol used, the encryption algorithm used, the security parameter index (SPI), the selector and the period of validity.
SAD	All the parameters that are set while configuring IPSec are stored in the router in the form of databases. These are the Security Policy Database (SPD) and the Security Association Database (SAD). The SAD receives information about every security connection. That is, which encryption algorithms, keys, protocols, session numbers or periods of validity are to be used. For an outgoing connection, an SPD entry displays an SAD entry. In this way, the SPD can specify which SA is to be used for a particular packet. With an incoming connection, the SAD is addressed in order to specify how the packet is to be processed.
SCEP	The Simple Certificate Enrollment Protocol (SCEP) is used to manage digital certificates.
Scheduling	Scheduling refers to the planning of tasks. Particular actions (e. g. deactivating an interface) are triggered by events (e. g. time or changing a MIB variable).
Serial interface	The serial interface is used to exchange data between computers and peripheral devices. It can be used to configure the device or to transmit data via an IP infrastructure (Serial over IP).
Server	A server offers services used by clients.
SFP	Small Form-factor Pluggable (SFP) is a plug-in connector that was developed for extremely fast Ethernet.

SHA1	Secure Hash Algorithm version 1 (SHA1) is a hash function that generates a 160 bit hash value (checksum). See also Hash.
SHDSL	Symmetrical High-bit-rate Digital Subscriber Line. See DSL.
Shell	The shell is an input interface (e. g. command line or graphic user interface) between computer and user.
Short hold	The short hold is the defined amount of time after which a network connection is automatically cleared if no more data is transmitted.
SIF	With a Stateful Inspection Firewall (SIF), the routing of a data packet is not determined only by source and destination addresses but also using dynamic packet filtering based on the connection status.
Single phone number (VoIP)	Single phone number access is a VoIP connection that is also known as a point-to-multipoint connection. It is used to connect VoIP terminals. Multiple subscriber numbers (MSNs) are provided. See also Direct dial-in (VoIP)
SIP	The Session Initiation Protocol is a network protocol for setting up a communication session between two or more subscribers. The protocol is used for IP telephony (VoIP).
SIP provider	A SIP provider does the switching between a SIP connection and other analogue, ISDN and VoIP connections.
SNMP	The Simple Network Management Protocol (SNMP) is used to configure, control and monitor different network components (e. g. routers, servers, etc.) from a single, central system. The network component settings that can be changed are stored in a database – the Management Information Base (MIB). SNMP uses UDP. The network component receives requests to port 161 while the managing system receives confirmation messages (TRAPs) at port 162.
Spatial streams	Spatial streams are data streams that are sent out at the same time on the same frequency in the wireless LAN. The transmission rate is multiplied as a result.
SPD	All the parameters that are set while configuring IPSec are stored in the router in the form of databases. These are the Security Policy Database (SPD) and the Security Association Database (SAD). The Security Policy Database lists the forms of data traffic that are to be secured. Factors such as the source and destination address of the data packet are used to do this.
SRTP	The Secure Real-Time Transport Protocol (SRTP) is the variant of

	the Real-Time Transport Protocol (RTP) that is encrypted using AES.
SSH	Secure Shell (SSH) is a network protocol that can be used to establish an encrypted connection to a device's shell.
SSID	The Service Set Identifier (SSID) defines a wireless network that is based on IEEE 802.11. The SSID is the network name of the wireless LAN. All the access points and clients that belong to the same network use the same SSID. The SSID string can be up to 32 characters long and is placed, unencrypted, in front of all packets. A client uses SSID ANY to contact all the accessible access points. The user is then shown all the available WLANs and he can select the appropriate network. If an access point is used for different networks, each wireless network is given a separate MSSID (Multi Service Set Identifier).
SSL	Secure Sockets Layer (SSL) is a protocol for data encryption. Since version 3.1, the new term Transport Layer Security (TLS) has been used. SSL is mainly used for HTTPS to encrypt the data transmission between web server and web browser.
STAC	STAC is used to reduce the data volume transmitted (data compression).
Static IP Address	In contrast to a dynamic IP address, the static IP address is assigned permanently by the user. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.
STUN Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). A STUN server enables VoIP devices behind an active NAT to access the network.
Sub-addressing	As well as the ISDN telephone number, a sub-address can also be sent when establishing the connection. This sub-address can transmit any additional information. It can be used, e. g., to systematically address multiple ISDN terminals that can be reached under one telephone number, or to open particular programs on a PC.
Subnet	A sub-network in an IP network is known as a subnet. A subnet is defined like a normal network, via an IP address and (sub-)netmask (IPv4) and prefix length (IPv6). Example: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 possible IP addresses) is a subnet of 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 pos-

sible IP addresses).

Switch

A switch is a network component that connects individual network segments to one another. On the one hand, a switch can be operated as a bridge to the data link layer in the OSI model. Unlike the bridge, however, a switch has more than one input and output. On the other hand, the switch can be operated as a gateway to the network layer in the OSI model. The device comparable to the switch in the physical layer is known as the hub.

SWYX

SwyxWare is a software-based communication solution for VoIP.

Syslog

The syslog protocol is used to transmit status messages in an IP network. In this way, different network components can be monitored from a single, central system. Syslog messages are sent as unencrypted text messages over the UDP port 514.

T.38

T.38 or Fax over IP (FoIP) refers to fax transmission via an IP network.

TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) is a client-server protocol for authenticating, authorising and accounting for users. The TACACS+ server authenticates the client by checking, e. g., the username and password. In contrast to the UDP-based RADIUS protocol, TACACS+ uses TCP on port 49 and transmits the entire communication encrypted.

TAPI

The Telephony Applications Programming Interface (TAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also CAPI.

TCP

The Transmission Control Protocol (TCP) is a connection-oriented protocol. It works on the transport layer of the OSI model. With a connection-oriented protocol, a logical connection is established before transmission and maintained. This enables data to be transmitted reliably. Nonetheless, control information is constantly being sent alongside the actual data packets. This causes the data volume sent to increase. See also UDP.

TCP-ACK packet

An ACK (acknowledgement) signal is used when transmitting data to confirm the receipt or the processing of data or commands. TCP uses ACK signals for communication.

TE

Terminal equipment (TE) refers to a connection or operating type. The TE connector is a terminal's connector. In TE operation, the gateway is connected to the PABX's internal S0 and thus constitutes

	an ISDN terminal. See also NT.
Telnet	Telecommunication Network (Telnet) is a network protocol. It enables communication with another, remote device in the network, e. g. PCs, routers, etc.
TFTP	The Trivial File Transfer Protocol (TFTP) regulates the transmission of files. Compared with FTP, there is no option to display data, issue permissions or authenticate users.
Tiger 192	Tiger 192 is a hash function that generates a 192 bit hash value (checksum). See also Hash.
Time slot	A time slot is a period of time which is permanently assigned within a transmission frame, and is usually equivalent to one transmission channel.
TLS	See SSL.
TOS	Type of Service (TOS) is a field in the header of IP data packets. It specifies the priority of the data packet. See also QoS.
Traceroute	Traceroute is used to determine which routers will be used to route data packets to the queried destination host.
Trigger	This refers to a trigger impulse.
Triple DES	See DES.
TTL	The Time to live (TTL) is the configured period of validity of a data packet. With the Internet Protocol (IP), TTL specifies how many hops a data packet may pass. The maximum value is 255 hops. The TTL is reduced by 1 with each hop. If a data packet has not yet reached its destination when its TTL expires, it is discarded.
Twofish	Twofish is an encryption method (see Cipher). Twofish uses a fixed block length of 128 bits. The key length is 128, 192 or 256 bits.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) is a DSL variant. It was developed as ANSI T1.413 and standardised as G.992.2. U-ADSL enables different communication technologies to be used in parallel, e. g. ISDN and POTS, and does not require a splitter.
UDP	The User Datagram Protocol (UDP) is a connectionless protocol. It works on the transport layer of the OSI model. With a connectionless protocol, no control is integrated for delivering the packet. The

	control must take place in the application layer. Conversely, UDP is faster than connection-oriented protocols.
ULA	Unique Local Addresses (ULA) are IPv6 addresses that are not routed. They can be used in private networks (e. g. a LAN). ULAs begin with the prefix fd.
UMTS	The Universal Mobile Telecommunications System (UMTS), also known as 3G, is a mobile communications standard with a specified max. data transmission rate of 384 kbit/s and 21 Mbit/s in association with HSPA+.
Unicast	With Unicast, data packets are transmitted from a sender to a single recipient.
UPnP	Universal Plug and Play (UPnP) is used to control devices (audio devices, routers, printers, etc.) from any manufacturer via an IP-based network.
Upstream	The gateway forwards the data from its own network.
URL	A Uniform Resource Locator (URL) identifies a file's storage location. Example: http://www.example.org/index.htm (Internet website)
V.110	V.110 describes a method of aligning bitstreams with 0.6, 1.2, 2.4, 2.8, 7.2, 9.6, 12, 14.4, 19.2 and 38.4 kbit/s with the ISDN bitstream of 64 kbit/s.
VDSL	Very High Speed Digital Subscriber Line. See DSL.
VID	See VLAN.
VLAN	A network can be divided up into one or more logical sub-networks—so-called Virtual Local Area Networks (VLAN) – by the network components no longer forwarding the data packet of a defined sub-network to other sub-networks. Each VLAN is assigned a unique number, This number is called a VLAN ID (VID) and assigned to the data packets in the VLAN tag.
VoIP	Voice over IP (VoIP), also known as IP telephony, refers to the transmitting of voice via an IP network. The telephone is connected and disconnected using signalling protocols, e. g. SIP.
VPN	A virtual private network (VPN) is used to transport private data packets through a public network. The data is separated from the publicly accessible data by being encapsulated in new protocols so that they can be routed to the intended recipient. In this context, one

	also refers to a tunnel that is established between the private networks of the two connected parties. VPN protocols are IPSec, PPTP, L2TP and GRE.
VSS	The Virtual Service Set (VSS) refers to a prefix for wireless LAN interfaces.
Walled garden	In the context of hotspots, a walled garden refers to the area of the website which is available to users free of charge and without logging in.
WAN	A Wide Area Network (WAN) refers to a network that is spread over a large geographic area. Global WAN networks provide access to the Internet.
WDS	The Wireless Distribution System (WDS) is used to establish a wireless connection between access points.
Web server	A web server provides HTML documents (web pages).
WEP	Wired Equivalent Privacy (WEP) is an encryption protocol for WLANs. The key length is 40 or 104 bits.
WINS	The Windows Internet Name Service (WINS) is a translation of the NetBIOS over TCP/IP network protocol by Microsoft. Like DNS, WINS is used for centralised name resolution. See also DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) refers to a local wireless network based on the 802.11 standard.
WMM	Wi-Fi Multimedia (WMM) prioritises the data packets from different applications, thus improving the transmission of voice, music and video data in WLAN networks. To do this, WMM provides quality-of-service features (QoS) for IEEE 802.11-based networks.
WPA	Wi-Fi-Protected Access (WPA) is an encryption protocol for WLANs. WPA uses dynamic keys that are based on the Temporal Key Integrity Protocol (TKIP).
WPA 2	Wi-Fi Protected Access (WPA) is an encryption protocol for WLANs. WPA 2 uses AES.
WPA Enterprise	With WPA 1 / 2, WPA Enterprise enables subscribers to be authenticated using the Extensible Authentication Protocol (EAP). After successful authentication, the server transfers a shared key to the client and the access point for data transfer in the WLAN.

WPA-PSK	With WPA 1 / 2, WPA-PSK enables subscribers to be authenticated using pre-shared keys. The access point and the client use the same string for the key calculation in the WLAN. This string needs to be configured by the users.
X.25	X.25 is a standardised series of protocols for wide area networks (WANs) via the telephone network.
X.31	The X.31 standard describes the connecting of ISDN and X.25 systems. It is a standard for connecting card terminals.
X.500	The X.500 standard describes the setting up of a directory service. See also LDAP.
X.509	The X.509 standard describes the generating of certificates for a public key infrastructure (PKI).
X.75	X.75 is a standardised series of protocols for ISDN networks with a transmission rate of 64 kbit/s.
XAuth	XAUTH (Extended Authentication) is used to add further authentication mechanisms to IKE. After a successful phase 1 authentication, the user can be separately identified again. The identifying is done using the username and password, PAP, CHAP or hardware-based systems.

Index

205

Custom DHCP Options 420
 Vendor Description 420
 ISDN Timeserver 62
 Modem Init Sequence 110
 Power Off Timeout 57
 System Admin Password 58

#

#1 #2, #3 104

A

Access Control 164 , 198
 Access Filter 252
 Access Level 96
 Access Type 129
 Access Filter 247
 Access Profiles 89
 Access Rules 245
 ACCESS_ACCEPT 79
 ACCESS_REJECT 79
 ACCESS_REQUEST 79
 ACCOUNTING_START 79
 ACCOUNTING_STOP 79
 Action 168 , 168 , 205 , 219 , 252 ,
 384 , 426 , 436 , 466 , 482 , 500 ,
 504
 Action if license not registered 424
 Action if server not reachable 424
 Action to be performed 448
 Actions 435
 Active Clients 199
 Active IPSec Tunnels 53
 Active Radio Profile 183
 Active Sessions (SIF, RTP, etc...) 53
 Actual Network 121 , 128
 Additional Traffic Filter 331
 Additional freely accessible Domain

Names 458

Additional Traffic Filter 322
 Address Mode 138
 Address Range 391
 Address Type 391
 Address List 391
 Address / Subnet 391
 Addresses 391
 Admin Status 230 , 269
 Admin Status 514
 Administration 144 , 170
 Administrative Status 325 , 405
 Administrative Access 72
 ADSL Logic 482
 Advertisement send interval 473
 Airtime fairness 151 , 188
 Alert Service 491
 Alert Service 494
 Alert Recipient 491
 Alert Settings 494
 Alert Service 491
 Alive Check 83 , 346 , 351
 Alive Check 501
 All Multicast Groups 280
 Allowed Addresses 164 , 198
 Allowed HotSpot Client 460
 Always on 291 , 297 , 301 , 306 , 364
 , 371
 Answer to client request 454
 AP MAC Address 168
 APN (Access Point Name) 121
 APN (Access Point Name) 110
 Apply QoS 384
 Area 516
 Area ID 267 , 269
 Areas 267
 ARP Lifetime 255
 ARP Processing 193
 As DHCP Server 404
 As IPCP Server 404
 Assert State 522 , 523
 Assert Winner IP Address 522 , 523
 Assigned Wireless Network (VSS)
 183

Assistants 51
 Attacked Access Point 203
 Authentication 294 , 299 , 303 , 308 ,
 367 , 374
 Authentication Key 269
 Authentication Method 127 , 325 ,
 341
 Authentication Type 81 , 86 , 269
 Authentication Method 501
 Authentication for PPP Dialin 89
 Autosave Mode 105 , 436
 AUX 109 , 305
 AUX Port Status 110

B

Back Route Verify 333
 Back Route Verify 215
 Backup Designated Router 514
 Bandwidth 149 , 186
 Based on Ethernet Interface 138
 Baudrate 116
 Beacon Period 164 , 189
 Black / White List 428
 Blacklist blocktime 198
 Blacklisted 428
 Block after connection failure for 294 ,
 299 , 303 , 308 , 367 , 374
 Block Time 87 , 346
 BOSS 482
 BOSS Version 53
 Bridge Links 169
 Bridge Link Name (ID) 169
 Bridges 511
 BRRP 468
 Burst size 242
 Burst Mode 188
 Byte Count 118
 Bytes 501

C

CA Certificate 101
 CA Certificates 346
 CA Name 436

Cache 409
 Cache Hitrate (%) 410
 Cache Hits 410
 Cache Size 402
 Call Number 311
 Callback 376
 Callback Mode 308
 CAPWAP Encryption 182
 Category 426
 Cell ID 128
 Certificate Request 100
 Certificate List 97
 Certificate Servers 108
 Certificate is CA Certificate 98
 Certificate Request Description 101 ,
 436
 Certificate Revocation List (CRL)
 Checking 98
 Certificates 97
 Channel 149 , 168 , 183
 Channel Plan 153 , 189
 Class ID 236 , 242
 Class map 236
 Clear Serial RX-Buffer 119
 Clear Serial TX-Buffer 119
 Client Link 165
 Client Management 200
 Client Band select 163 , 196
 Client Link Description 168
 Client MAC Address 510
 Code 393
 Command Mode 436
 Command Type 436
 Common Name 103
 Compare Condition 430
 Compare Value 430
 Compression 76 , 316 , 319 , 374
 Config Mode 328
 Configuration Encryption 482
 Configuration Access 89
 Configuration contains
 certificates/keys 436
 Configuration Interface 69
 Configured Speed / Mode 113

Confirm Admin Password 58
 Congestion Avoidance (RED) 244
 Connected 168
 Connection State 233 , 248 , 462
 Connection Type 364
 Connection Idle Timeout 291 , 297 ,
 301 , 306 , 364 , 371
 Consider 225
 Contact 55
 Control Mode 239 , 321
 Controlled Interfaces 320
 Controller Configuration 178
 Corrupt Frames Received 507
 COS Filter (802.1p/Layer 2) 233 , 248
 , 462
 Count 436
 Country 103
 CPU Usage 53
 Create area default route (only ABR)
 267
 Create NAT Policy 293 , 298 , 302 ,
 307 , 365 , 373
 CRLs 106
 CSV File Format 436
 CTS frames received in response to an
 RTS 507
 Current File Name in Flash 482
 Current Local Time 61
 Current Speed / Mode 113
 Custom 103
 Cyclic Background Scanning 189

D

D Channel Mode 337
 Data Bits 116
 Data Packets Sequence Numbers
 362
 Data Rate mbps 508 , 510
 Date 499
 Date and Time 59
 Day 426
 Default Route 293 , 298 , 302 , 307 ,
 315 , 318 , 328 , 365 , 373 , 380
 Default Idle Timeout 460

Default Route Distribution 263
 Default User Password 81
 Delete 203 , 214
 Delete complete IPSec configuration
 356
 Demand Circuit Options 269
 Description 91 , 98 , 108 , 132 , 182 ,
 186 , 211 , 218 , 230 , 233 , 236 ,
 242 , 248 , 252 , 291 , 297 , 301 ,
 306 , 315 , 318 , 325 , 331 , 341 ,
 349 , 354 , 361 , 364 , 371 , 380 ,
 390 , 391 , 392 , 393 , 396 , 405 ,
 422 , 430 , 436 , 462 , 466 , 500 ,
 501 , 504 , 505 , 507
 Description - Connection Information -
 Link 54
 Designated Router 514 , 518
 Designated Router Priority 282
 Destination 384
 Destination Interface 280
 Destination Port 211 , 331
 Destination Port/Range 219 , 230 ,
 233 , 248 , 462
 Destination File Name 482
 Destination IP Address 430 , 436 ,
 452
 Destination IP Address/Netmask 210
 , 219 , 230 , 233 , 248 , 331 , 462
 Destination IP Address 214
 Destination Port Range 393
 Details 500
 Device 128 , 182
 DH Group 341
 DHCP Hostname 140
 DHCP Options 419
 DHCP Server 178
 DHCP Configuration 417
 DHCP Broadcast Flag 140
 DHCP Client on Interface 255
 DHCP MAC Address 140
 DHCP Relay Settings 422
 DHCP Server 416
 Diagnostics 478
 Direction 236 , 261

- Distribution Mode 225
- Distribution Policy 225 , 226
- Distribution Ratio 227
- DNS 400
- DNS assignment via DHCP 255
- DNS Hostname 407
- DNS Negotiation 294 , 299 , 303 ,
308 , 368 , 375
- DNS Server 313 , 355 , 379 , 408 ,
417
- DNS Requests 410
- DNS Servers 404
- DNS Test 479
- Domain 408
- Domain Forwarding 407
- Domain at the HotSpot Server 458
- Domain Name 402
- Done 205
- Drop non-members 144
- Drop In 254
- Drop In Groups 254
- Drop untagged frames 144
- Dropped 503 , 513
- Dropping Algorithm 244
- DSA Key Status 75
- DSCP / TOS Value 211
- DSCP/TOS Filter (Layer 3) 233 , 248
, 462
- DTIM Period 164 , 189
- Duplicate received MSDUs 507
- Dynamic blacklisting 198
- Dynamic LS Update Compression
271
- Dynamic RADIUS Authentication 357
- DynDNS Provider 414
- DynDNS Update 412
- DynDNS Client 412

E

- E-mail 103
- EAP Preauthentication 161 , 194
- Enable authentication 473
- Enable update 413
- Enable BRRP 476

- Enable IPSec 356
- Enable VLAN 145
- Enabled 380
- Encrypt configuration 436
- Encrypted 503
- Encryption 87 , 367 , 374
- Encryption Method 239
- Encryption Algorithms 75
- Entries 311
- Entry active 81 , 86
- Error 205
- Errors 501 , 503
- Ethernet Interface 472
- Ethernet Ports 111
- Ethernet Interface Selection 113
- Event 491
- Event Type 430
- Event List 430 , 436
- Event List Condition 436
- Exclude from NAT (DMZ) 255
- Expiry Timer 518 , 522 , 523 , 524
- Export indirect static routes 269
- Extended Route 214
- External Filename 106 , 107
- External Reporting 486

F

- Facility 487
- Failed attempts per Time 198
- Fallback Number 121
- Fallback interface to get DNS server
402
- File Encoding 106 , 107
- File Name 436
- File Name in Flash 436
- Filename 482
- Filter 236
- Filter Rules 387
- Filter Rules 383
- Filter List 426
- Filtered Input Interface(s) 424
- Firewall 382
- Firewall Status 389
- Firmware Maintenance 204

First Timeserver 62
First seen 203
Fixed IP Address 127
Force certificate to be trusted 98
Forward 408
Forward to 408
Forwarded Requests 410
Forwarding 280
Fragmentation Threshold 153 , 189
Frame transmissions without ACK received 507
Frozen Parameters 231
Full Filtering 389

G

Garbage Collection Timer 264
Gateway 214 , 419
Gateway IP Address 210
General 274 , 424 , 454
Generate Private Key 101
Generate default route for the AS 271
Generation ID 518
GEO Zone Status 430
GEO Zones 131
Global Settings 271 , 402
Global Status 517
Global Settings 55
Google Maps 136
GPS 129
GPS Configuration 129
GPS Port Status 130
GRE 379
GRE Tunnels 380
GRE Window Adaption 377
GRE Window Size 377
Group Description 81 , 225 , 226 , 255
Group ID 448
Groups 390 , 392 , 395

H

Handshake 116
Hashing Algorithms 75

Hello Interval 283
Hello Intervall 362
Hello Hold Time 283
High Priority Class 236
History 429
Hold Down Timer 265
Home PLMN 128
Horizontal Dilution Of Precision (HDOP) 136
Host 408
Host for multiple locations 461
Host Name 413
Hosts 447
HotSpot Gateway 457
HotSpot Gateway 455 , 512
HTTP 72
HTTPS 72 , 411
HTTPS Server 411
HTTPS TCP Port 411

I

ICC ID 128
IGMP 275
IGMP Proxy 278
IGMP State Limit 276
IGMP State Limit 279
IGMP Status 279
Ignore Certificate Request Payloads 358
IKE (Phase-1) 503
IKE (Phase-1) SAs 501
Image already exists. 205
IMEI 128
Import external routes 267
Import summary routes 267
Include certificates and keys 482
Incoming ISDN Number 376
Incoming Phone Number 337
Incoming Service Type 121
Incoming Service Type 110
Index Variables 430 , 436
Inter-Byte Gap 118
Interface 70 , 71 , 73 , 144 , 178 , 209 , 214 , 215 , 218 , 227 , 239 , 253 ,

261 , 276 , 282 , 321 , 387 , 405 ,
 408 , 413 , 418 , 436 , 451 , 454 ,
 458 , 468 , 512 , 513 , 514 , 515 ,
 518 , 518 , 522 , 523 , 524
 Interface Action 451
 Interface Mode 138 , 405
 Interface Status 430
 Interface Traffic Condition 430
 Interface Description 69
 Interface Assignment 253 , 467
 Interface - Connection Information -
 Link 54
 Interface is UPnP controlled 454
 Interface Mode / Bridge Groups 66
 Interface Selection 255
 Interface-Specific States 522
 Interfaces 68 , 137 , 236 , 269 , 314 ,
 390 , 450 , 453 , 489 , 503
 Internal Log 499
 Internal Time Server 62
 Internet + Dialup 288
 Internet Key Exchange 325
 Interval 430 , 436 , 448 , 452
 Intra-cell Repeating 160 , 193
 Invalid DNS Packets 410
 IP Compression 351
 IP Accounting 489
 IP Configuration 137
 IP Address 268 , 407 , 422 , 472 , 487
 , 498 , 508 , 510 , 512 , 518 , 518
 IP Address Assignment 328
 IP Address Mode 293 , 298 , 302 ,
 307 , 365 , 373
 IP Address Range 313 , 355 , 379 ,
 417
 IP Address Range 178
 IP Address / Netmask 138 , 261
 IP Address / Netmask 505
 IP Address Owner 468
 IP Assignment Pool 307 , 328
 IP Assignment Pool (IPCP) 365 , 373
 IP Pool Name 313 , 355 , 379 , 417 ,
 418
 IP Pool Configuration 416

IP Pools 312 , 355 , 378
 IP/MAC Binding 421
 IPSec 322 , 500
 IPSec (Phase-2) 503
 IPSec Tunnels 502
 IPSec Statistics 502
 IPSec Tunnels 500
 IPSec (Phase-2) SAs 501
 IPSec Debug Level 356
 IPSec over TCP 357
 IPSec Peers 323
 IPv4 Route Configuration 207
 IPv4 Routing Table 214
 ISDN Login 72

J

Join/Prune Interval 283
 Join/Prune State 522 , 523 , 524
 Join/Prune Hold Time 283

K

Keepalive Period 287
 Key Size 436
 Key Value 380

L

L2TP 359
 LAN 137
 Language for login window 458
 Last Command 128
 Last Fix 130
 Last configuration stored 53
 Last Member Query Interval 276
 Last Reply 128
 Last seen 203
 Latitude 130 , 132 , 133
 Layer 4 Protocol 211
 LCP Alive Check 294 , 299 , 303 ,
 308 , 316 , 319 , 367 , 374
 LDAP URL Path 108
 Lease Time 419
 Leased Line 313
 LED mode 55

Level 487 , 499
 Level No. 91
 Licence Key 66
 Licence Status 425
 Licence Key 425
 Licence Serial Number 66
 License valid until 425
 Lifetime 341 , 349
 Line Speed 110
 Link State ID 516
 Load Balancing 224
 Load Balancing Groups 224
 Local Certificate 341
 Local Hostname 361
 Local Address 505
 Local Certificate 411
 Local Services 400
 Local Certificate Description 106 ,
 107 , 436
 Local File Name 436
 Local GRE IP Address 380
 Local ID 325 , 501
 Local ID Type 325 , 341
 Local ID Value 341
 Local IP Address 210 , 255 , 293 ,
 298 , 302 , 307 , 315 , 318 , 328 ,
 362 , 365 , 373 , 380
 Local IP Address 118 , 501
 Local Port 118 , 501 , 505
 Local PPTP IP Address 299
 Local WLAN SSID 436
 Locality 103
 Location 55 , 182
 Location Area Code 128
 Log Format 490
 Logged Actions 389
 Logging Level 76
 Login Frameset 460
 Login Grace Time 76
 Logon 512
 Long Retry Limit 189
 Longitude 130 , 132 , 133
 Loopback active 217

M

MAC Address 138 , 422
 MAC Address 505 , 508 , 511
 Mail Exchanger (MX) 414
 Maintenance 204 , 478
 Management VID 145
 Manual WLAN Controller IP Address
 55
 Marker Position (Latitude, Longitude)
 133
 Marker Position (Longitude, Latitude)
 132
 Master down trials 473
 Matching String 491
 Max. incoming control connections per
 remote IP Address 377
 Max. number of clients - hard limit
 163 , 196
 Max. number of clients - soft limit 163
 , 196
 Max. Period Passive Scan 155
 Max. Period Active Scan 155
 Max. queue size 244
 Max. Scan Duration 155
 Max. Transmission Rate 188
 Maximum Number of Dialup Retries
 294 , 299 , 303 , 308
 Maximum Retries 362
 Maximum Groups 279
 Maximum Message Level of Syslog
 Entries 55
 Maximum Number of Accounting Log
 Entries 55
 Maximum Number of History Entries
 424
 Maximum Sources 279
 Maximum E-mails per Minute 494
 Maximum Number of Syslog Entries
 55
 Maximum number of concurrent connec-
 tions 74
 Maximum Response Time 276
 Maximum Time between Retries 362

- Maximum TTL for Negative Cache
 - Entries 402
 - Maximum TTL for Positive Cache
 - Entries 402
 - Maximum Upload Speed 239 , 242 , 321
 - mbps 506
 - Members 390 , 396
 - Memory Usage 53
 - Message 499
 - Message Compression 491
 - Message Timeout 491
 - Messages 501
 - Metric 210 , 214 , 328
 - Metric Determination 269
 - Metric (direct routes) 269
 - Metric Offset for Inactive Interfaces 261
 - Metric Offset for Active Interfaces 261
 - MIB Variables 436
 - MIB/SNMP Variable to add/edit 436
 - Min. Period Passive Scan 155
 - Min. Period Active Scan 155
 - Min. queue size 244
 - Minimum Time between Retries 362
 - MobiKE 333
 - Mobile Network Provider 126
 - Mode 101 , 118 , 168 , 211 , 215 , 255 , 276 , 279 , 311 , 337 , 341 , 354
 - Mode / Bridge Group 69
 - Modem Model 128
 - Modem Status 121
 - Modem Escape Character 110
 - Monitored Certificate 430
 - Monitored Interface 430 , 451
 - Monitored Subsystems 491
 - Monitored Variable 430
 - Monitored GEO Zone 430
 - Monitored IP Address 448
 - Monitoring 199 , 499
 - Monitoring Mode 475
 - MSDUs that could not be transmitted 507
 - MTU 294 , 380 , 501
 - Multicast 273
 - Multicast Group Prefix Length 285
 - Multicast Group Prefix Length 519
 - Multicast Routing 275
 - Multicast Group Address 280 , 285
 - Multicast Group Range 285
 - Multicast Group Address 519 , 520 , 521 , 521 , 522 , 523 , 524
 - Multicast MSDUs received
 - successfully 507
 - Multicast MSDUs transmitted successfully 507
- ## N
- Name 129 , 130 , 182 , 354
 - NAT 216 , 505
 - NAT method 218
 - NAT Traversal 346
 - NAT Detection 501
 - NAT Configuration 217
 - NAT active 217
 - NAT Interfaces 216
 - Negative Cache 402
 - Negotiation Type 501
 - Neighbor 515
 - Neighbor APs 201
 - Netmask 214 , 255
 - Network Address 255
 - Network Configuration 255
 - Network Provider 121
 - Network Quality 121 , 128
 - Network Name (SSID) 160 , 166 , 168 , 193
 - Network Name (SSID) 203
 - Networking 207
 - New Destination Port 222
 - New Destination IP Address/Netmask 222
 - New File Name 482
 - New Source Port 222
 - New Source IP Address/Netmask 222
 - NMEA TCP Port 130
 - No. 215 , 499 , 504

Noise dBm 508 , 510
 Not Interface-Specific Status 519
 Number of Messages 491
 Number of Spatial Streams 149 , 186
 Number of Admitted Connections 332

O

Oper Status 128
 Operation Band 149 , 186
 Operation Mode 149 , 183 , 186
 Operation Mode (Active) 436
 Operation Mode (Inactive) 436
 Options 88 , 215 , 278 , 356 , 369 ,
 377 , 388 , 397 , 446 , 461 , 476 ,
 480 , 489
 Organization 103
 Organizational Unit 103
 Original Destination IP Address/Net-
 mask 219
 Original Destination Port/Range 219
 Original Source Port/Range 219
 Original Source IP Address/Netmask
 219
 OSPF 265 , 513
 OSPF Status 271
 OSPF Mode 316 , 319 , 368 , 375
 Other Inactivity 389
 Outbound Interface 242
 Outgoing ISDN Number 376
 Outgoing Phone Number 337
 Overbooking allowed 242
 Override Interval 283
 Overwrite similar certificate 436

P

Packets 501
 Parity 116
 Passed 503
 Password 96 , 101 , 106 , 107 , 127 ,
 291 , 297 , 301 , 306 , 354 , 361 ,
 364 , 371 , 413 , 436 , 466 , 494
 Password for protected Certificate
 436

Passwords 58
 Peer Address 325
 Peer ID 325
 Phase-1 Profile 332
 Phase-1 Profiles 339
 Phase-2 Profile 332
 Phase-2 Profiles 348
 Physical Address 512
 Physical Interfaces 109
 PIM 281 , 517
 PIM Mode 282
 PIM Status 287
 PIM Interfaces 281
 PIM Options 286
 PIM Rendezvous Points 285
 Ping 72
 Ping Generator 451
 Ping Test 478
 PLMN 129
 Poisoned Reverse 263
 Policies 383
 Policy 83 , 87
 Pool Usage 418
 Pop-Up window for status indication
 460
 POP3 Server 494
 POP3 Timeout 494
 Port 217 , 415 , 511
 Port Configuration 113 , 144
 Port Mode 115
 Port Number 118
 Positive Cache 402
 Post Login URL 458
 PPPoE 290
 PPPoE Mode 291
 PPPoE Ethernet Interface 291
 PPPoE Interfaces for Multilink 291
 PPTP 296 , 370
 PPTP Inactivity 389
 PPTP Passthrough 217
 PPTP Tunnels 370
 PPTP Address Mode 299
 PPTP Ethernet Interface 297
 PPTP Mode 371

Pre-empt mode (go back into master state) 473
 Precedence 285
 Preferred Network Type 121
 Preshared Key 161 , 166 , 169 , 194 , 325
 Primary DHCP Server 423
 Primary DNS Server 405
 Primary IP Address 468
 Prioritisation Algorithm 239
 Prioritize SIP Calls 397
 Prioritize TCP ACK Packets 294 , 299 , 303 , 308 , 316 , 319 , 367
 Priority 81 , 86 , 242 , 384 , 405
 Priority Queueing 242
 Propagate PMTU 351
 Propagate routes bound on discard/refuse interface 271
 Propagation Delay 283
 Proposals 341 , 349
 Protocol 214 , 219 , 230 , 233 , 248 , 331 , 393 , 415 , 436 , 462 , 487
 Protocol Header Size below Layer 3 239
 Provider 413
 Provider Name 415
 Provisioning Server 420
 Proxy Interface 278
 Proxy ARP 140 , 333
 Proxy ARP Mode 311 , 316 , 319 , 368 , 375
 Public Interface 333
 Public Interface Mode 333
 Public Source IP Address 333
 PUK 121
 PVID 144

Q

QoS 232 , 387 , 512
 QoS Classification 235
 QoS Interfaces/Policies 238
 QoS Filter 232
 QoS Queue 513
 Query Interval 276

Queued 513
 Queues/Policies 239

R

RA Encrypt Certificate 101
 RA Sign Certificate 101
 Radio Profiles 185
 Radio Settings 147
 RADIUS 79
 RADIUS Dialout 83
 RADIUS Secret 81
 Radius Server 194
 RADIUS Server Group ID 354
 Rate 510
 Real Time Jitter Control 239
 Real Time Jitter Control 320
 Reboot 485
 Reboot after execution 436
 Reboot device after 436
 Receive Version 259
 Received Database Description Packets 517
 Received DNS Packets 410
 Received Hello Messages 517
 Received Link State Acknowledge Packets 517
 Received Link State Request Packets 517
 Received Link State Update Packets 517
 Received MPDUs that couldn't be decrypted 507
 Recipient 491
 Region 170 , 178
 Register Suppression Timer 287
 Remaining Validity 430
 Remote Hostname 361
 Remote Address 505
 Remote Networks 500
 Remote Port 501 , 505
 Remote Authentication 78
 Remote File Name 436
 Remote GRE IP Address 380
 Remote ID 501

- Remote IP 118 , 500
 - Remote IP Address 361
 - Remote IP Address 501
 - Remote PPTP IP Address 299 , 371
 - Remote PPTP IP AddressHost Name 371
 - Rendezvous Point IP Address 285
 - Rendezvous Point IP Address 519 , 520
 - Reporting Method 253
 - Response 407
 - Restore Default Settings 72
 - Retransmission Timer 265
 - Retries 83
 - Reverse-Path-Forwarding (RPF) 520 , 521
 - RFC 2091 Variable Timer 263
 - RFC 2453 Variable Timer 263
 - RIP 258
 - RIP Filter 260
 - RIP Interfaces 258
 - RIP Options 263
 - RIP UDP Port 263
 - Roaming Mode 126
 - Roaming Profile 155
 - Robustness 276
 - Rogue Clients 203
 - Rogue APs 202
 - Rogue Client MAC Address 203
 - Role 354
 - Route Announce 259
 - Route Class 209
 - Route Entries 293 , 298 , 302 , 307 , 315 , 318 , 328 , 365 , 373 , 380
 - Route Selector 227
 - Route Timeout 264
 - Route Type 209 , 214
 - Router ID 515 , 516
 - Routes 207
 - Routing Protocols 258
 - Routing table updates caused by External Advertisements 517
 - Routing table updates caused by Summary Links Advertisements 517
 - RSA Key Status 75
 - RTS Threshold 153 , 189
 - RTS frames with no CTS received 507
 - RTSP 398
 - RTSP Port 399
 - RTSP Proxy 398 , 399
 - RTT Mode (Realtime Traffic Mode) 242
 - Rule Chain 252 , 253 , 468
 - Rule Chains 251
 - Running 205
 - Rx Bytes 504 , 505
 - Rx Errors 504
 - Rx Packets 504 , 505 , 506 , 508 , 510
- ## S
- Save configuration 92
 - Scan channels 155
 - Scan Interval 155
 - Scan Threshold 155
 - SCEP URL 101
 - Schedule Interval 447
 - Schedule (Start / Stop Time) 426
 - Scheduling 429
 - Second Timeserver 62
 - Secondary DHCP Server 423
 - Secondary DNS Server 405
 - Security Mode 161 , 166 , 194
 - Security Algorithm 500
 - Select radio 436
 - Select vendor 420
 - Select file 482
 - Selected Channel 149
 - Selected Channels 153
 - Selected PLMN 128
 - Selected Ports 377
 - Selection 392
 - Send 513
 - Send Version 259
 - Send Certificate Chains 358
 - Send Certificate Request Payloads 358

- Send CRLs 358
- Send Initial Contact Message 357
- Send Key Hash Payloads 358
- Send WOL packet over Interface 466
- Sender E-mail Address 494
- Sent Database Description Packets 517
- Sent Hello Messages 517
- Sent Link State Acknowledge Packets 517
- Sent Link State Request Packets 517
- Sent Link State Update Packets 517
- Sequence Age 516
- Serial Number 53
- Serial Port 115 , 115
- Server 415
- Server Address 436
- Server Timeout 83
- Server URL 436
- Server Failures 410
- Server IP Address 81 , 86
- Service 219 , 230 , 233 , 248 , 384 , 462
- Service List 393
- Service Center Address 128
- Services 393
- Set status 436
- Set Time 61
- Set COS value (802.1p/Layer 2) 236
- Set Date 61
- Set DSCP/TOS value (Layer 3) 236
- Set interface status 436
- Severity 491
- Short Guard Interval 153 , 189
- Short Retry Limit 189
- Shortest Path Tree 521
- Show Position on Google Maps 131
- Show passwords and keys in clear text 59
- Signal 168
- Signal dBm 203
- Signal dBm (RSSI1, RSSI2, RSSI3) 508 , 510
- Silent Deny 253
- Silent Deny 217
- SIM Card Uses PIN 121
- SIM Card Uses PIN 110
- SIP 397
- SIP Port 397
- SIP Proxy 397
- Slave Access Points 181
- Slave AP location 178
- Slave AP configuration 180
- Slave AP LED mode 178
- SMS Device 495
- SMTP Authentication 494
- SMTP Server 494
- SNMP 72 , 77 , 496
- SNMP Version 78
- SNMP Listen UDP Port 78
- SNMP Read Community 58
- SNMP Trap Broadcasting 496
- SNMP Trap Community 496
- SNMP Trap Hosts 497
- SNMP Trap Options 496
- SNMP Trap UDP Port 496
- SNMP Write Community 58
- SNR dB 510
- Software & Configuration 480
- Source 384
- Source Interface 211 , 230 , 280
- Source Location 436
- Source Port 211 , 331
- Source Port/Range 219 , 230 , 233 , 248 , 462
- Source Location 205 , 482
- Source File Name 482
- Source IP Address 430 , 436 , 448 , 452
- Source IP Address/Netmask 211 , 219 , 230 , 233 , 248 , 331 , 462
- Source IP Address 521 , 521 , 523 , 524
- Source Port Range 393
- Special Handling Timer 230
- Special Session Handling 228
- Specific Ports 377
- Specify bandwidth 387

SSH 72 , 73
 SSH Port 74
 SSH service active 74
 SSID 203
 Start Mode 332
 Start Time 434
 State 129 , 514 , 515
 State/Province 103
 Static Blacklist 203
 Static Hosts 406
 Statistics 410 , 503 , 516
 Status 52 , 430 , 500 , 502 , 504 , 505
 , 513
 Stop Bits 116
 Stop Time 434
 Subject 491
 Subject Name 436
 Subscriber Number 128
 Subsystem 499
 Successful Trials 448
 Successfully Answered Queries 410
 Summary 103
 Surveillance 447
 Switch Port 113
 Switch to SNMP Browser 92
 Sync SAs with ISP interface state 357
 Synchronisation Mode 476
 Syslog 486
 Syslog Servers 486
 System 55
 System Logic 482
 System Name 55
 System Licences 64
 System Messages 499
 System Reboot 485
 System Management 52
 System Date 53

T

TACACS+ 85
 TACACS+ Secret 86
 Target MAC-Address 466
 TCP Inactivity 389
 TCP Keepalives 76

TCP Port 87
 TCP-MSS Clamping 140
 Telnet 72
 Terms & Conditions 458
 Third Timeserver 62
 Ticket Type 460
 Time 499
 Time Condition 434
 Time Update Interval 62 , 64
 Time Update Policy 62
 Time Zone 61
 Timeout 87 , 118
 Timestamp 487
 Total 503
 Traceroute Test 479
 Tracking IP Address 227
 Traffic Direction 430
 Traffic shaping 239 , 242 , 387
 Transfer Mode 337
 Transfer own IP address over ISDN/
 GSM 337
 Transferred Traffic 430
 Transmit Key 161 , 166 , 194
 Transmit Power 149 , 183
 Transmitted MPDUs 507
 Transparent MAC Address 71
 Trials 430 , 452
 Trigger 430 , 451
 Trigger Status 436
 Triggered Hello Interval 283
 TTL 407
 Tunnel Profile 364
 Tunnel Profiles 360
 Tx Bytes 504 , 505
 Tx Errors 504
 Tx Packets 504 , 505 , 506 , 508 ,
 510
 Type 233 , 248 , 393 , 462 , 466 , 504
 , 516
 Type of Messages 487
 Type of traffic 218
 Type of attack 203

U

U-APSD 160
 UDP Inactivity 389
 UDP Destination Port 361
 UDP Destination Port 369
 UDP Port 83
 UDP Source Port 361
 UDP Source Port Selection 369
 UMTS/LTE 119 , 300
 UMTS/LTE Interface 301
 UMTS/LTE Status 121
 Unchanged for 504
 Unicast MPDUs received successfully 507
 Unicast MSDUs transmitted successfully 507
 Unsuccessful Trials 448
 Update Interval 415
 Update Path 415
 Update Timer 264
 UPnP 453
 UPnP Status 455
 UPnP TCP Port 455
 Upstream Join State 520 , 520 , 521
 Upstream Join Timer 520 , 520 , 521
 Upstream Neighbor IP Address 520 , 520 , 521
 Upstream Override Timer 521
 Uptime 53 , 508 , 510 , 518 , 520 , 520 , 521 , 521 , 522 , 523 , 524
 URL 205 , 482
 URL / IP Address 428
 URL Path Depth 424
 URL SCEP Server URL 436
 Usage Area 149
 Usage Type 308
 Use 132 , 133
 Use CRL 436
 Use as Stub interface 282
 Use PFS Group 349
 Use Zero Cookies 357
 Used Channel 183
 Used Secondary Channel 149
 User 96
 User Defined Channel Plan 155 , 189

User must change password 96
 User Name 291 , 297 , 301 , 306 , 364 , 371 , 413 , 494 , 512
 Username 127
 Users 93 , 354 , 363

V

Value 507
 Vendor Mode 81
 Version Check 436
 View 514 , 518 , 519 , 522
 Virtual Routers 469
 Virtual Interface Priority 472
 Virtual Router 468
 Virtual Router ID 472 , 475 , 476
 Virtual Router Interface 472
 Virtual Router Backup 468
 Virtual Router IP Address 472
 Virtual Router Master 468
 VLAN 141 , 199 , 291
 VLAN Identifier 143
 VLAN Members 143
 VLAN ID 138 , 199 , 291
 VLAN Name 143
 VLANs 143
 VoIP 397
 VPN 322
 VR Synchronisation 475
 VRRP Advertisement 468
 VRRP router 468
 VSS 508

W

Wake-On-LAN 462
 Wake-On-LAN Filter 466
 Wake-On-LAN Filter 462
 Wake-On-LAN Rule Chain 466
 Walled Garden 458
 Walled Garden URL 458
 Walled Network / Netmask 458
 WAN 288
 Web Filter 423
 Web Filter Status 424

Weight 242
WEP Key 1-4 161 , 166 , 194
Whitelisted 428
Wildcard 414
Wildcard Mode 71
Wildcard MAC Address 71
WINS Server 402
Wireless Mode 151 , 188
Wireless LAN 146
Wireless LAN Controller 172
Wireless Networks (VSS) 157 , 192 ,
200
WLAN 147 , 506
WLANx 506
WLC SSID 436
WMM 193
WOL Rules 465
WPA Cipher 161 , 166 , 194
WPA Mode 161 , 166 , 194
WPA2 Cipher 161 , 166 , 194
Write certificate in configuration 436

X

XAUTH Profile 332
XAUTH Profiles 353

Z

Zero Cookie Size 357
Zone Coverage Fail State Time 134
Zone Valid 134
Zone Coverage Fail State 134
Zone Initial State 134
Zone Initial State Time 134
Zone Time To False 134
Zone Time To True 134