



# Manual bintec RS Series

New Generation

Copyright© Version 10.1.4 (SVN4082), 2016 bintec elmeg GmbH

## Legal Notice

### Warranty

This publication is subject to change.

bintec elmeg GmbH offers no warranty whatsoever for information contained in this manual. bintec elmeg GmbH is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Copyright © bintec elmeg GmbH.

All rights to the data included, in particular the right to copy and propagate, are reserved by bintec elmeg GmbH.

# Table of Contents

Chapter 1	Installation. . . . .	1
1.1	bintec RS353j, bintec RS353jw and bintec RS353j-4G. . . . .	1
1.1.1	Setting up and connecting . . . . .	1
1.1.2	Connectors . . . . .	4
1.1.3	LEDs . . . . .	5
1.1.4	Scope of supply . . . . .	7
1.1.5	General Product Features . . . . .	8
1.1.6	Reset . . . . .	9
1.2	bintec RS123, bintec RS123w, bintec RS353a and bintec RS353aw. . . . .	10
1.2.1	Setting up and connecting . . . . .	10
1.2.2	Connectors . . . . .	13
1.2.3	LEDs . . . . .	14
1.2.4	Scope of supply . . . . .	16
1.2.5	General Product Features . . . . .	17
1.2.6	Reset . . . . .	19
1.3	Support information . . . . .	20
1.4	Cleaning. . . . .	20
1.5	Pin Assignments . . . . .	20
1.5.1	USB console interface. . . . .	20
1.5.2	Ethernet interface. . . . .	21
1.5.3	xDSL interface . . . . .	21
1.5.4	ISDN S0 port. . . . .	22
1.5.5	USB interface . . . . .	23
1.6	Inserting the SIM card . . . . .	23
Chapter 2	Basic configuration . . . . .	25
2.1	Presettings . . . . .	25

2.1.1	IP Configuration . . . . .	25
2.1.2	Software update . . . . .	26
2.2	System requirements . . . . .	26
2.3	Preparation . . . . .	26
2.3.1	Gathering data . . . . .	27
2.3.2	Configuring a PC . . . . .	29
2.3.3	Modify system password. . . . .	30
2.4	Setting up an internet connection . . . . .	31
2.4.1	Internet connection over internal xDSL modem . . . . .	31
2.4.2	Internet connection over UMTS/LTE. . . . .	31
2.4.3	Other internet connections . . . . .	32
2.4.4	Testing the configuration. . . . .	32
2.5	Setting up wireless LAN . . . . .	32
2.6	Software Update . . . . .	33
<b>Chapter 3</b>	<b>Access and configuration. . . . .</b>	<b>35</b>
3.1	Access Options. . . . .	35
3.1.1	Access via LAN . . . . .	35
3.1.2	Access via the Console Interface . . . . .	38
3.1.3	Access over ISDN . . . . .	39
3.2	Login . . . . .	40
3.2.1	User names and passwords in ex works state . . . . .	40
3.2.2	Logging in for Configuration . . . . .	41
3.3	Configuration options . . . . .	41
3.3.1	GUI (Graphical User Interface) . . . . .	42
3.3.2	SNMP shell . . . . .	51
<b>Chapter 4</b>	<b>Assistants . . . . .</b>	<b>52</b>

<b>Chapter 5</b>	<b>System Management . . . . .</b>	<b>53</b>
5.1	Status . . . . .	53
5.2	Global Settings . . . . .	56
5.2.1	System . . . . .	56
5.2.2	Passwords . . . . .	59
5.2.3	Date and Time . . . . .	61
5.2.4	System Licences . . . . .	66
5.3	Interface Mode / Bridge Groups . . . . .	68
5.3.1	Interfaces . . . . .	70
5.4	Administrative Access . . . . .	74
5.4.1	Access . . . . .	74
5.4.2	SSH . . . . .	75
5.4.3	SNMP . . . . .	79
5.5	Remote Authentication . . . . .	81
5.5.1	RADIUS . . . . .	81
5.5.2	TACACS+ . . . . .	87
5.5.3	Options . . . . .	90
5.6	Configuration Access . . . . .	91
5.6.1	Access Profiles . . . . .	91
5.6.2	Users . . . . .	95
5.7	Certificates . . . . .	99
5.7.1	Certificate List . . . . .	99
5.7.2	CRLs . . . . .	108
5.7.3	Certificate Servers . . . . .	110
<b>Chapter 6</b>	<b>Physical Interfaces . . . . .</b>	<b>111</b>
6.1	Ethernet Ports . . . . .	111
6.1.1	Port Configuration . . . . .	112

6.2	ISDN Ports . . . . .	114
6.2.1	ISDN Configuration . . . . .	115
6.2.2	MSN Configuration . . . . .	117
6.3	DSL Modem . . . . .	120
6.3.1	DSL Configuration . . . . .	120
6.4	UMTS/LTE. . . . .	123
6.4.1	UMTS/LTE. . . . .	123
<b>Chapter 7</b>	<b>LAN . . . . .</b>	<b>134</b>
7.1	IP Configuration . . . . .	134
7.1.1	Interfaces . . . . .	134
7.2	VLAN . . . . .	147
7.2.1	VLANs . . . . .	149
7.2.2	Port Configuration . . . . .	150
7.2.3	Administration . . . . .	151
<b>Chapter 8</b>	<b>Wireless LAN . . . . .</b>	<b>152</b>
8.1	WLAN . . . . .	152
8.1.1	Radio Settings . . . . .	152
8.1.2	Wireless Networks (VSS) . . . . .	163
8.1.3	Client Link . . . . .	172
8.1.4	Bridge Links . . . . .	176
8.2	Administration . . . . .	177
8.2.1	Basic Settings . . . . .	178
8.3	Configuration. . . . .	178
8.3.1	WLAN - Configuration example . . . . .	178
<b>Chapter 9</b>	<b>Wireless LAN Controller . . . . .</b>	<b>181</b>
9.1	Wizard . . . . .	181

9.1.1	Basic Settings . . . . .	182
9.1.2	Radio Profile . . . . .	183
9.1.3	Wireless Network . . . . .	183
9.1.4	Start automatic installation . . . . .	185
9.2	Controller Configuration . . . . .	187
9.2.1	General . . . . .	187
9.2.2	Slave AP Autoprofile . . . . .	189
9.3	Slave AP configuration . . . . .	191
9.3.1	Slave Access Points . . . . .	192
9.3.2	Radio Profiles . . . . .	196
9.3.3	Wireless Networks (VSS) . . . . .	203
9.4	Monitoring . . . . .	211
9.4.1	WLAN Controller . . . . .	212
9.4.2	Slave Access Points . . . . .	213
9.4.3	Active Clients . . . . .	215
9.4.4	Wireless Networks (VSS) . . . . .	217
9.4.5	Client Management . . . . .	217
9.5	Neighbor Monitoring . . . . .	218
9.5.1	Neighbor APs . . . . .	218
9.5.2	Rogue APs . . . . .	219
9.5.3	Rogue Clients . . . . .	220
9.6	Maintenance . . . . .	221
9.6.1	Firmware Maintenance . . . . .	222
<b>Chapter 10</b>	<b>Networking . . . . .</b>	<b>224</b>
10.1	Routes . . . . .	224
10.1.1	IPv4 Route Configuration . . . . .	224
10.1.2	IPv6 Route Configuration . . . . .	230
10.1.3	IPv4 Routing Table . . . . .	233
10.1.4	IPv6 Routing Table . . . . .	234

10.1.5	Options . . . . .	234
10.2	IPv6 General Prefixes . . . . .	236
10.2.1	General Prefix Configuration . . . . .	236
10.3	NAT . . . . .	238
10.3.1	NAT Interfaces . . . . .	238
10.3.2	NAT Configuration . . . . .	239
10.3.3	NAT - Configuration example . . . . .	246
10.4	Load Balancing . . . . .	248
10.4.1	Load Balancing Groups . . . . .	248
10.4.2	Special Session Handling . . . . .	253
10.4.3	Load balancing - Configuration example . . . . .	256
10.5	QoS . . . . .	259
10.5.1	IPv4/IPv6 Filter . . . . .	259
10.5.2	QoS Classification . . . . .	263
10.5.3	QoS Interfaces/Policies . . . . .	266
10.6	Access Rules . . . . .	273
10.6.1	Access Filter . . . . .	275
10.6.2	Rule Chains . . . . .	279
10.6.3	Interface Assignment . . . . .	281
10.7	Drop In . . . . .	283
10.7.1	Drop In Groups . . . . .	283
<b>Chapter 11</b>	<b>Routing Protocols . . . . .</b>	<b>286</b>
11.1	RIP . . . . .	286
11.1.1	RIP Interfaces . . . . .	286
11.1.2	RIP Filter . . . . .	288
11.1.3	RIP Options . . . . .	291
<b>Chapter 12</b>	<b>Multicast . . . . .</b>	<b>294</b>



12.1	General . . . . .	295
12.1.1	General . . . . .	296
12.2	IGMP . . . . .	296
12.2.1	IGMP . . . . .	297
12.2.2	Options . . . . .	299
12.3	Forwarding . . . . .	301
12.3.1	Forwarding . . . . .	301
<b>Chapter 13</b>	<b>WAN. . . . .</b>	<b>303</b>
13.1	Internet + Dialup . . . . .	303
13.1.1	PPPoE . . . . .	305
13.1.2	PPTP . . . . .	312
13.1.3	PPPoA . . . . .	317
13.1.4	ISDN . . . . .	323
13.1.5	UMTS/LTE. . . . .	331
13.1.6	IP Pools . . . . .	336
13.2	ATM . . . . .	337
13.2.1	Profiles . . . . .	338
13.2.2	Service Categories . . . . .	342
13.2.3	OAM Controlling . . . . .	345
13.3	Real Time Jitter Control . . . . .	349
13.3.1	Controlled Interfaces . . . . .	349
<b>Chapter 14</b>	<b>VPN . . . . .</b>	<b>351</b>
14.1	IPSec . . . . .	351
14.1.1	IPSec Peers . . . . .	352
14.1.2	Phase-1 Profiles . . . . .	370
14.1.3	Phase-2 Profiles . . . . .	379
14.1.4	XAUTH Profiles . . . . .	384
14.1.5	IP Pools . . . . .	386

14.1.6	Options . . . . .	387
14.2	L2TP . . . . .	391
14.2.1	Tunnel Profiles . . . . .	391
14.2.2	Users . . . . .	395
14.2.3	Options . . . . .	401
14.3	PPTP . . . . .	402
14.3.1	PPTP Tunnels . . . . .	402
14.3.2	Options . . . . .	410
14.3.3	IP Pools . . . . .	411
14.4	GRE . . . . .	412
14.4.1	GRE Tunnels . . . . .	412
<b>Chapter 15</b>	<b>Firewall . . . . .</b>	<b>415</b>
15.1	Policies . . . . .	416
15.1.1	IPv4 Filter Rules . . . . .	416
15.1.2	IPv6 Filter Rules . . . . .	419
15.1.3	Options . . . . .	422
15.2	Interfaces . . . . .	424
15.2.1	IPv4 Groups . . . . .	424
15.2.2	IPv6 Groups . . . . .	425
15.3	Addresses . . . . .	426
15.3.1	Address List . . . . .	426
15.3.2	Groups . . . . .	428
15.4	Services . . . . .	429
15.4.1	Service List . . . . .	429
15.4.2	Groups . . . . .	431
15.5	Configuration. . . . .	432
15.5.1	SIF - Configuration example . . . . .	432

Chapter 16	VoIP . . . . .	437
16.1	SIP . . . . .	437
16.1.1	Options . . . . .	437
16.2	RTSP . . . . .	438
16.2.1	RTSP Proxy . . . . .	438
Chapter 17	Local Services . . . . .	440
17.1	DNS . . . . .	440
17.1.1	Global Settings . . . . .	442
17.1.2	DNS Servers . . . . .	444
17.1.3	Static Hosts . . . . .	447
17.1.4	Domain Forwarding . . . . .	448
17.1.5	Dynamic Hosts . . . . .	450
17.1.6	Cache . . . . .	450
17.1.7	Statistics . . . . .	451
17.2	HTTPS . . . . .	452
17.2.1	HTTPS Server . . . . .	452
17.3	DynDNS Client . . . . .	453
17.3.1	DynDNS Update . . . . .	453
17.3.2	DynDNS Provider . . . . .	455
17.4	DHCP Server . . . . .	457
17.4.1	IP Pool Configuration . . . . .	457
17.4.2	DHCP Configuration . . . . .	458
17.4.3	IP/MAC Binding . . . . .	463
17.4.4	DHCP Relay Settings . . . . .	464
17.4.5	DHCP - Configuration example . . . . .	465
17.5	DHCPv6 Server . . . . .	468
17.5.1	DHCPv6 Server . . . . .	470
17.5.2	DHCPv6 Global Options . . . . .	472

17.5.3	Stateful Clients . . . . .	473
17.5.4	Stateful Clients Configuration. . . . .	474
17.6	Web Filter . . . . .	475
17.6.1	General . . . . .	476
17.6.2	Filter List . . . . .	478
17.6.3	Black / White List . . . . .	480
17.6.4	History . . . . .	481
17.7	CAPi Server . . . . .	481
17.7.1	User . . . . .	481
17.7.2	Options . . . . .	483
17.8	Scheduling . . . . .	484
17.8.1	Trigger . . . . .	484
17.8.2	Actions . . . . .	491
17.8.3	Options . . . . .	502
17.8.4	Configuration example - Time-controlled Tasks (Scheduling) . . . . .	503
17.9	Surveillance . . . . .	506
17.9.1	Hosts . . . . .	506
17.9.2	Interfaces . . . . .	509
17.9.3	Ping Generator . . . . .	510
17.10	ISDN Theft Protection . . . . .	512
17.10.1	Options . . . . .	512
17.11	UPnP . . . . .	514
17.11.1	Interfaces . . . . .	515
17.11.2	General . . . . .	516
17.12	HotSpot Gateway . . . . .	517
17.12.1	HotSpot Gateway . . . . .	519
17.12.2	Options . . . . .	523
17.13	Wake-On-LAN . . . . .	524
17.13.1	Wake-On-LAN Filter . . . . .	524
17.13.2	WOL Rules . . . . .	528

17.13.3	Interface Assignment . . . . .	530
17.14	BRRP . . . . .	531
17.14.1	Virtual Routers . . . . .	532
17.14.2	VR Synchronisation . . . . .	538
17.14.3	Options . . . . .	539
<b>Chapter 18</b>	<b>Maintenance . . . . .</b>	<b>541</b>
18.1	Log out Users . . . . .	541
18.1.1	Log out Users . . . . .	541
18.2	Diagnostics . . . . .	542
18.2.1	Ping Test . . . . .	542
18.2.2	DNS Test . . . . .	543
18.2.3	Traceroute Test . . . . .	544
18.3	Software & Configuration . . . . .	544
18.3.1	Options . . . . .	545
18.4	Reboot . . . . .	549
18.4.1	System Reboot . . . . .	549
18.5	Factory Reset . . . . .	550
<b>Chapter 19</b>	<b>External Reporting . . . . .</b>	<b>551</b>
19.1	Syslog . . . . .	551
19.1.1	Syslog Servers . . . . .	551
19.2	IP Accounting . . . . .	554
19.2.1	Interfaces . . . . .	554
19.2.2	Options . . . . .	554
19.3	Alert Service . . . . .	556
19.3.1	Alert Recipient . . . . .	556
19.3.2	Alert Settings . . . . .	559
19.4	SNMP . . . . .	561

19.4.1	SNMP Trap Options . . . . .	561
19.4.2	SNMP Trap Hosts . . . . .	563
19.5	SIA . . . . .	563
19.5.1	SIA . . . . .	563
<b>Chapter 20</b>	<b>Monitoring . . . . .</b>	<b>565</b>
20.1	Internal Log . . . . .	565
20.1.1	System Messages . . . . .	565
20.2	IPSec . . . . .	566
20.2.1	IPSec Tunnels . . . . .	566
20.2.2	IPSec Statistics . . . . .	568
20.3	ISDN/Modem . . . . .	569
20.3.1	Current Calls . . . . .	569
20.3.2	Call History . . . . .	570
20.4	Interfaces . . . . .	571
20.4.1	Statistics . . . . .	571
20.5	WLAN . . . . .	574
20.5.1	WLANx . . . . .	574
20.5.2	VSS . . . . .	576
20.5.3	Client Management . . . . .	579
20.5.4	Bridge Links . . . . .	580
20.5.5	Client Links . . . . .	582
20.6	Bridges . . . . .	585
20.6.1	br<x> . . . . .	585
20.7	HotSpot Gateway . . . . .	585
20.7.1	HotSpot Gateway . . . . .	585
20.8	QoS . . . . .	586
20.8.1	QoS . . . . .	586

Index . . . . . 588





# Chapter 1 Installation



## Caution

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

## 1.1 bintec RS353j, bintec RS353jw and bintec RS353j-4G

### 1.1.1 Setting up and connecting



## Note

All you need for this are the cables and antennas supplied with the equipment.



## Caution

The use of the wrong mains equipment may damage your device. You should only use the power supply unit provided! If you require foreign adapters/mains units, please contact our bintec elmeg service.

Incorrect cabling of the ISDN and ETH interfaces may also damage your device. Connect only the ETH interface of the device to the LAN interface of the computer/hub or a WAN interface if available and the ISDN interface of the device only to the ISDN connection.



## 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. If no entry is specified, every incoming ISDN call is accepted by the ISDN Login service.

**bintec RS353jw** is equipped with two external WLAN antennas, **bintec RS353j-4G** is

equipped with two external LTE UMTS antennas and one external GPS antenna.

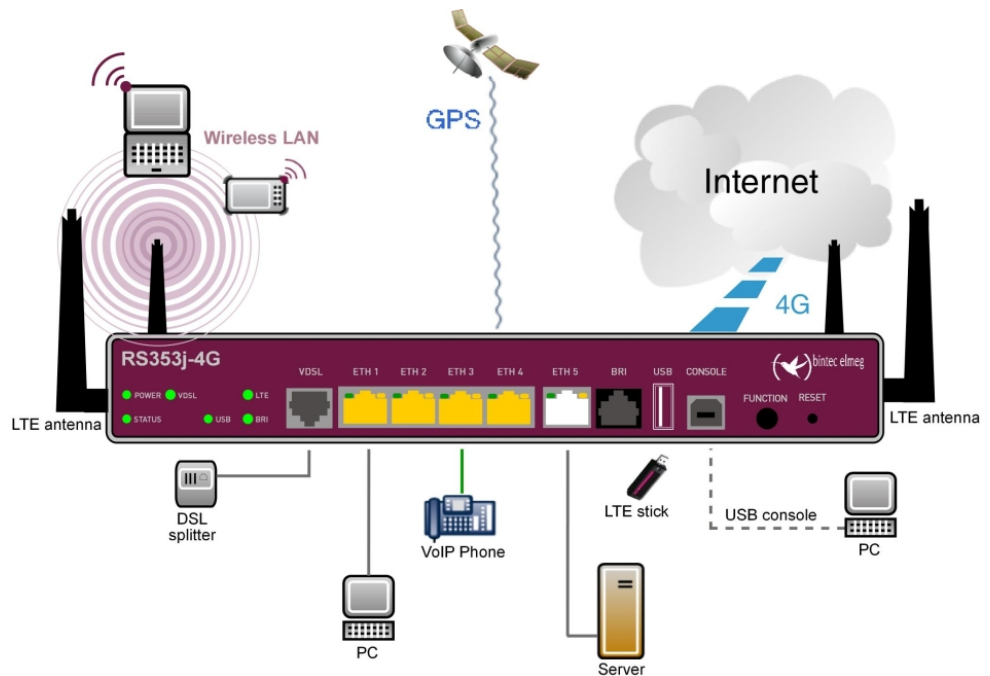


Fig. 1: Connection options using the example of **bintec RS353j-4G**

When setting up and connecting, carry out the steps in the following sequence:

- (1) **Antennas**  
Screw the external WLAN antennas (only **bintec RS353jw**) supplied to the connections provided for this purpose. With **bintec RS353j-4G** screw the two external UMTS antenna and the GPS antenna to the connections provided.
- (2) **ETH1-4**  
Connect the first switch port (**ETH1**, yellow connector) your device through the supplied Ethernet cable to your LAN to configure the device. The device automatically detects whether It is connected to a switch or directly to a PC. Connect more devices, LANs or WANs to the Port ETH1 up ETH4 on.
- (3) **VDSL**  
Connect the VDSL interface (**VDSL**, grey connector) of your device to the DSL output of the splitter using the DSL cable (grey cable) supplied.
- (4) **Power connection**  
Connect the POWER interface of your device via the supplied power cord to your power supply.

You can set up further connections as required:

- ETH5

Connect the **ETH5** interface (white connector) of your device via a RJ45 cable to your LAN/WAN interface.

- **BRI**

Connect the **BRI** interface (black connector) of the device to your ISDN socket using the ISDN BRI cable provided.

- **USB**

Connect a wireless flash drive to the USB port on your device.

- **USB CONSOLE**

For alternative configurations, connect the USB console type B of your device via a USB cable to the PC. A suitable cable is available as an accessory.

The device is now ready for configuration with the **GUI**. Chapter [Basic configuration](#) on page 25 provides a detailed step-by-step guide to the basic functions on your device.

## Installation

The devices are optionally equipped with straps in the housing on the wall, as a table top unit or for installation in 19 inch cabinet.

### Use as a table-top device

Attach the four self-adhesive feet on the bottom of the device. Place your device on a solid, level base.

### The 19- inch cabinet installation

Screw your device using the supplied brackets and screws into the cabinet.

### Wallmounting

To attach the **bintec RS353x** series on the wall, use the tabs on the back side of the housing.



#### Warning

Before drilling, make sure that there are no building installations where you are drilling. If gas, electricity, water or waste water lines are damaged, you may endanger your life or damage property.

### Kensington Lock

The devices offer the possibility of a Kensington lock to secure. You will find the required

notch on the right side of the housing.

## 1.1.2 Connectors

The devices have about a 4-port gigabit switch-port, a gigabit LAN/WAN connection, a VDSL connection, an ISDN BRI interface, a USB port (type A), as well as a USB console port (type B).

The connections are arranged as follows:

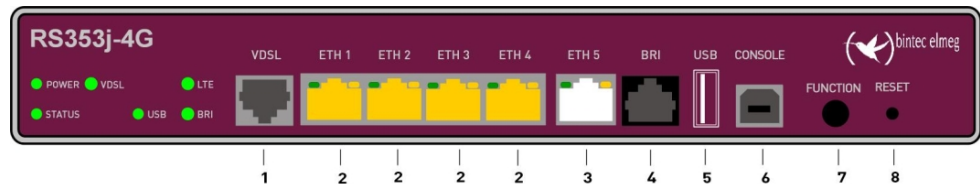


Fig. 2: **bintec RS353j-4G** front panel

### Front panel connections

1	VDSL (gray)	VDSL interface
2	ETH1 / ETH2 / ETH3 / ETH4 (yellow)	10/100/1000 Base-T Ethernet interfaces
3	ETH5 (white)	10/100/1000 Base-T Ethernet interfaces
4	BRI (black)	BRI connection
5	USB	USB connection type A
6	USB CONSOLE	USB console type B
7	FUNCTION	Function button
8	RESET	Reset button

On the back of the device the mains connection and the on/off switch is located. **bintec RS353j-4G** has connectors for two external Wi-Fi antenna. The devices **bintec RS353j-4G** have a connectors for the GPS antenna and 2 ports for the LTE/UMTS antenna. The connectors for the LTE/UMTS antenna are located on the sides of the device.

The connections are arranged as follows:



Fig. 3: **bintec RS353j-4G** rear panel

### Rear panel connections

9	POWER	IEC C6 power connection and on/off switch
10	WLAN 1 / 2	Connections for the WLAN antenna (only <b>bintec RS353jw</b> )
11	GPS	Connection for the GPS antenna (only <b>bintec RS353j-4G</b> )
12	LTE 1 - 2	Connections for the LTE/UMTS antenna (only <b>bintec RS353j-4G</b> )

### 1.1.3 LEDs

The LEDs of your device provide information about specific activities and states of the device.

The LEDs are arranged as follows:

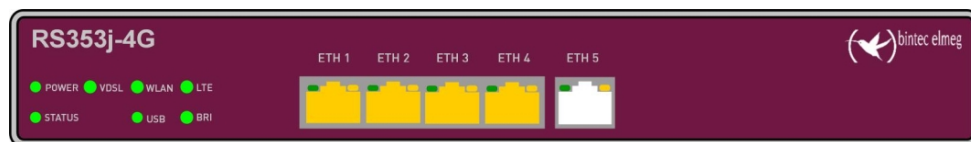


Fig. 4: Arrangement of the LEDs

### LED status display

LED	Colour	Status	Information
POWER	green	on	Power supply is connected.
		off	No power supply.
STATUS	green	on	After switching on: The device has started. During operation: An error has occurred.
		flashing	The device is active.
		off	During operation: An error has occurred.
VDSL	green	on	Connection established.
		slow flashing	Synchronisation running.

LED	Colour	Status	Information
		off	No Synchronisation.
		flickering	Data transfer.
WLAN (only RS353jw)	green	on	WLAN connection established.
	green	off	Radio or all assigned VSS inactive
	green	on (slowly flashing)	VSS is active, no client connected
	green	on (fast flashing)	VSS is active, at least one client connected
USB	green	on (flickering)	VSS is active, at least one client connected, active data traffic
	green	flashing	Data traffic via USB send / receive.
		off	No USB connection.
LTE	green	on	LTE connection established.
	green	flashing	Data traffic via LTE send / receive.
		off	No LTE connection.
BRI	green	on	D-channel is active.
	green	flashing	At least one B-channel is active.
		off	No ISDN connection.
LAN 1 bis 4 (Link/Act)	green	on	Ethernet connection established.
	green	flashing	Data traffic via Ethernet.
		off	No Ethernet connection.
LAN 1 bis 4 (Speed)	green	on	1000 Mbits transfer rate.
	orange	on	100 Mbits transfer rate.
		off	10 Mbits transfer rate.
LAN 5 (Link/Act)	green	on	WAN-Ethernet connection established.
	green	flashing	Data via LAN 5 send / receive.
		off	No Ethernet connection.
LAN 5 (Speed)	green	on	The device is connected to the WAN at 1000 Mbits.
	orange	on	The device is connected to the WAN at 100

LED	Colour	Status	Information
			Mbits.
		off	The device is connected to the WAN at 10 Mbits, or no Data transfer.

You can determine the status of the router in BRRP operation with the aid of the status LED.

#### LED BRRP-Anzeige

LED	Colour	Status	Information
STATUS	green	flashing	The device is functioning as a master router.
STATUS	green	Heartbeat (on - on - off)	The device is functioning as a backup router.

### 1.1.4 Scope of supply

Your device is supplied with the following parts:

Scope of supply	bintec RS353j	bintec RS353jw	bintec RS353j-4G
Cable sets/mains unit/ other	Ethernet cable (yellow)  xDSL cable Type 2 (gray)  ISDN cable (black)  Power cable  19" Mounting frame  Screws	Ethernet cable (yellow)  xDSL cable Type 2 (gray)  ISDN cable (black)  Power cable  19" Mounting frame  Screws  2 external WLAN antenna	Ethernet cable (yellow)  xDSL cable Type 2 (gray)  ISDN cable (black)  Power cable  19" Mounting frame  Screws  2 external LTE/UMTS antenna  1 GPS antenna
Documentation	Safety notices Installation poster	Safety notices Installation poster	Safety notices Installation poster
Online documentation	User's Guide  Workshops  MIB reference	User's Guide  Workshops  MIB reference	User's Guide  Workshops  MIB reference

## 1.1.5 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 RS353j , bintec RS353jw and bintec RS353j-4G
Dimensions and weights:	
Equipment dimensions without cable (B x H x D):	240 mm x 42 mm x 180 mm
Weight	approx. 1,100 g
Transport weight (incl. documentation, cables, packaging)	approx. 1600 g
Memory	128 MB RAM, 32 MB Flash-ROM
LEDs	18 (1x Power, 1x Status, 5x2 Ethernet, 6x Function)
Power consumption of the device	4.7 Watt
Voltage supply	AC 100 bis 240 V, 50 bis 60 Hz
Environmental requirements:	
Storage temperature	-25 °C to +70 °C
Operating temperature	0 °C to +40 °C
Relative atmospheric humidity	10 % to 95 % (non-condensing)
Room classification	Only use in dry rooms.
Available interfaces:	
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, Auto MDIX
Gigabit LAN/WAN Port	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, Auto MDIX
VDSL/ADSL	Internal VDSL/ADSL modem for Annex B and Annex J
ISDN BRI Port	Permanently installed
USB Port	USB2.0 type A
USB Console (Type B)	Supported Baud rates: 1200-115200 (default: 115200 Baud)
Standards & Guidelines	R&TTE Directive 1999/5/EC



<b>Property</b>	<b>bintec RS353j , bintec RS353jw and bintec RS353j-4G</b>
	CE symbol for all EU states
SAFERNET TM Security Technology	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec

### Antennas and sockets

<b>Property</b>	<b>bintec RS353j</b>	<b>bintec RS353jw</b>	<b>bintec RS353j-4G</b>
WLAN interface (antennas)	-	802.11a/b/g/h; 802.11n 2.4 GHz and 5 GHz;  2 TX, 2 RX (2x2)  Channel level (2.4 GHz / 5GHz)  RSMA socket	-
LTE - UMTS antennas	-	-	SMA socket
GPS antennas	-	-	SMA socket
Available sockets:			
Ethernet interface	RJ45 socket (yellow)	RJ45 socket (yellow)	RJ45 socket (yellow)
Ethernet interface	RJ45 socket (white)	RJ45 socket (white)	RJ45 socket (white)
VDSL/ADSL	RJ45 socket (gray)	RJ45 socket (gray)	RJ45 socket (gray)
ISDN BRI interface	RJ45 socket (black)	RJ45 socket (black)	RJ45 socket (black)
USB	USB-Anschluss type A	USB-Anschluss type A	USB-Anschluss type A
USB Console	USB socket type B	USB socket type B	USB socket type B

## 1.1.6 Reset

If the configuration is incorrect or if your device cannot be accessed, you can reset the device to the ex works standard settings using the Reset button on the back of the device. All the existing data will be deleted if you do this.

Proceed as follows:

- (1) Switch off your device.
- (2) Press the **Reset** button on your device.
- (3) Keep the **Reset** button on your device pressed down and switch the device back on.
- (4) After the *Status* LED has flashed five times, release the **Reset** button.

**Note**

If you delete the boot configuration via the **GUI** (menu **Maintenance->Software & Configuration**) all passwords are also reset and the current boot configuration is 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 25

## 1.2 bintec RS123, bintec RS123w, bintec RS353a and bintec RS353aw

### 1.2.1 Setting up and connecting

**Note**

All you need for this are the cables and antennas supplied with the equipment.

**Caution**

The use of the wrong mains equipment may damage your device. You should only use the power supply unit provided! If you require foreign adapters/mains units, please contact our bintec elmeg service.

Incorrect cabling of the ISDN and ETH interfaces may also damage your device. Connect only the ETH interface of the device to the LAN interface of the computer/hub or a WAN interface if available and the ISDN interface of the device only to the ISDN connection.

**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. If no entry is specified, every incoming ISDN call is accepted by the ISDN Login service.

**bintec RS123aw** and **bintec RS353aw** are equipped with two external WLAN antennas.

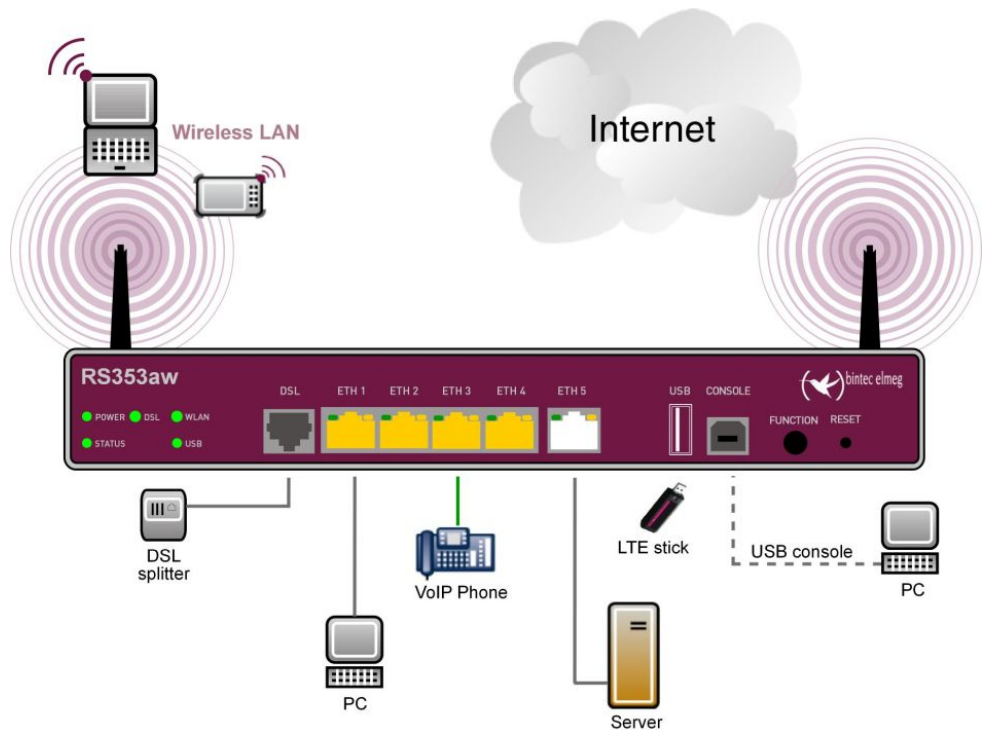


Fig. 5: Connection options using the example of **bintec RS353aw**

When setting up and connecting, carry out the steps in the following sequence:

- (1) **Antennas**  
Screw the external WLAN antennas (only **bintec 123w** and **bintec RS353aw**) supplied to the connections provided for this purpose.
- (2) **ETH1-4**  
Connect the first switch port (**ETH1**, yellow connector) your device through the supplied Ethernet cable to your LAN to configure the device. The device automatically detects whether It is connected to a switch or directly to a PC. Connect more devices, LANs or WANs to the Port ETH1 up ETH4 on.
- (3) **DSL (bintec RS353a and bintec RS353aw)**  
Connect the DSL interface (**DSL**, grey connector) of your device to the DSL output of the splitter using the DSL cable (grey cable) supplied.
- (4) **Power connection**  
Connect the POWER interface of your device via the supplied power cord to your power supply.

You can set up further connections as required:

- **ETH5**

Connect the **ETH5** interface (white connector) of your device via a RJ45 cable to your LAN/WAN interface.

- USB

Connect a wireless flash drive to the USB port on your device.

- USB CONSOLE

For alternative configurations, connect the USB console type B of your device via a USB cable to the PC. A suitable cable is available as an accessory.

The device is now ready for configuration with the **GUI**. Chapter *Basic configuration* on page 25 provides a detailed step-by-step guide to the basic functions on your device.

## Installation

The devices are optionally equipped with straps in the housing on the wall, as a table top unit or for installation in 19 inch cabinet.

### Use as a table-top device

Attach the four self-adhesive feet on the bottom of the device. Place your device on a solid, level base.

### The 19- inch cabinet installation

Screw your device using the supplied brackets and screws into the cabinet.

### Wallmounting

To attach the devices **bintec RS123**, **bintec RS123w**, **bintec RS353a** or **bintec RS353aw** on the wall, use the tabs on the back side of the housing.



#### Warning

Before drilling, make sure that there are no building installations where you are drilling. If gas, electricity, water or waste water lines are damaged, you may endanger your life or damage property.

### Kensington Lock

The devices offer the possibility of a Kensington lock to secure. You will find the required notch on the right side of the housing.

## 1.2.2 Connectors

The devices provides five Gigabit Ethernet ports which can be independently configured for use in a LAN, WAN, or DMZ, a USB port (type A), as well as a USB console port (type B). Furthermore, the devices **bintec RS123** and **bintec RS123w** have a SFP slot for optical fiber expansion modules.



### Note

Note that the switch port ETH5 is deactivated if a SFP module is equipped.

The devices **bintec RS353a** and **bintec RS353aw** also feature a DSL connection.

The connections are arranged as follows:

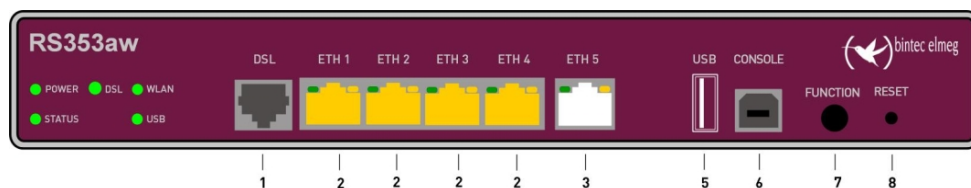


Fig. 6: **bintec RS353aw** front panel

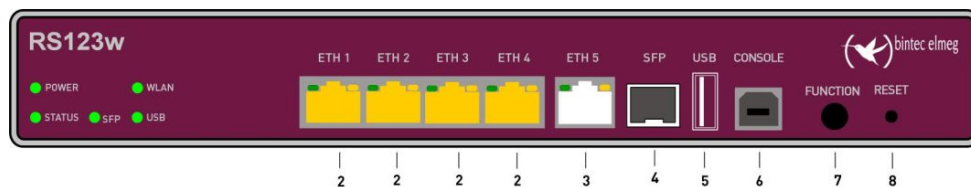


Fig. 7: **bintec RS123w** front panel

### Front panel connections

1	DSL (gray)	VDSL interface ( <b>RS353a</b> , <b>RS353aw</b> )
2	ETH1 / ETH2 / ETH3 / ETH4 (yellow)	10/100/1000 Base-T Ethernet interfaces
3	ETH5 (white)	10/100/1000 Base-T Ethernet interfaces
4	SFP	SFP Slot for 1000 Mbit/s Ethernet SFP module ( <b>RS123</b> and <b>RS123w</b> )
5	USB	USB connection type A
6	USB CONSOLE	USB console type B

7	FUNCTION	Function button
8	RESET	Reset button

On the back of the device the mains connection and the on/off switch is located. **bintec RS123w** and **bintec RS353aw** has connectors for two external Wi-Fi antenna.

The connections are arranged as follows:



Fig. 8: **bintec RS123w**, **bintec RS353aw** rear panel

### Rear pannel connections

9	POWER	IEC C6 power connection and on/off switch
10	WLAN 1 / 2	Connections for the WLAN antenna (only <b>bintec RS123w</b> and <b>bintec RS353aw</b> )

## 1.2.3 LEDs

The LEDs of your device provide information about specific activities and states of the device.

The LEDs are arranged as follows:

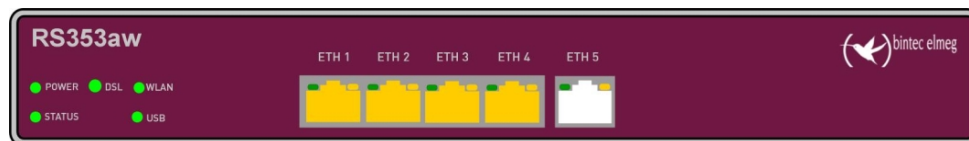


Fig. 9: Arrangement of the LEDs **bintec RS353aw**

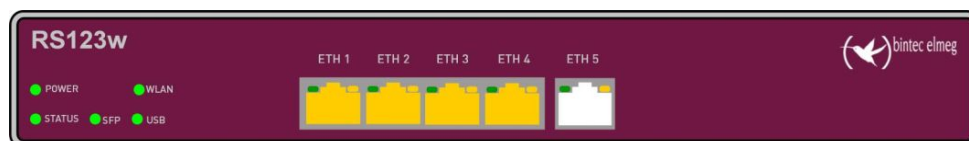


Fig. 10: Arrangement of the LEDs **bintec RS353aw**

### LED status display

LED	Colour	Status	Information
POWER	green	on	Power supply is connected.
		off	No power supply.
STATUS	green	on	After switching on: The device has started. During operation: An error has occurred.
	green	flashing	The device is active.
	green	off	During operation: An error has occurred.
DSL (RS353a, RS353aw)	green	on	Connection established.
	green	slow flashing	Synchronisation running.
		off	No Synchronisation.
SFP (RS123, RS123w)	green	flickering	Data transfer.
		off	No connection.
		flashing	Data traffic via SFP interface.
WLAN (RS123w, RS353aw)	green	on	WLAN connection established.
	green	off	Radio or all assigned VSS inactive
	green	on (slowly flashing)	VSS is active, no client connected
	green	on (fast flashing)	VSS is active, at least one client connected
USB	green	on (flickering)	VSS is active, at least one client connected, active data traffic
	green	flashing	Data traffic via USB send / receive.
		off	No USB connection.
LAN 1 bis 4 (Link/Act)	green	on	Ethernet connection established.
	green	flashing	Data traffic via Ethernet.
		off	No Ethernet connection.
LAN 1 bis 4 (Speed)	green	on	1000 Mbits transfer rate.
	orange	on	100 Mbits transfer rate.
		off	10 Mbits transfer rate.

LED	Colour	Status	Information
LAN 5 (Link/Act)	green	on	WAN-Ethernet connection established.
	green	flashing	Data via LAN 5 send / receive.
		off	No Ethernet connection.
LAN 5 (Speed)	green	on	The device is connected to the WAN at 1000 Mbits.
	orange	on	The device is connected to the WAN at 100 Mbits.
		off	The device is connected to the WAN at 10 Mbits, or no Data transfer.

You can determine the status of the router in BRRP operation with the aid of the status LED.

#### LED BRRP-Anzeige

LED	Colour	Status	Information
STATUS	green	flashing	The device is functioning as a master router.
STATUS	green	Heartbeat (on - on - off)	The device is functioning as a backup router.

### 1.2.4 Scope of supply

Your device is supplied with the following parts:

#### bintec RS123 and bintec RS123w

Scope of supply	bintec RS123	bintec RS123w
Cable sets/mains unit/ other	Ethernet cable (yellow) ISDN cable (black) Power cable 19" Mounting frame Screws	Ethernet cable (yellow) ISDN cable (black) Power cable 19" Mounting frame Screws 2 external WLAN antenna
Documentation	Safety notices Installation poster	Safety notices Installation poster
Online documentation	User's Guide	User's Guide



Scope of supply	bintec RS123	bintec RS123w
	Workshops	Workshops
	MIB reference	MIB reference

### bintec RS353a and bintec RS353aw

Scope of supply	bintec RS353a	bintec RS353aw
Cable sets/mains unit/ other	Ethernet cable (yellow) xDSL cable type 2 (gray) ISDN cable (black) Power cable 19" Mounting frame Screws	Ethernet cable (yellow) xDSL cable type 2 (gray) ISDN cable (black) Power cable 19" Mounting frame Screws 2 external WLAN antenna
Documentation	Safety notices Installation poster	Safety notices Installation poster
Online documentation	User's Guide Workshops MIB reference	User's Guide Workshops MIB reference

## 1.2.5 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 RS123 , bintec RS123w, bintec RS353a and bintec RS353aw
Dimensions and weights:	
Equipment dimensions without cable (B x H x D):	240 mm x 42 mm x 180 mm
Weight	approx. 1,100 g
Transport weight (incl. documentation, cables, packaging)	approx. 1600 g

<b>Property</b>	<b>bintec RS123 , bintec RS123w, bintec RS353a and bintec RS353aw</b>
Memory	128 MB RAM, 32 MB Flash-ROM
LEDs	17 (1x Power, 1x Status, 5x2 Ethernet, 5x Function) for devices with WLAN <b>RS123w</b> and <b>RS353aw</b>  16 (1x Power, 1x Status, 5x2 Ethernet, 4x Function) for devices without WLAN <b>RS123w</b> and <b>RS353aw</b>
Power consumption of the device	4.7 Watt
Voltage supply	AC 100 bis 240 V, 50 bis 60 Hz
Environmental requirements:	
Storage temperature	-25 °C to +70 °C
Operating temperature	0 °C to +40 °C
Relative atmospheric humidity	10 % to 95 % (non-condensing)
Room classification	Only use in dry rooms.
Available interfaces:	
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, Auto MDIX
Gigabit LAN/WAN Port	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, Auto MDIX
VDSL2/ADSL2+	Internal VDSL2/ADSL2+ modem for Annex A ( <b>RS353a</b> and <b>RS353aw</b> )
SFP LAN Port	SFP Slot for common optical 1000 mbps Ethernet SFP modules ( <b>RS123</b> and <b>RS123w</b> )
USB Port	USB2.0 type A
USB Console (Type B)	Supported Baud rates: 1200-115200 (default: 115200 Baud)
Standards & Guidelines	R&TTE Directive 1999/5/EC  CE symbol for all EU states
SAFERNET TM Security Technology	Community passwords, PAP, CHAP, MS-CHAP, MS-CHAP v.2, PPTP, PPPoE, PPPoA, Callback, Access Control Lists, CLID, NAT, SIF, MPPE Encryption, PPTP Encryption, VPN with PPTP or IPSec

### Antennas and sockets

Property	bintec RS123	bintec RS123w	bintec RS353a	bintec RS353aw
WLAN interface	-	802.11a/b/g/h; 802.11n 2.4 GHz	-	802.11a/b/g/h; 802.11n 2.4 GHz

Property	bintec RS123	bintec RS123w	bintec RS353a	bintec RS353aw
(antennas)		and 5 GHz; 2 TX, 2 RX (2x2) Channel level (2.4 GHz / 5GHz) RSMA socket		and 5 GHz; 2 TX, 2 RX (2x2) Channel level (2.4 GHz / 5GHz) RSMA socket
Available sockets:				
Ethernet interface	RJ45 socket (yellow)	RJ45 socket (yellow)	RJ45 socket (yellow)	RJ45 socket (yellow)
Ethernet interface	RJ45 socket (white)	RJ45 socket (white)	RJ45 socket (white)	RJ45 socket (white)
DSL	-	-	RJ45 socket (gray)	RJ45 socket (gray)
USB	USB-Anschluss type A	USB-Anschluss type A	USB-Anschluss type A	USB-Anschluss type A
USB Console	USB socket type B	USB socket type B	USB socket type B	USB socket type B

## 1.2.6 Reset

If the configuration is incorrect or if your device cannot be accessed, you can reset the device to the ex works standard settings using the Reset button on the back of the device. All the existing data will be deleted if you do this.

Proceed as follows:

- (1) Switch off your device.
- (2) Press the **Reset** button on your device.
- (3) Keep the **Reset** button on your device pressed down and switch the device back on.
- (4) After the *Status* LED has flashed five times, release the **Reset** button.



### Note

If you delete the boot configuration via the **GUI** (menu **Maintenance->Software & Configuration**) all passwords are also reset and the current boot configuration is 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 25

## 1.3 Support information

If you have any questions about your new product, please contact a local, certified retailer for prompt technical support. Resellers have been trained by us and receive privileged support. Further information on our support and service offers can be found on our web site at [www.bintec-elmeg.com](http://www.bintec-elmeg.com).

## 1.4 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.

## 1.5 Pin Assignments

### 1.5.1 USB console interface

The devices have a USB console connection for connecting to a console. This supports Baud rates from 1200 to 115200 Bps.

The interface is executed as a standard USB Type B socket.

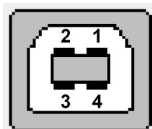


Fig. 11: USB Type B socket

The pin assignment is as follows:

#### Pin assignment in USB Type B socket

Pin	Position
1	Vbus
2	D-
3	D+
4	GND
Shell	Shield

**Note**

You may need a serial to USB driver for the CP210x component. You can download it from [www.bintec-elmeg.com](http://www.bintec-elmeg.com).

## 1.5.2 Ethernet interface

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

The connection is made via an RJ45 connector (yellow). The devices also have a fifth Ethernet interface (white).

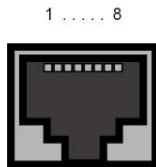


Fig. 12: 10/100/1000 Base-T Ethernet interface (RJ45 connector)

The pin assignment for the 10/100/1000 Base-T Ethernet interface (RJ45 connector) is as follows:

### RJ45 socket for LAN connection

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

## 1.5.3 xDSL interface

The xDSL interface is connected via an RJ45 plug.

Only the two inner pins are used for the xDSL connection.

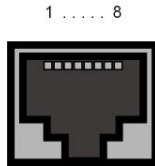


Fig. 13: xDSL interface (RJ45)

The pin assignment for the xDSL interface (RJ45 socket) is as follows:

#### RJ45 socket for xDSL connection

Pin	Position
1	Not used
2	Not used
3	Not used
4	a
5	b
6	Not used
7	Not used
8	Not used

### 1.5.4 ISDN S0 port

Some devices have an ISDN-BRI(S0) interface, which can be used for backup functions, for example.

The connection is made via an RJ45 connector (black).

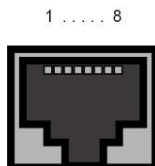


Fig. 14: ISDN S0 BRI interface (RJ45 socket)

The pin assignment for the ISDN S0 BRI interface (RJ45 socket) is as follows:

#### RJ45 socket for ISDN connection

Pin	Position
1	Not used

Pin	Position
2	Not used
3	Transmit (+)
4	Receive (+)
5	Receive (-)
6	Transmit (-)
7	Not used
8	Not used

### 1.5.5 USB interface

The devices have a USB connection for connecting a UMTS stick.

The interface is executed as a standard USB Type A socket.



Fig. 15: USB Type A socket


The pin assignment is as follows:

#### Pin assignment in USB Type A socket


Pin	Position
1	Vbus
2	D-
3	D+
4	GND
Shell	Shield

## 1.6 Inserting the SIM card

Proceed as follows to insert the SIM card:

- Access the card slot at the bottom of the device by removing the screw from the cover cap and removing the cap. Push the card lock in the direction of the arrow  and lift the card slot slightly.
- Make sure that 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 up-

wards.

- Close the card slot. Press the card slot downwards again.
- Push the card lock in the direction of the arrow . You will hear a click as the card locks into place.

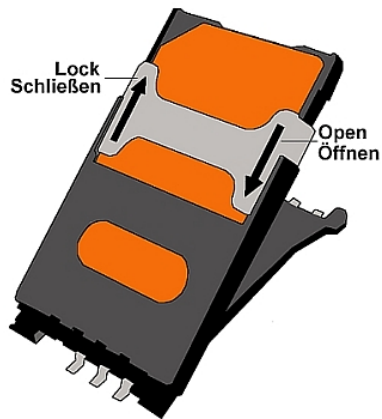


Fig. 16: SIM card



## Chapter 2 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, how to perform configuration for a conventional ADSL connection, 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 on-line help system gives you extra support.

### 2.1 Presettings

#### 2.1.1 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 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. 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 30.

Furthermore, the device is factory configured as a DHCP server so that it can provide PCs on your LAN that have no IP configuration with all the information required for a connection. Steps for setting up of your PC to automatically obtain an IP configuration are described in [Configuring a PC](#) on page 29.

**Note**

If you already run a DHCP server on your LAN, it is recommended that you configure the device on a separate PC that is not connected to your LAN.

The following settings are transferred to a non-configured PC:

- a suitable IP address for configuration of the device (IP address in the range 192.168.0.10 to 192.168.0.49 are assigned)
- the corresponding netmask (255.255.255.0)
- the IP address of the device as standard gateway and standard DNS server.

## 2.1.2 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 33.

## 2.2 System requirements

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

- Suitable operating system (Windows, Linux, MAC OS)
- A web browser (Internet Explorer, Firefox, Chrome) in the current version
- Installed network card (Ethernet)
- Installed TCP/IP protocol
- High colour display (more than 256 colours) for correct representation of the graphics.

## 2.3 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.

### 2.3.1 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).

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	<i>192.168.0.254</i>	
Netmask of your gateway	<i>255.255.255.0</i>	

#### Internet access over ADSL

If you want to set up Internet access, you need an Internet Service Provider (ISP). You also receive your personal access data from your ISP. The terms used for the required access data may vary from provider to provider, However, the type of information you need for dial-in is basically the same.

The following table lists the access data that your device also needs for a DSL connection to the Internet.

##### Data for internet access over ADSL

Access data	Example value	Your values
Provider name	<i>GoInternet</i>	
Protocol	<i>PPP over Ethernet (PPPoE)</i>	
Encapsulation	<i>bridged-no-fcs</i>	
VPI (Virtual Path Identifier)	<i>1</i>	
VCI (Virtual Circuit Identifier)	<i>32</i>	
Your user name	<i>MyName</i>	
Password	<i>TopSecret</i>	

Some Internet Service Providers, such as T-Online, require additional information:

#### Additional information for T-Online

Access data	Example value	Your values
User account (12 digits)	<i>000123456789</i>	
T-Online number (usually 12 digits)	<i>06112345678</i>	
Joint user account	<i>0001</i>	



#### Note

To configure T-Online Internet access, enter the following succession of numbers without intervening spaces in the **User Name** field: User account (12 digits) + T-Online number (usually 12 digits) + co-user number (for the main user, always 0001). If your T-Online number is less than 12 digits long, a "#" character is required between the T-Online number and the co-user number. If you use T-DSL, you must add the character string "@t-online.de" at the end of this string of numbers. Your user name could, for example, look like this: 00012345678906112345678#0001@t-online.de

#### Internet access over UMTS/LTE

The following table lists the access data that you need for an internet connection over UMTS/LTE.

#### Data for internet access over UMTS/LTE

Access data	Example value	Your values
UMTS/LTE PIN	<i>Obtained from your provider</i>	
Access point (APN)	<i>UMTS/LTE</i>	
Login name	<i>MyName</i>	

Access data	Example value	Your values
Password	<i>TopSecret</i>	

### Wireless LAN (optional)

You can operate your device as an access point and therefore connect individual work stations (e.g. laptops, PCs with wireless card or wireless adapter) by wireless connections to your local network via WLAN (Wireless LAN) and let them communicate with each other. The table "Data for the Wireless LAN configuration" shows the information required.

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.

Note the following:

- Follow the safety precautions when configuring your WLAN.
- Please also read **Sicherheit im Funk-LAN** [Security in Wireless LAN] published by the Federal Office for Information Security, see <http://www.bsi.de>.

#### Data for the Wireless LAN configuration

Access data	Example value	Your values
Preshared key for WPA2-PSK	without default	
Installation location of your system	<i>Germany</i>	
Channel to be used for WLAN	<i>11</i>	
Network name (SSID) for your WLAN	without default	
Visibility of the SSID in the wireless network	<i>not visible</i>	
Security setting	<i>WPA2-PSK</i>	

### 2.3.2 Configuring a PC

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

Have the device assign an IP address to your PC as follows:

- (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) Select **Internet Protocol (TCP/IP)** and click **Properties**.
- (5) Choose **Determine IP address automatically**.
- (6) Also choose **Determine DNS server address automatically**.

If you now close all windows with **OK**, the device transfers a suitable IP configuration to your PC, which then meets all the prerequisites for configuring your device. Likewise, once internet access has been set up, the computer can access the internet via the device.



#### Note

You can now launch **GUI** for configuration by entering the IP address of your device (192.168.0.254) in a supported browser (Internet Explorer 6 or 7, Mozilla Firefox version 1.2 or later) and entering the pre-configured login information ( **User:** *admin*, **Password:** *admin*).

### 2.3.3 Modify system password

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. 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.

## 2.4 Setting up an internet connection

You can set up different types of Internet connections using your device. The most common configurations are described below. The **GUI** Internet wizard can be used to help configure alternative configuration types.

### 2.4.1 Internet connection over internal xDSL modem

Apart from **bintec RS123** and **bintec RS123w**, all devices in the **RS series** have an integrated xDSL modem for rapid Internet access set-up. To make it easier to configure an xDSL internet connection, the **GUI** has a wizard to guide you through the connection set-up process simply and quickly. A selection of preconfigured connections from leading providers makes configuration even easier.

- (1) In **GUI** select the **Assistants->Internet Access** menu.
- (2) With **New** make a new entry and take over the **Connection Type** *Internal ADSL Modem*.
- (3) Follow the steps shown by the wizard. The wizard has its own online help, which offers all of the information you may require.
- (4) Once you have exited the wizard, save the configuration by clicking on the **Save configuration** button above the menu navigation.

### 2.4.2 Internet connection over UMTS/LTE

Setting up an Internet connection (if your device supports UMTS/LTE connections) over UMTS/LTE requires an activated SIM card for your UMTS/LTE provider. Insert the card as described in *Inserting the SIM card* on page 23.

- (1) In **GUI** select the **Assistants->Internet Access** menu.
- (2) Click **New** to create a new entry and as **Connection Type** select *UMTS/LTE*.
- (3) Follow the steps shown by the wizard. The wizard has its own online help, which offers all of the information you may require.
- (4) Once you have exited the wizard, save the configuration by clicking on the **Save configuration** button above the menu navigation.

### 2.4.3 Other internet connections

In addition to an ADSL connection over the internal ADSL2+ modem or a UMTS/LTE connection, you can connect your device over other connection types with the internet or over an external modem (e.g. a cable modem) or an external gateway. The corresponding wizard in **GUI** provides support for configurations of this type. You can find the Internet wizards and other wizards for easy configuration of various applications at the top of the menu tree under **Assistants**.

### 2.4.4 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. In the Windows Start menu, click **Run** and enter `ping` followed by a space and then the IP address of your device (e.g. `192.168.0.254`). A window appears with the response "Reply from...".
- (2) Test the internet access by entering [www.bintec-elmeg.com](http://www.bintec-elmeg.com) in the internet browser. bintec elmeg GmbH's Internet site offers you the latest news, updates and documentation.



#### 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).

## 2.5 Setting up wireless LAN

Proceed as follows to use your device (if your device supports WLAN) as an access point:

- (1) In **GUI** select the **Assistants->Wireless LAN** menu.
- (2) Follow the steps shown by the wizard. The wizard has its own online help, which offers all of the information you may require.
- (3) 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.

## 2.6 Software Update

The range of functions of bintec elmeg devices is continuously being extended. These extensions are made available to you by bintec elmeg GmbH free of charge. Checking for new software versions and the installation of updates can be carried out easily with the **GUI**. 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.10.1 Rev. 4 IPv6, IPSec from 2015/05/07 00:00:00
System Logic	1.0
ADSL Logic	2.5.1.10.0.2
Software and Configuration Options	
Action	Update system software ▾
Source Location	Current Software from Update Server ▾

**Start**

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 3 Access and configuration

This chapter describes all the access and configuration options.

### 3.1 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 console interface
- Via an ISDN connection if your device supports ISDN)

#### 3.1.1 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.

##### 3.1.1.1 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`

##### 3.1.1.2 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 41.

### 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 41.

### 3.1.1.3 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 40).
- (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 43).
- (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 40.

### 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 40.



#### 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.

## 3.1.2 Access via the Console Interface

Each bintec elmeg gateway has a console interface, with which a PC can be connected directly. Access via the console 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 console connection, e.g. HyperTerminal. You can use any other terminal program that can be set to the corresponding parameters (see below).

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

Check the settings used to connect to the console interface:

The following settings are necessary:

- Bits per second: *115200*

- Data bits: *8*
- Parity: *open*
- Stopbits: *1*
- Flow control: *open*

## 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 -s 115200 -c/dev/ttyS1`

Example of a command line for using `tip`: `tip -115200 /dev/ttyS1`

### 3.1.3 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 console 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 41.

## 3.2 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.

### 3.2.1 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 <b>GUI</b> .
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`.

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 59.

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.

## 3.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in [Access Options](#) on page 35.

### 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**.

## 3.3 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, <b>GUI</b> , shell command
console 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.

### 3.3.1 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](http://www.bintec-elmeg.com) and installed on your device. To do this, proceed as described in *Options* on page 545.

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.

Automatic Refresh Interval <input type="text" value="60"/> Seconds <input type="button" value="Apply"/>		
<b>Warning: System Password not changed!</b>		
System Information		
Uptime	24 Day(s) 1 Hour(s) 57 Minute(s)	
System Date	Tuesday, 2000 Jan 25, 06:12:32	
Serial Number	SR6AAA009400008	
BOSS Version	V.9.1 Rev. 7 IPsec from 2013:08:01 00:00:00	
Last configuration stored	Sunday, 2000 May 21, 04:38:27	
Resource Information		
CPU Usage	0%	
Memory Usage	21.8/63.9 MByte (33%)	
ISDN Usage External	0 / 2 B Channels	
Active Sessions (SIF, RTP, etc...)	0	
Active IPsec Tunnels	0 / 0	
Physical Interfaces		
Interface	Connection Information	Link
en1-0	192.168.0.254 / 255.255.255.0	<input checked="" type="checkbox"/>
en1-4	Not configured / Not configured	<input type="checkbox"/>
WLAN1	Off	<input type="checkbox"/>
bri-0	Not configured	<input type="checkbox"/>
ADSL	<input type="text" value="0"/> kbps Downstream	<input type="checkbox"/>
	<input type="text" value="0"/> kbps Upstream	
WAN Interfaces		
Description	Connection Information	Link

Fig. 17: GUI home page

### 3.3.1.1 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 29).
- (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 53).

### 3.3.1.2 Operating elements

#### GUI window

The GUI window is divided into three areas:

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

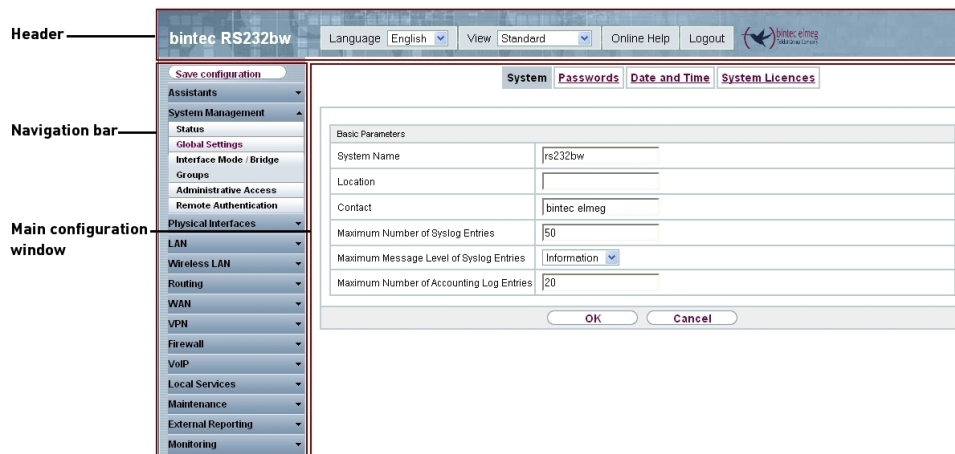


Fig. 18: Areas of the GUI

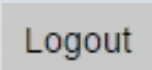
## Header



Fig. 19: GUI header

## GUI header

Menu	Position
Language English	<b>Language:</b> 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.
View Full Access	<b>View:</b> Select the desired view from the dropdown menu. Standard and SNMP browsers can be selected.
Online Help	<b>Online Help:</b> Click this button if you want help with the menu now active. The description of the sub-menu where you are now

Menu	Position
	is displayed.
	<p><b>Logout:</b> If you want to end the configuration, click this button to log out of your device. A window is opened offering you the following options:</p> <ul style="list-style-type: none"> <li>• Save configuration, save previous boot configuration, then exit.</li> <li>• Save configuration, then exit.</li> <li>• Exit without saving.</li> </ul>

### Navigation bar



Fig. 20: Save Configuration button

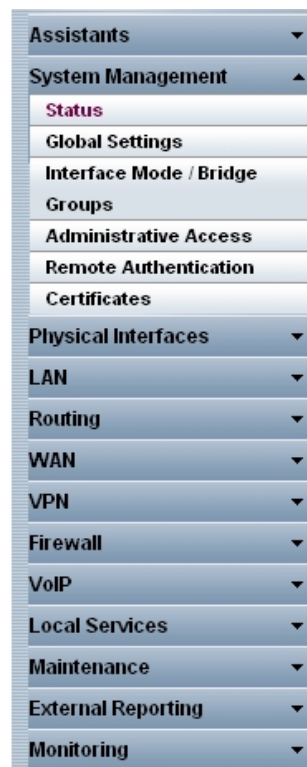


Fig. 21: Menus

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


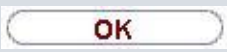
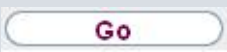


The sub-menus generally contain several pages. These are called using the buttons at the top of the main window. If you click a button, the window is opened with the basic parameters. You can extend this by clicking the **Advanced Settings** tab, which displays the additional options.

### Configuration elements


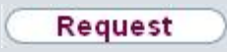


The various actions that you can perform when configuring your device in the **GUI** are triggered by means of the following buttons:

#### GUI buttons

Button	Position
	Updates the view.








Button	Position
	If you do not want to save a newly configured list entry, cancel this and any settings made by pressing <b>Cancel</b> .
	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 <b>System Management-&gt;Certificates-&gt;Certificate List</b> menu and the <b>System Management-&gt;Certificates-&gt;CRLs</b> menu, this button activates the sub-menus for configuration of the certificate or CRL imports.
	In the <b>System Management-&gt;Certificates-&gt;Certificate List</b> menu, this button activates the sub-menu for the configuration of the certificate request.
	In the <b>Monitoring-&gt;ISDN/Modem-&gt;Current Calls</b> 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> .

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



Menu	Position
	ing list entry directly in the list.

Automatic Refresh Interval  Seconds

Fig. 22: Configuration of the update interval




View  per page

Fig. 23: Filter list

### Structure of the GUI configuration menu



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



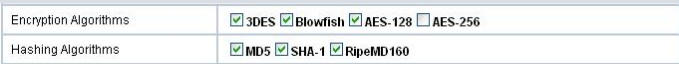

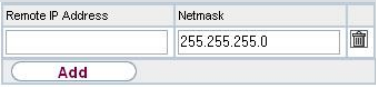

#### GUI Menu architecture

Menu	Position
Basic configuration menu/list	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.  The menu contains either a list of all the configured entries or the basic settings for the function concerned.
Sub-menu 	The <b>New</b> 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	e.g. empty text field  Text field with hidden input 

Menu	Position
	Enter the data.
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> 
Dropdown menus	<p>e.g.</p>  <p>Click the arrow to open the list. Select the required option using the mouse.</p>
Internal lists	<p>e.g.</p>  <p>Click <b>Add</b>. A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm with <b>OK</b>. 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.

### 3.3.1.3 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](http://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!

### 3.3.2 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.

## Chapter 4 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 5 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.

### 5.1 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	60	Seconds	<input type="button" value="Apply"/>
<b>Warning: System Password not changed!</b>			
System Information			
Uptime	24 Day(s) 1 Hour(s) 57 Minute(s)		
System Date	Tuesday, 2000 Jan 25, 06:12:32		
Serial Number	SR6AAA009400008		
BOSS Version	V.9.1 Rev. 7 IPsec from 2013:08:01 00:00:00		
Last configuration stored	Sunday, 2000 May 21, 04:38:27		
Resource Information			
CPU Usage	0%		
Memory Usage	21.8/63.9 MByte (33%)		
ISDN Usage External	0 / 2 B Channels		
Active Sessions (SIF, RTP, etc...)	0		
Active IPsec Tunnels	0 / 0		
Physical Interfaces			
Interface	Connection Information		Link
en1-0	192.168.0.254 / 255.255.255.0		
en1-4	Not configured / Not configured		
WLAN1	Off		
bri-0	Not configured		
ADSL	0	kbps Downstream	
	0	kbps Upstream	
WAN Interfaces			
Description	Connection Information		Link

Fig. 24: System Management->Status

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

#### Fields in the System Information menu.

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

#### Fields in the Resource Information menu.

Field	Value
<b>CPU Usage</b>	Displays the CPU usage as a percentage.
<b>Memory Usage</b>	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is

Field	Value
	also displayed in brackets as a percentage.
<b>ISDN Usage External</b>	Shows the number of active B channels and the maximum number of available B channels for external connections.
<b>Active Sessions (SIF, RTP, etc... )</b>	Displays the total of all SIF, TDRRC, and IP load balancing sessions.
<b>Active IPsec Tunnels</b>	Displays the number of currently active IPsec tunnels in relation to the number of configured IPsec tunnels.

#### Fields in the Physical Interfaces menu.

Field	Value
<b>Interface - Connection Information - Link</b>	<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><b>Connection Information</b> for Ethernet interfaces:</p> <ul style="list-style-type: none"> <li>• IP address</li> <li>• Netmask</li> </ul> <p><b>Connection Information</b> for ISDN interfaces:</p> <ul style="list-style-type: none"> <li>• Configured</li> <li>• Not configured</li> </ul> <p><b>Connection Information</b> for xDSL interfaces:</p> <ul style="list-style-type: none"> <li>• Downstream/Upstream Line Speed</li> </ul> <p><b>Connection Information</b> for WLAN interfaces:</p> <p>Access Point Mode:</p> <ul style="list-style-type: none"> <li>• Operation Mode: Access Point or Off</li> <li>• The channel used on this wireless module</li> <li>• Number of connected clients</li> <li>• Number of WDS links</li> <li>• Software version of the wireless card</li> </ul> <p><b>Connection Information</b> for UMTS/LTE interfaces:</p> <ul style="list-style-type: none"> <li>• <i>SIM insert required</i> appears if no SIM card is inserted.</li> </ul>

Field	Value
	<ul style="list-style-type: none"> <li>• <i>PIN input required</i> is displayed if the SIM card is inserted, but the PIN has not yet been entered.</li> <li>• <i>Init</i> is displayed while the SIM card is initialized.</li> <li>• If the SIM card is operational, the <b>Network Quality</b> is displayed.</li> </ul>

#### Fields in the WAN Interfaces menu.

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

## 5.2 Global Settings

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

### 5.2.1 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	<input type="text" value="w2003ac"/>
Location	<input type="text"/>
Contact	<input type="text" value="BINTECELMEG"/>
Maximum Number of Syslog Entries	<input type="text" value="50"/>
Maximum Message Level of Syslog Entries	Information ▾
Maximum Number of Accounting Log Entries	<input type="text" value="20"/>
Cloud NetManager communication	<input checked="" type="checkbox"/> Enabled
Cloud NetManager address	<input type="text" value="https://discover.networkcloud"/>
LED mode	Status ▾
Show Manufacturer Names	<input checked="" type="checkbox"/> Enabled

Fig. 25: **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
<b>System Name</b>	<p>Enter the system name of your device. This is also used as the PPP host name.</p> <p>A character string with a maximum of 255 characters is possible.</p> <p>The device type is entered as the default value.</p>
<b>Location</b>	Enter the location of your device.
<b>Contact</b>	<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>
<b>Maximum Number of Syslog Entries</b>	<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 <b>Monitoring-&gt;Internal Log</b>.</p>
<b>Maximum Message Level of Syslog Entries</b>	<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"> <li>• <i>Emergency</i>: Only messages with emergency priority are recorded.</li> <li>• <i>Alert</i>: Messages with emergency and alert priority are recorded.</li> </ul>

Field	Value
	<ul style="list-style-type: none"> <li>• <i>Critical</i>: Messages with emergency, alert and critical priority are recorded.</li> <li>• <i>Error</i>: Messages with emergency, alert, critical and error priority are recorded.</li> <li>• <i>Warning</i>: Messages with emergency, alert, critical, error and warning priority are recorded.</li> <li>• <i>Notice</i>: Messages with emergency, alert, critical, error, warning and notice priority are recorded.</li> <li>• <i>Information</i> (default value): Messages with emergency, alert, critical, error, warning, notice and information priority are recorded.</li> <li>• <i>Debug</i>: All messages are recorded.</li> </ul>
<b>Maximum Number of Accounting Log Entries</b>	<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>
<b>Cloud NetManager communication</b>	<p>Only for devices with support for being managed by the Cloud NetManager.</p> <p>Enable or disable the option <b>Cloud NetManager communication</b></p> <p>The function is enabled by default.</p>
<b>Cloud NetManager address</b>	<p>Only for devices with support for being managed by the Cloud NetManager.</p> <p>The address of the bintec elmeg Cloud NetManager is preconfigured. If you want to run your own management system, you need to enter the address of your server here.</p>
<b>Manual WLAN Controller IP Address</b>	<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>

Field	Value
<b>LED mode</b>	<p>Only for WLAN devices</p> <p>Select the LEDs' lighting behaviour.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Status</i> (default value): The LEDS display their default behaviour.</li> <li>• <i>Flashing</i>: Only the status LED flashes once per second.</li> <li>• <i>Off</i>: All LEDs are disabled.</li> </ul>
<b>Show Manufacturer Names</b>	<p>Here you can determine if the manufacturer part of a MAC address is to be "translated". The manufacturer part takes up to eight characters at the beginning of the MAC address. Instead of, e.g., <code>00:a0:f9:37:12:c9</code>, <code>BintecCo_37:12:c9</code> is displayed if this option is enabled.</p>

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

Field	Value
<b>Power Off Timeout</b>	<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 <code>900</code> seconds.</p>

## 5.2.2 Passwords

Setting the passwords is another basic system setting.

Fig. 26: **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
<b>System Admin Password</b>	Enter the password for the user name <code>admin</code> .  This password is also used with SNMPv3 for authentication (MD5) and encryption (DES).
<b>Confirm Admin Password</b>	Confirm the password by entering it again.

#### Fields in the SNMP Communities menu.

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

Field	Value
munity	

#### Fields in the Global Password Options menu

Field	Value
<b>Show passwords and keys in clear text</b>	<p>Define whether the passwords are to be displayed in clear text (plain text).</p> <p>The function is enabled with <i>Show</i></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 <b>OK</b> or call the menu again, they are displayed as asterisks.</p>

### 5.2.3 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	<input type="checkbox"/> Enabled						
Time Settings (GPS)							
Time Update Interval	<input type="checkbox"/> Enabled						
				OK		Cancel	

Fig. 27: 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

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
<b>Time Zone</b>	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> .
<b>Current Local Time</b>	The current date and current system time are shown here. The entry cannot be changed.

#### Fields in the menu **Manual Time Settings**

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

**Fields in the menu Automatic Time Settings (Time Protocol)**

Field	Description
<b>ISDN Timeserver</b>	<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>
<b>First Timeserver</b>	<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"> <li>• <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123.</li> <li>• <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37.</li> <li>• <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37.</li> <li>• <i>None</i>: This time server is not currently used for the time request.</li> </ul>
<b>Second Timeserver</b>	<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"> <li>• <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123.</li> <li>• <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37.</li> <li>• <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37.</li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• <i>None</i>: This time server is not currently used for the time request.</li> </ul>
<b>Third Timeserver</b>	<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"> <li>• <i>SNTP</i> (default value): This server uses the simple network time protocol via UDP port 123.</li> <li>• <i>Time Service / UDP</i>: This server uses the Time service with UDP port 37.</li> <li>• <i>Time Service / TCP</i>: This server uses the Time service with TCP port 37.</li> <li>• <i>None</i>: This time server is not currently used for the time request.</li> </ul>
<b>Time Update Interval</b>	<p>Enter the time interval in minutes at which the time is automatically updated.</p> <p>The default value is <i>1440</i>.</p>
<b>Time Update Policy</b>	<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"> <li>• <i>Normal</i> (default value): The system attempts to contact the time server after 1, 2, 4, 8, and 16 minutes.</li> <li>• <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.</li> <li>• <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.</li> </ul> <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 <b>Time Update Policy</b>, select the value <i>Endless</i>.</p>

Field	Description
<b>Internal Time Server</b>	<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
<b>Time Update Interval</b>	<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>

## 5.2.4 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](http://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](http://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).

#### 5.2.4.1 Edit or New

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

The screenshot shows a navigation bar with tabs: System, Passwords, Date and Time, Timer, and System Licences (selected). Below the tabs is a form titled 'Basic Settings' with two input fields: 'Licence Serial Number' and 'Licence Key'. At the bottom of the form are 'OK' and 'Cancel' buttons.

Fig. 28: **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
<b>Licence Serial Number</b>	Enter the licence serial number you received when you bought the licence.
<b>Licence Key</b>	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.

## 5.3 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 bridge link is made up of the following parts:

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

Example: *wds1-0* (first 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)

### 5.3.1 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:

Fig. 29: 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
<b>Interface Description</b>	Displays the name of the interface.
<b>Mode / Bridge Group</b>	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, 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 <b>OK</b> button.
<b>Configuration Interface</b>	Select the interface via which the configuration is to be carried out.  Possible values: <ul style="list-style-type: none"> <li>• <i>Select one</i> (default value): Ex works setting The right configuration interface must be selected from the other options.</li> <li>• <i>Ignore</i>: No interface is defined as configuration interface.</li> <li>• <i>&lt;Interface name&gt;</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.</li> </ul>

#### 5.3.1.1 Add

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

Fig. 30: **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 Wxxxxn and RS series


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


Fig. 31: **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
<b>Interface</b>	Shows the interface that is being edited.
<b>Wildcard Mode</b>	<p>Select the Wildcard mode you want to use on the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>none</i> (default value): Wildcard mode is not used.</li> <li>• <i>static</i>: With this setting, you must enter the MAC address of a device that is connected over IP under <b>Wildcard MAC Address</b>. Each packet without IP and without ARP is forwarded to this device. This occurs even when the device is no longer connected.</li> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Wildcard MAC Address</b>	<p>Only for <b>Wildcard Mode</b> = <i>static</i></p> <p>Enter the MAC address of a device that is connected over IP.</p>
<b>Transparent MAC Address</b>	<p>Only for <b>Wildcard Mode</b> = <i>static, first</i></p> <p>Choose whether or not the <b>Wildcard MAC Address</b> 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.

## 5.4 Administrative Access

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

### 5.4.1 Access

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

Access SSH SNMP

**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. 32: **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*.

For PABX systems only: You can also authorise your device for maintenance work from bintec elmeg's Customer Service department. To 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!

**Service Login (ISDN Web-Access)** is disabled by default.

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

**Fields in the menu Advanced Settings**

Field	Description
<b>Restore Default Settings</b>	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.

### 5.4.1.1 Add

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



Fig. 33: **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
<b>Interface</b>	Select the interface for which administrative access is to be configured.

### 5.4.2 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.

Access SSH SNMP

SSH (Secure Shell) Parameters	
SSH service active	<input checked="" type="checkbox"/> Enabled
SSH Port	22
Maximum number of concurrent connections	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 <a href="#">[Generate]</a>
Advanced Settings	
Login Grace Time	600 Seconds
Compression	<input type="checkbox"/> Enabled
TCP Keepalives	<input checked="" type="checkbox"/> Enabled
Logging Level	Information
<span>OK</span> <span>Cancel</span>	

Fig. 34: 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](http://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
<b>SSH service active</b>	Select whether the SSH Daemon is to be enabled for the inter-

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

#### Fields in the menu **Authentication and Encryption Parameters**

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

#### Fields in the menu **Key Status**

Field	Value
<b>RSA Key Status</b>	<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> <p>The status is <i>Not generated</i> by default.</p>
<b>DSA Key Status</b>	<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> <p>The status is <i>Not generated</i> by default.</p>

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

#### Fields in the menu **Advanced Settings**

Field	Value
<b>Login Grace Time</b>	<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>

Field	Value
<b>Compression</b>	<p>Select whether data compression should be used.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>TCP Keepalives</b>	<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>
<b>Logging Level</b>	<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"> <li>• <i>Information</i> (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded.</li> <li>• <i>Fatal</i>: Only fatal errors of the SSH Daemon are recorded.</li> <li>• <i>Error</i>: Fatal and simple errors of the SSH Daemon are recorded.</li> <li>• <i>Debug</i>: All messages are recorded.</li> </ul>

### 5.4.3 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.

Access SSH SNMP

Basic Settings	
SNMP Version	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> v3
SNMP Listen UDP Port	161
SNMP multicast discovery	<input checked="" type="checkbox"/> Enabled

OK Cancel

Fig. 35: **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
<b>SNMP Version</b>	<p>Select the SNMP version your device is to use to listen for external SNMP access.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>v1</i>: SNMP Version 1</li> <li>• <i>v2c</i>: Community-Based SNMP Version 2</li> <li>• <i>v3</i>: SNMP Version 3</li> </ul> <p>By default, <i>v1</i>, <i>v2c</i> and <i>v3</i> are enabled.</p> <p>If no option is selected, the function is deactivated.</p>
<b>SNMP Listen UDP Port</b>	<p>Shows the UDP port ( <i>161</i> ) at which the device receives SNMP requests.</p> <p>The value cannot be changed.</p>
<b>SNMP multicast discovery</b>	<p>Enable or disable the function <b>SNMP multicast discovery</b>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>



**Tip**

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

## 5.5 Remote Authentication

This menu contains the settings for user authentication.

### 5.5.1 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

Field	Value
	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.
ACCESS_REJECT	Server -> Client  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.
ACCOUNTING_START	Client -> Server  If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the start of each connection.
ACCOUNTING_STOP	Client -> Server  If a RADIUS server is used for accounting, your device sends an accounting message to the RADIUS server at the end of each connection.

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

### 5.5.1.1 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	<input checked="" type="checkbox"/> Enabled
Group Description	Default Group 0
Advanced Settings	
Policy	Authoritative
UDP Port	1812
Server Timeout	1000 <small>Milliseconds</small>
Alive Check	<input checked="" type="checkbox"/> Enabled
Retries	1
RADIUS Dialout	<input type="checkbox"/> Enabled Reload Interval: 0 <small>Seconds</small>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 36: 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
<b>Authentication Type</b>	Select what the RADIUS server is to be used for.  Possible values: <ul style="list-style-type: none"> <li>• <i>PPP Authentication</i> (default value only for PPP connections): The RADIUS server is used for controlling access to a network.</li> <li>• <i>Accounting</i> (for PPP connections only): The RADIUS server is used for recording statistical call data.</li> <li>• <i>Login Authentication</i>: The RADIUS server is used for controlling access to the SNMP shell of your device.</li> <li>• <i>IPSec Authentication</i>: The RADIUS server is used for sending configuration data for IPSec peers to your device.</li> </ul>

Field	Value
	<ul style="list-style-type: none"> <li>• <i>WLAN (802.1x)</i>: The RADIUS server is used for controlling access to a wireless network.</li> <li>• <i>XAUTH</i>: The RADIUS server is used for authenticating IPsec peers via XAuth.</li> </ul>
<b>Vendor Mode</b>	<p>Only for <b>Authentication Type</b> = <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"> <li>• <i>France Telecom</i>: For France Telecom hotspot applications.</li> <li>• <i>bintec HotSpot Server</i>: For hotspot applications.</li> </ul>
<b>Server IP Address</b>	Enter the IP address of the RADIUS server.
<b>RADIUS Secret</b>	Enter the shared password used for communication between the RADIUS server and your device.
<b>Default User Password</b>	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.
<b>Priority</b>	<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 0 (highest priority) to 7 (lowest priority).</p> <p>The default value is 0.</p> <p>See also <b>Policy</b> in the Advanced Settings.</p>
<b>Entry active</b>	<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>
<b>Group Description</b>	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 <b>Priority</b> and the <b>Policy</b> .</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>New</i> (default value): Enter a new group description in the text field.</li> <li>• <i>Default Group 0</i>: Select this entry for special applications, such as Hotspot Server configuration.</li> <li>• <i>&lt;Group Name&gt;</i>: Select a predefined group from the list.</li> </ul>

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

#### Fields in the **Advanced Settings** menu.

Field	Value
<b>Policy</b>	<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"> <li>• <i>Authoritative</i> (default value): A negative response to a request is accepted.</li> <li>• <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.</li> </ul>
<b>UDP Port</b>	<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>
<b>Server Timeout</b>	<p>Enter the maximum wait time between ACCESS_REQUEST and response in milliseconds.</p> <p>After timeout, the request is repeated according to <b>Retries</b> 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).
<b>Alive Check</b>	<p>Here you can activate a check of the accessibility of a RADIUS server in <b>Status</b> <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, <b>Status</b> 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>
<b>Retries</b>	<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 <b>Status</b> is set to <i>down</i>. In <b>Alive Check</b> = <i>Enabled</i> your device attempts to reach the server every 20 seconds. If the server responds, <b>Status</b> 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 <b>Status</b> being set to <i>down</i>, set this value to <i>0</i>.</p>
<b>RADIUS Dialout</b>	<p>Only for <b>Authentication Type</b> = <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"> <li>• <i>Reload Interval</i>: Enter the time period in seconds between update intervals.</li> </ul> <p>The default entry here is <i>0</i> i.e. an automatic reload is not car-</p>

Field	Value
	ried out.

## 5.5.2 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.

### 5.5.2.1 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	<input checked="" type="checkbox"/> Enabled

Advanced Settings	
Policy	Non-authoritative
TCP Port	49
Timeout	3 Seconds
Block Time	60 Seconds
Encryption	<input checked="" type="checkbox"/> Enabled

Fig. 37: 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
<b>Authentication Type</b>	<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"> <li><i>Login Authentication</i>: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.</li> </ul>
<b>Server IP Address</b>	Enter the IP address of the TACACS+ server that is to be requested for login authentication.
<b>TACACS+ Secret</b>	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.
<b>Priority</b>	Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login



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

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Policy</b>	<p>Select the interpretation of the TACACS+ response.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Non-authoritative</i> (default value): The TACACS+ servers are queried in order of their priority (see <b>Priority</b>) until a positive response is received or a negative response has been received from an authoritative server.</li> <li>• <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.</li> </ul>
<b>TCP Port</b>	<p>Shows the default TCP port ( 49) used for the TACACS+ protocol. The value cannot be changed.</p>
<b>Timeout</b>	<p>Enter time in seconds for which the NAS is to wait for a response from TACACS+.</p> <p>If a response is not received during the wait time, the next configured TACACS+ server is queried (only if <b>Policy</b> = <i>Non-authoritative</i>) and the status of the current server is set to <i>Blocked</i>.</p> <p>The possible values are 1 to 60, the default value is 3.</p>

Field	Description
<b>Block Time</b>	<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 <b>Entry active</b> field.</p> <p>The possible values are <i>0</i> to <i>3600</i>, the default value is <i>60</i>. The value <i>0</i> means that the server is never set to <i>Blocked</i> status and thus no other servers are queried.</p>
<b>Encryption</b>	<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>

### 5.5.3 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.

Fig. 38: **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
<b>Authentication for PPP Dialin</b>	<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"> <li>• <i>Inband</i>: Only inband RADIUS requests (PAP, CHAP, MS-CHAP V1 &amp; V2) (i.e. PPP requests without CLID) are sent to the RADIUS server defined in <b>Server IP Address</b>.</li> <li>• <i>Outband (CLID)</i> : Only outband RADIUS requests (i.e. requests for calling line identification = CLID) are sent to the RADIUS server.</li> </ul> <p><i>Inband</i> is enabled by default, <i>Outband (CLID)</i> is disabled by default.</p>



## 5.6 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.

### 5.6.1 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, the access profiles *TCC\_ADMIN*, *HOTEL*, *CHARGES*, *PHONEBOOK*, *PBX\_USER\_ACCESS* are preconfigured for PABX systems. You can change these using the icon  or reset them to the default settings using the icon .

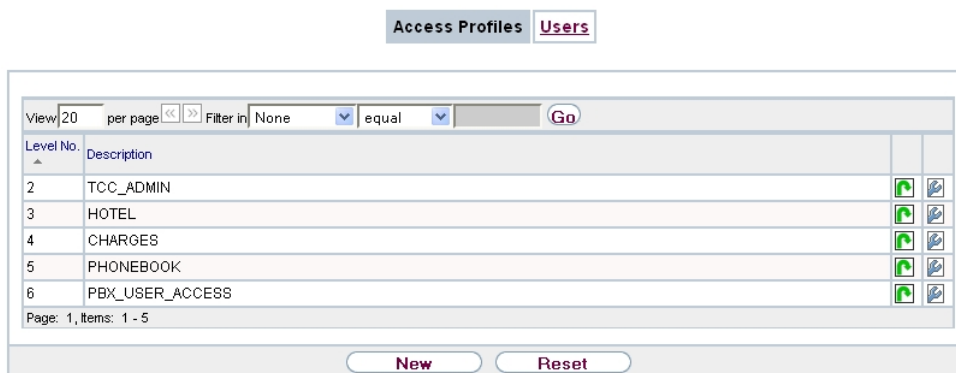


Fig. 39: System Management->Configuration Access->Access Profiles

### 5.6.1.1 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	<input style="width: 100%;" type="text"/>
Level No.	7
Buttons	
Save configuration	<input type="checkbox"/> Enabled
Switch to SNMP Browser	<input type="checkbox"/> Enabled
Navigation Entries	
<b>Assistants</b> ▲ ✖	
First steps ▼ ✖	
PBX ▼ ✖	
<b>System Management</b> ▼ ✖	
Physical Interfaces ▼ ✖	
VoIP ▼ ✖	
Numbering ▼ ✖	
Terminals ▼ ✖	
Call Routing ▼ ✖	
Applications ▼ ✖	
LAN ▼ ✖	
Networking ▼ ✖	
Firewall ▼ ✖	
VoIP ▼ ✖	
Local Services ▼ ✖	
Maintenance ▼ ✖	
External Reporting ▼ ✖	
Monitoring ▼ ✖	
User Access ▼ ✖	

OK Cancel



Fig. 40: **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
<b>Description</b>	Enter a unique name for the access profile.
<b>Level No.</b>	The system automatically assigns a sequential number to the access profile. This cannot be edited.


## Fields in the menu Buttons

Field	Description
<b>Save configuration</b>	<p>If you activate the button <b>Save configuration</b> the user is permitted to save configurations.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p><b>Note</b></p> <p>Note that the passwords in the saved file can be viewed in clear text.</p> </div> <p>Enable or disable <b>Save configuration</b>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>Switch to SNMP Browser</b>	<p>If you activate the button <b>Switch to SNMP Browser</b>, the user can switch to the SNMP browser view, access the parameters and modify all the settings displayed there.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p><b>Caution</b></p> <p>Note that the permission for <b>Switch to SNMP Browser</b> 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 <b>Save configuration</b>.</p> <p>With the permission for <b>Switch to SNMP Browser</b> you remove the configured GUI restrictions at the MIB level once more.</p> </div> <p>Enable or disable <b>Switch to SNMP Browser</b>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

## Fields in the menu Navigation Entries

Field	Description
<b>Menus</b>	<p>You see all the menus from the GUI's navigation bar. Menus that contain at least one sub-menu are flagged by  and . 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"> <li>• <i>Deny</i>: The menu and all its lower-level menus are blocked.</li> <li>• <i>Allow</i>: The menu is released. Lower-level menus may need to be specifically released.</li> <li>• <i>Allow all</i>: The menu and all its lower-level menus are released.</li> </ul> <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>

## 5.6.2 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 .

There are no preconfigured users.

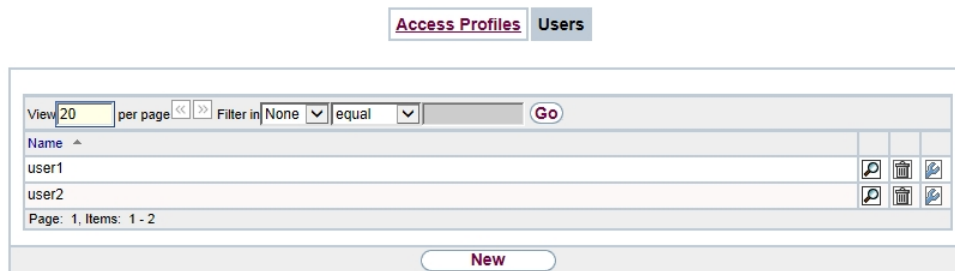



Fig. 41: **System Management->Configuration Access->Users**

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. 42: 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.

### 5.6.2.1 Edit or New


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

Fig. 43: 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
<b>User</b>	Enter a unique name for the user.
<b>Password</b>	Enter a password for the user.
<b>User must change password</b>	<p>The administrator can use the option <b>User must change password</b> to specify that the user must select their own password the first time they log in. To do this, the option <b>Save configuration</b> needs to be enabled in the menu <b>Access Profiles</b>. If this option is not enabled, a warning message displays.</p> <p>Enable or disable <b>User must change password</b>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>Access Level</b>	<p>Use <b>Add</b> to assign at least one access profile to the user. Selecting <b>Read-only</b> specifies that the user can view the parameters of the access profile, but not change them. Selecting <b>Read-only</b> is only possible if the option <b>Switch to SNMP Browser</b> in the menu <b>Access Profiles</b> is not enabled.</p> <p>If the option <b>Switch to SNMP Browser</b> 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 <b>Read-only</b> 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 <b>Read-only</b> . Buttons cannot be set to the setting <b>Read-only</b> .

## 5.7 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.

### 5.7.1 Certificate List


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

### 5.7.1.1 Edit

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

Certificate List CRLs Certificate Servers

Edit parameters	
Description	<input type="text" value="test"/>
Certificate is CA Certificate	<input checked="" type="checkbox"/> True
Certificate Revocation List (CRL) Checking	<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
Force certificate to be trusted	<input type="checkbox"/> True
View details	
<pre> Certificate =   SerialNumber = 11   SubjectName = &amp;lt;CN=r1200_aw, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE&amp;gt;   IssuerName = &amp;lt;CN=linuxCA, OU=Support, O=Teldat GmbH, ST=Bavaria, C=DE&amp;gt;   Validity =     NotBefore = 2006 Sep 15th, 07:07:49 GMT     NotAfter = 2008 Sep 14th, 07:07:49 GMT   PublicKeyInfo =     Algorithm name (X.509) : rsaEncryption     Modulus n (1024 bits) :       1657430007353061929971175628985365836058592284552111716307381855989730994       4241959750497426343375890536490502929548450998243448632595011570952551767       7011616656908963216398179133323977323187771274664312501085550617414306630       0411834850766905090689578661769721208181141085359073369329733126120426693       320106097890434357773     Exponent e ( 17 bits) : 65537   Extensions =     Available = key usage, basic constraints   KeyUsage = DigitalSignature NonRepudiation KeyEncipherment   BasicConstraints =     cA = FALSE           </pre>	
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	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 44: **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
<b>Description</b>	Shows the name of the certificate, key, or request.
<b>Certificate is CA Certificate</b>	<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>
<b>Certificate Revocation List (CRL) Checking</b>	<p>Only for <b>Certificate is CA Certificate</b> = <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"> <li>• <i>Disabled</i>: No CRLs check.</li> <li>• <i>Always</i>: CRLs are always checked.</li> <li>• <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.</li> <li>• <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".</li> </ul>
<b>Force certificate to be trusted</b>	<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.

### 5.7.1.2 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 List CRLs Certificate Servers

Certificate Request	
Certificate Request Description	<input type="text"/>
Mode	<input checked="" type="radio"/> Manual <input type="radio"/> SCEP
Generate Private Key	RSA <input type="text"/> 1024 <input type="text"/> Bits
Subject Name	
Custom	<input type="checkbox"/> Enabled
Common Name	<input type="text"/>
E-mail	<input type="text"/>
Organizational Unit	<input type="text"/>
Organization	<input type="text"/>
Locality	<input type="text"/>
State/Province	<input type="text"/>
Country	<input type="text"/>
Advanced Settings	
Subject Alternative Names	
#1	None <input type="text"/>
#2	None <input type="text"/>
#3	None <input type="text"/>
Options	
Autosave Mode	<input checked="" type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 45: 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
<b>Certificate Request Description</b>	Enter a unique description for the certificate.
<b>Mode</b>	Select the way in which you want to request the certificate.  Possible settings: <ul style="list-style-type: none"> <li><i>Manual</i> (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 <b>View details</b></li> </ul>

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"> <li>• <i>SCEP</i> : The key is requested from a CA using the Simple Certificate Enrolment Protocol.</li> </ul>
<b>Generate Private Key</b>	<p>Only for <b>Mode</b> = <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>
<b>SCEP URL</b>	<p>Only for <b>Mode</b> = <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>
<b>CA Certificate</b>	<p>Only for <b>Mode</b> = <i>SCEP</i></p> <p>Select the CA certificate.</p> <ul style="list-style-type: none"> <li>• In <code>-- Download --</code>: In <b>CA Name</b>, 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.</li> </ul> <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 <b>Generate Certificate Request</b> 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"> <li>&lt;name of an existing certificate&gt;: If all the necessary certificates are already available in the system, you select these manually.</li> </ul>
<b>RA Sign Certificate</b>	<p>Only for <b>Mode</b> = <i>SCEP</i></p> <p>Only for <b>CA Certificate</b> 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>
<b>RA Encrypt Certificate</b>	<p>Only for <b>Mode</b> = <i>SCEP</i></p> <p>Only if <b>RA Sign Certificate</b> 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>
<b>Password</b>	<p>Only for <b>Mode</b> = <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
<b>Custom</b>	<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 <b>Summary</b> 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 <b>Common Name</b>, <b>E-mail</b>, <b>Organizational Unit</b>, <b>Organization</b>, <b>Locality</b>, <b>State/Province</b> and <b>Country</b>.</p> <p>The function is disabled by default.</p>
<b>Summary</b>	<p>Only for <b>Custom</b> = 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>
<b>Common Name</b>	<p>Only for <b>Custom</b> = disabled.</p> <p>Enter the name according to CA.</p>
<b>E-mail</b>	<p>Only for <b>Custom</b> = disabled.</p> <p>Enter the e-mail address according to CA.</p>
<b>Organizational Unit</b>	<p>Only for <b>Custom</b> = disabled.</p> <p>Enter the organisational unit according to CA.</p>
<b>Organization</b>	<p>Only for <b>Custom</b> = disabled.</p> <p>Enter the organisation according to CA.</p>
<b>Locality</b>	<p>Only for <b>Custom</b> = disabled.</p> <p>Enter the location according to CA.</p>
<b>State/Province</b>	<p>Only for <b>Custom</b> = disabled.</p> <p>Enter the state/province according to CA.</p>
<b>Country</b>	<p>Only for <b>Custom</b> = 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"> <li>• <i>None</i> (default value): No additional name is entered.</li> <li>• <i>IP</i>: An IP address is entered.</li> <li>• <i>DNS</i>: A DNS name is entered.</li> <li>• <i>E-mail</i>: An e-mail address is entered.</li> <li>• <i>URI</i>: A uniform resource identifier is entered.</li> <li>• <i>DN</i>: A distinguished name (DN) name is entered.</li> <li>• <i>RID</i>: A registered identity (RID) is entered.</li> </ul>

#### Fields in the Options menu

Field	Description
<b>Autosave Mode</b>	<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>

#### 5.7.1.3 Import

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

Certificate List CRLs Certificate Servers

Import	
External Filename	<input type="text"/> <span style="float: right;">Browse...</span>
Local Certificate Description	<input type="text"/>
File Encoding	Auto <span style="font-size: small;">▼</span>
Password	<input type="text"/>

OK Cancel

Fig. 46: **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
<b>External Filename</b>	Enter the file path and name of the certificate to be imported, or use <b>Browse...</b> to select it from the file browser.
<b>Local Certificate Description</b>	Enter a unique description for the certificate.
<b>File Encoding</b>	Select the type of coding so that your device can decode the certificate.  Possible values: <ul style="list-style-type: none"> <li>• <i>Auto</i> (default value): Activates automatic code recognition. If downloading the certificate in auto mode fails, try with a certain type of encoding.</li> <li>• <i>Base64</i></li> <li>• <i>Binary</i></li> </ul>
<b>Password</b>	You may need a password to obtain certificates for your keys.  Enter the password here.

## 5.7.2 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.

### 5.7.2.1 Import

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

Fig. 47: **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
<b>External Filename</b>	Enter the file path and name of the CRL to be imported, or use <b>Browse...</b> to select it from the file browser.
<b>Local Certificate Description</b>	Enter a unique description for the CRL.
<b>File Encoding</b>	Select the type of encoding, so that your device can decode the CRL.  Possible values: <ul style="list-style-type: none"> <li><i>Auto</i> (default value): Activates automatic code recognition. If downloading the CRL in auto mode fails, try with a certain</li> </ul>

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

### 5.7.3 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.

#### 5.7.3.1 New

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

Fig. 48: **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
<b>Description</b>	Enter a unique description for the certificate server.
<b>LDAP URL Path</b>	Enter the LDAP URL or the HTTP URL of the server.

## Chapter 6 Physical Interfaces

### 6.1 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 preconfigured.



#### 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 console 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.

### 6.1.1 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  Seconds

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

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

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Auto 10 mbps / Half Duplex</i></li> <li>• <i>Fixed 1000 mbps / Full Duplex</i></li> <li>• <i>Fixed 100 mbps / Full Duplex</i></li> <li>• <i>Fixed 100 mbps / Half Duplex</i></li> <li>• <i>Fixed 10 mbps / Full Duplex</i></li> <li>• <i>Fixed 10 mbps / Half Duplex</i></li> <li>• <i>None: The interface is created but remains inactive.</i></li> </ul>
<b>Current Speed / Mode</b>	<p>Shows the actual mode and actual speed of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>1000 mbps / Full Duplex</i></li> <li>• <i>100 mbps / Full Duplex</i></li> <li>• <i>100 mbps / Half Duplex</i></li> <li>• <i>10 mbps / Full Duplex</i></li> <li>• <i>10 mbps / Half Duplex</i></li> <li>• <i>Down</i></li> </ul>
<b>Flow Control</b>	<p>Select whether a flow control should be conducted on the corresponding interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Disabled</i> (default value): No flow control is performed.</li> <li>• <i>Enabled</i>: Flow control is performed.</li> <li>• <i>Auto</i>: Automatic flow control is performed.</li> </ul>

## 6.2 ISDN Ports

In this menu, you configure the ISDN interface of your device. Here you enter data such as the type of ISDN connection to which your device is connected.

You can use the ISDN BRI interface of your device for both dialup and leased lines over ISDN. Proceed as follows to configure the ISDN BRI interface:

- Enter the settings for your ISDN connection: Here you set the most important parameters of your ISDN connection.

- **MSN Configuration:** Here you tell your device how to react to incoming calls from the WAN.

## 6.2.1 ISDN Configuration




### Note

If the ISDN protocol is not detected, it must be selected manually under **Port Usage** und **ISDN Configuration Type**. The automatic D channel detection is then switched off. An incorrectly set ISDN protocol prevents ISDN connections being set up.

In the **Physical Interfaces->ISDN Ports->ISDN Configuration** menu, a list of all ISDN ports and their configuration are displayed.

### 6.2.1.1 Edit

Choose the  button to edit the configuration of the ISDN port.

ISDN Configuration MSN Configuration

Basic Parameters	
Port Name	bri-0 (TE)
Autoconfiguration on Bootup	<input checked="" type="checkbox"/> Enabled
Result of Autoconfiguration	Port Usage: Not used, ISDN Configuration Type: Point-to-Multipoint
Port Usage	Not used
ISDN Configuration Type	<input checked="" type="radio"/> Point-to-Multipoint <input type="radio"/> Point-to-Point
Advanced Settings	
X.31 (X.25 in D Channel)	<input type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 50: **Physical Interfaces->ISDN Ports->ISDN Configuration->** 

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

#### Fields in the Basic Parameters menu.

Field	Description
Port Name	Shows the name of the ISDN port.

Field	Description
<b>Autoconfiguration on Bootup</b>	<p>Select whether the ISDN switch type (D channel detection for switched line) is to be automatically identified.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>Result of Autoconfiguration</b>	<p>Shows the status of the ISDN Auto Config.</p> <p>Automatic D-channel detection runs until a setting is found, or until the ISDN protocol is selected manually under <b>Port Usage</b>. This field cannot be edited. The result of automatic configuration for the <b>Port Usage</b> and the <b>ISDN Configuration Type</b> is displayed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>All possible values for the <b>Port Usage</b> and the <b>ISDN Configuration Type</b>.</li> <li><i>Running</i>: Detection is still running.</li> </ul>
<b>Port Usage</b>	<p>Only if <b>Autoconfiguration on Bootup</b> is disabled.</p> <p>Select the protocol that you want to use for the ISDN port.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>Not used</i>: The ISDN connection is not used.</li> <li><i>Dialup (Euro ISDN)</i></li> </ul>
<b>ISDN Configuration Type</b>	<p>Only if <b>Autoconfiguration on Bootup</b> is disabled and for <b>Port Usage</b> = <i>Dialup (Euro ISDN)</i> is set.</p> <p>Select the ISDN connection type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>Point-to-Multipoint</i> (default value): Point-to-multipoint connection</li> <li><i>Point-to-Point</i>: Point-to-point ISDN access.</li> </ul>

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

#### Fields in the Advanced Settings menu.

Field	Description
<b>X.31 (X.25 in D Channel)</b>	<p>Select whether you want to use X.31 (X.25 in the D channel) e.g. for CAPI applications.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>X.31 TEI Value</b>	<p>Only if <b>X.31 (X.25 in D Channel)</b> is enabled</p> <p>With the ISDN autoconfiguration, the X.31-TEI is detected automatically. If the autoconfiguration has not detected TEI, you can manually enter the value assigned by the exchange.</p> <p>Possible values are <i>0</i> to <i>63</i>.</p> <p>The default value is <i>-1</i> (for automatic detection).</p>
<b>X.31 TEI Service</b>	<p>Only for <b>X.31 (X.25 in D Channel)</b> = enabled</p> <p>Select the service for which you want to use X.31 TEI.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>CAPI</i></li> <li>• <i>CAPI Default</i></li> <li>• <i>Packet Switch</i> (default value)</li> </ul> <p><i>CAPI</i> and <i>CAPI Default</i> are only for the use of X.31 TEI for CAPI applications. For <i>CAPI</i>, the TEI value set in the CAPI application is used. For <i>CAPI Default</i>, the value of the CAPI application is ignored and the default value set here is always used.</p> <p><i>Packet Switch</i> is set if you want to use X.31 TEI for the X.25 device.</p>

## 6.2.2 MSN Configuration

In this menu, you can assign the available ISDN numbers to the required services (e.g. PPP routing, ISDN login).

If you use the ISDN interface for outgoing and incoming dialup connections, your own numbers for this interface can be entered in this menu (these settings are not possible for leased lines). Your device distributes the incoming calls to the internal services according

to the settings in this menu. Your own number is included as the calling party number for outgoing calls.

The device supports the following services:

- **PPP (Routing):** The PPP (routing) service is your device's general routing service. This enables ISDN remote terminals to establish data connections with your LAN, among other things. This enables partners outside your own local network to access hosts within your LAN. It is also possible to establish outgoing data connections to ISDN remote terminals.
- **ISDN Login:** The ISDN login service enables both incoming data connections with access to the SNMP shell of your device, and outgoing data connections to other bintec elmeg devices. As a result, your device can be remotely configured and administrated.
- **IPSec:** bintec elmeg devices support the DynDNS service to enable hosts without fixed IP addresses to obtain a secure connection over the Internet. With the IPSec Callback function and using a direct ISDN call to an IPSec peer with a dynamic IP address you can signal to this IPSec peer that you are online and waiting for the setup of 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. The identification of the caller from his or her ISDN number is enough information to initiate setting up a tunnel.
- **X.25 PAD:** X.25 PAD is used to provide a protocol converter, which converts non-packet-oriented protocols to packet-oriented communication protocols and vice versa. Data terminal equipment sending or receiving data on a non-data-packet-oriented basis can this be adapted in line with Datex-P (public data packet network based on the principle of a packet switching exchange).

When a call comes in, your device first uses the entries in this menu to check the type of call (data or voice call) and the called party number, whereby only part of the called party number reaches the device, which is forwarded from the local exchange or, if available, the PBX. The call is then assigned to the corresponding service.



#### Note

If no entry is specified (ex works state), every incoming ISDN call is accepted by the ISDN Login service. To avoid this, you should make the necessary entries here. As soon as an entry exists, the incoming calls not assigned to any entry are forwarded to the CAPI service.

A list of all MSNs is displayed in the **Physical Interfaces->ISDN Ports->MSN Configuration** menu.

### 6.2.2.1 New

Set the **New**, button to set up a new MSN.

Fig. 51: Physical Interfaces->ISDN Ports->MSN Configuration->New

The menu **Physical Interfaces->ISDN Ports->MSN Configuration->New** consists of the following fields:

#### Fields in the Basic Parameters menu.

Field	Description
<b>ISDN Port</b>	Select the ISDN port for which the MSN is to be configured.
<b>Service</b>	<p>Select the service to which a call is to be assigned on the <b>MSN</b> below.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>ISDN Login</i> (default value): Enables login with <i>ISDN Login</i></li> <li>• <i>PPP (Routing)</i>: Default setting for PPP routing. Contains automatic detection of the PPP connections stated below except <i>PPP DOVB</i>.</li> <li>• <i>IPSec</i>: Enables a number to be defined for IPSec callback.</li> <li>• <i>Other (PPP)</i>: Other services can be selected: <i>PPP 64k</i> (Allows 64 kbps PPP data connections), <i>PPP 56k</i> (Allows 56 kbps PPP data connections), <i>PPP V.110 (9600)</i> <i>PPP V.110 (14400)</i>, <i>PPP V.110 (19200)</i>, <i>PPP V.110 (38400)</i> (Allows PPP connections with V.110 and bitrates of 9,600 bps, 14,400 bps, 19,200 bps, 38,400 bps), <i>PPP V.120</i> (Allows PPP connections with V.120).</li> </ul>

Field	Description
<b>MSN</b>	Enter the number used to check the called party number. For the call to be accepted, it is sufficient for the individual numbers in the entry to agree, taking account of <b>MSN Recognition</b> .
<b>MSN Recognition</b>	Select the mode your device is to use for the number comparison for <b>MSN</b> with the called party number of the incoming call.  Possible values: <ul style="list-style-type: none"> <li>• <i>Right to Left</i> (default value)</li> <li>• <i>Left to Right (DDI)</i>: Always select if your device is connected to a point-to-point connection.</li> </ul>
<b>Bearer Service</b>	Select the type of incoming call (service detection).  Possible values: <ul style="list-style-type: none"> <li>• <i>Data + Voice</i> (default value): Both data and voice calls.</li> <li>• <i>Data</i>: data call</li> <li>• <i>Voice</i>: Voice call (modem, voice, analog fax)</li> </ul>

## 6.3 DSL Modem

### 6.3.1 DSL Configuration

In this menu, you make the basic settings for your xDSL connection.



#### Note

You require a licence for devices in the RS series to activate VDSL.



DSL Configuration

Automatic Refresh Interval <input type="text" value="60"/> Seconds <span style="float: right;"><b>Apply</b></span>	
<b>DSL Port Status</b>	
DSL Chipset	Lantiq VRX288
Physical Connection	Unknown
<b>Current Line Speed</b>	
Downstream	0bps
Upstream	0bps
<b>DSL Parameter</b>	
DSL Mode	VDSL/ADSL Multimode ▼
Transmit Shaping	Default (Line Speed) ▼
<b>Advanced Settings</b>	
ADSL Line Profile	Deutsche Telekom ▼
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 52: Physical Interfaces->DSL Modem->DSL Configuration

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

#### Fields in the DSL Port Status menu.

Field	Description
<b>DSL Chipset</b>	Shows the key of the installed chipset.
<b>Physical Connection</b>	<p>Shows the current ADSL operation mode. The value cannot be changed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Unknown</i>: The ADSL link is not active.</li> <li>• <i>ANSI T1.413</i>: ANSI T1.413</li> <li>• <i>ADSL1</i>: ADSL classic, G.DMT, ITU G.992.1</li> <li>• <i>G.lite G992.2</i>: Splitterless ADSL, ITU G.992.2</li> <li>• <i>ADSL2</i>: G.DMT.Bis, ITU G.992.3</li> <li>• <i>ADSL2 DELT</i>: ADSL2 Double Ended Line Test</li> <li>• <i>ADSL2 Plus</i>: ADSL2 Plus, ITU G.992.5</li> <li>• <i>ADSL2 Plus DELT</i>: ADSL2 Plus Double Ended Line Test</li> <li>• <i>READSL2</i>: Reach Extended ADSL2</li> <li>• <i>READSL2 DELT</i>: Reach Extended ADSL2 Double Ended Line Test.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>ADSL2 ITU-T G.992.3 Annex M</i></li> <li>• <i>ADSL2+ ITU-T G.992.5 Annex M</i></li> <li>• <i>VDSL2, ITU-T G.993.2</i></li> <li>• <i>ADSL2 Annex J</i></li> <li>• <i>ADSL2+ Annex J</i></li> </ul>

#### Fields in the Current Line Speed menu.

Field	Description
<b>Downstream</b>	Displays the data rate in the receive direction (direction from CO/DSLAM to CPE/router) in bits per second. The value cannot be changed.
<b>Upstream</b>	Displays the data rate in the send direction (direction from CPE/router to CO/DSLAM) in bits per second.  The value cannot be changed.

#### Fields in the DSL Parameter menu.

Field	Description
<b>DSL Mode</b>	<p>Select the xDSL synchronization type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Inactive</i>: The xDSL interface is not active.</li> <li>• <i>ETSI T1.413</i>: ADSL with ETSI T1.413 standard is used.</li> <li>• <i>ADSL1</i> : ADSL1 / G.DMT is used.</li> <li>• <i>ADSL Automode</i> : The ADSL mode is automatically adapted for the remote terminal.</li> <li>• <i>ADSL2</i>: ADSL2 / G.992.3 is used.</li> <li>• <i>ADSL2 Plus</i>: ADSL2 Plus / G.992.5 is used.</li> <li>• <i>VDSL</i>: VDSL is used.</li> <li>• <i>VDSL/ADSL Multimode</i> (default value): VDSL or ADSL is used. The mode is automatically adapted for the remote terminal.</li> </ul>
<b>Transmit Shaping</b>	Select whether the data rate in the send direction is to be reduced. This is only needed in a few cases for special DSLAMs.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Default (Line Speed)</i>: The data rate in the send direction is not reduced.</li> <li>• <i>128000 bps, 192000 bps, 256000 bps, 512000 bps, 768000 bps, 1024000 bps, 1536000 bps and 2048000 bps</i>: The data rate in the send direction is reduced to a maximum of 128,000 bps to 2,048,000 bps in defined steps.</li> <li>• <i>User-defined</i>: The data rate is reduced to the value entered in <b>Maximum Upstream Bandwidth</b>.</li> </ul> <p>The default value is <i>Default (Line Speed)</i>.</p>
<b>Maximum Upstream Bandwidth</b>	<p>Only for <b>Transmit Shaping</b> = <i>User-defined</i></p> <p>Enter the maximum data rate in the send direction in bits per second.</p>

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

#### Fields in the Advanced Settings menu.

Field	Description
<b>ADSL Line Profile</b>	<p>Select the internet service provider you require and, in doing so, implicitly select the modem parameter set used by this provider.</p> <p><i>Deutsche Telekom</i> is entered as the default value.</p> <p>If your provider is not shown in the list, use the <i>default</i> setting.</p>

## 6.4 UMTS/LTE

### 6.4.1 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 USB stick.

A list of compatible UMTS/LTE USB sticks can be found at [www.bintec-elmeg.com](http://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.

### 6.4.1.1 Edit

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

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 USB stick 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"/> <b>Enabled</b>
Modem Status	<b>PIN input required</b>
Actual Network	<b>Unknown</b>
Network Quality	-
Preferred Network Type	Automatic ▾
Incoming Service Type	<input checked="" type="radio"/> <b>Disabled</b> <input type="radio"/> ISDN Login <input type="radio"/> PPP Dialin <input type="radio"/> IPsec
SIM Card Uses PIN	*****
Fallback Number	
APN (Access Point Name)	

Advanced Settings

Roaming/PLMN Selection	
Roaming Mode	Auto Select ▾
Closed User Group	
Authentication APN	
Authentication Method	pap-chap ▾
Username	
Password	
Fixed IP Address	

Fig. 53: **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
<b>UMTS/LTE Status</b>	<p>Select whether the chosen UMTS/LTE modem should be enabled or disabled.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>Modem Status</b>	<p>Only for <b>UMTS/LTE Status</b> = <i>Enabled</i></p> <p>Shows the status of the UMTS/LTE modem.</p>


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

Field	Description
	<ul style="list-style-type: none"> <li>• <i>GPRS preferred</i>: GPRS is preferentially used; should GPRS not be available, UMTS is used.</li> <li>• <i>UMTS preferred</i>: UMTS is preferentially used; should UMTS not be available, GPRS is used.</li> <li>• <i>LTE only</i>: Only LTE is used; should LTE be unavailable, no connection is established.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> </ul>

Field	Description
	<div data-bbox="539 247 621 298" style="float: left; margin-right: 10px;">  </div> <p data-bbox="635 247 692 273"><b>Note</b></p> <p data-bbox="635 307 1263 435">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 data-bbox="635 461 1263 657">When a modem is in the "up" state and <b>Preferred Network Type</b> 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>
<p data-bbox="359 731 625 760"><b>Incoming Service Type</b></p>	<p data-bbox="635 731 1056 760">Only for <b>UMTS/LTE Status</b> = <i>Enabled</i></p> <p data-bbox="635 785 1285 854">Here you select the gateway subsystem to which an incoming call over the modem is to be assigned.</p> <p data-bbox="635 879 806 905">Possible values:</p> <ul data-bbox="635 930 1306 1169" style="list-style-type: none"> <li>• <i>Disabled</i>: Call is not accepted (default value for LTE connections).</li> <li>• <i>ISDN Login</i>: The call is assigned to the ISDN Login subsystem (default value for UMTS connections).</li> <li>• <i>PPP Dialin</i>: The call is assigned to the PPP subsystem.</li> <li>• <i>IPSec</i>: The call is made via IPSec.</li> </ul> <p data-bbox="635 1195 1263 1255">Please note the following for the setting <b>Incoming Service Type</b> <i>IPSec</i>:</p> <p data-bbox="635 1281 1306 1511">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 data-bbox="635 1537 1292 1614">In the <b>VPN-&gt;IPSec-&gt;IPSec Peers-&gt;</b><b>-&gt;Advanced Settings</b> menu, you can also choose whether the IP address for IPSec</p>



Field	Description
	tunnel setup should be transmitted with the UMTS/LTE callback call under <b>Transfer own IP address over ISDN/GSM</b> . This may shorten and simplify tunnel setup.
<b>PUK</b>	<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 <b>SIM Card Uses PIN</b> 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>
<b>SIM Card Uses PIN</b>	<p>Only for <b>UMTS/LTE Status</b> = <i>Enabled</i></p> <p>Enter the PIN for your UMTS/LTE modem card.</p>
	<p> <b>Note</b></p> <p>Entering a wrong PIN blocks communication until the entry is corrected.</p>
	<p> <b>Note</b></p> <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 <b>PUK</b> in order to unblock the SIM card.</p>
<b>Fallback Number</b>	<p>Only for <b>UMTS/LTE Status</b> = <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 <b>Always active</b> enabled in <b>WAN-&gt;Internet + Dialup-&gt;UMTS/LTE-&gt;</b>) , this means that the connection will be re-established immediately.</p>

Field	Description
	<div style="border: 1px solid gray; padding: 5px;">  <p><b>Note</b></p> <p>Please note that the SIM card must support this function, and that not all mobile telephony providers relay voice calls over data SIM cards.</p> </div>
<b>APN (Access Point Name)</b>	<p>Only for <b>UMTS/LTE Status</b> = <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
<b>Roaming Mode</b>	<p>Select if you intend to use Roaming.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Auto Select</i>(Default setting): Use this mode if neither <b>Roaming Mode</b> = <i>Disabled</i> nor <b>Roaming Mode</b> = <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.</li> <li>• <i>Unrestricted</i>: This mode is intended for specific requirements. Note that first a scan across all APNs is carried out in this mode.</li> <li>• <i>Fixed Operator</i>: At <b>Roaming Mode</b> = <i>Fixed</i> no scan is performed, and only the manually selected <b>Mobile Network Provider</b> is used. If the selected <b>Mobile Network Provider</b> is unavailable, no connection is made.</li> <li>• <i>Full Auto Select</i>: No scan is performed with this selection. The modem automatically selects the strongest <b>Mobile</b></li> </ul>

Field	Description
	<b>Network Provider</b> . Close to a country border this could also be the network of a foreign roaming partner.
<b>Mobile Network Provider</b>	<p>Only for <b>Roaming Mode</b> = <i>Fixed Operator</i></p> <p>Select a <b>Mobile Network Provider</b> from the list.</p> <p>Possible values</p> <ul style="list-style-type: none"> <li>• &lt;Provider&gt;: Select a <b>Mobile Network Provider</b> from the list.</li> <li>• <i>Manual Selection</i>: This allows entering a Provider ID (PLMN) manually.</li> </ul>
<b>Mobile Network Provider</b>	<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
<b>Authentication APN</b>	Enter the Authentication Access Point Name for the <b>Closed User Group</b> , that you have received from your provider.
<b>Authentication Method</b>	<p>Select an authentication protocol for the <b>Closed User Group</b>. Select only an authentication method that has been specified by your provider.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>None</i>: Some providers do not use authentication. Select this option if your provider is among them.</li> <li>• <i>pap</i>: Execute only PAP (PPP Password Authentication Protocol), the password is sent unencrypted.</li> <li>• <i>chap</i>: Execute only CHAP (PPP Challenge Handshake Authentication Protocol according to RFC 1994) the password is sent encrypted.</li> <li>• <i>pap-chap</i> (Default value): Prefer CHAP, use PAP if not available.</li> </ul>
<b>Username</b>	Enter the user name that has been supplied by your provider.

Field	Description
<b>Password</b>	Enter the password that has been supplied by your provider.
<b>Fixed IP Address</b>	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 <input type="text" value="60"/> Seconds <input type="button" value="Apply"/>			
Mobile Device Status			
Device	/dev/usbTTC0		
Modem Model	MC7710		
IMEI	355060020096827		
Oper Status	PIN input required		
ICC ID	8949020000473279466		
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. 54: Physical Interfaces->UMTS/LTE-> 

#### Values in the list Mobile Device Status

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

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

#### Values in the list Mobile Operators

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

## Chapter 7 LAN


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

### 7.1 IP Configuration

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



#### 7.1.1 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.

Change the status of the interface by clicking the  or the  button in the **Action** column.

Press the  button to display the details of an existing interface.



#### Note

For IPv4 note that:

If your device has obtained an IP address dynamically from a DHCP server operated in your network for the basic configuration, the default 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 default 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.

Here is an example for an IPv6 address:

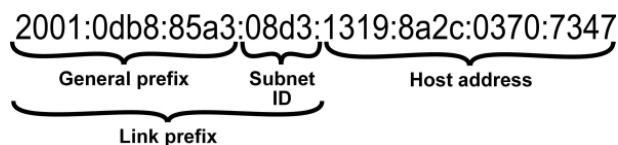


Fig. 55: IPv6 example address

Your device can act either as router or as device at one interface. In general, it acts as router at the LAN interfaces, and as host at the WAN and PPP interfaces.

If your device acts as router, its own IPv6 addresses can be created as follows: a Link Prefix can be derived from a General Prefix or you can manually specify a static value. One host address can be created through *Auto eui-64*, for additional host addresses you can specify static values.


If your device acts a router, it commonly distributes the configured link prefix to the hosts through Router Advertisements. A DHCP server may distribute additional information to the hosts, e.g., the address of a timer server. A client can create its own host address either through Stateless Address Autoconfiguration (SLAAC) or have this address assigned by a DHCP server.

In order to make use of the router mode described above, use the following settings in the menu **LAN->IP Configuration->Interfaces->New: IPv6 Mode = Router, Transmit Router Advertisement = Enabled, DHCP Server Enabled** and **IPv6 Addresses = Add**.

If your device acts as host, it has a Link Prefix assigned by another router through Router Advertisements. The host address is then automatically derived through SLAAC. Additional information like, e.g., the General Prefix of the provider or the address of a time server can be received through DHCP. Use the following settings in the menu **LAN->IP**

->**Interfaces->New: IPv6 Mode** = *Client*, **Accept Router Advertisement** = *Enabled* and **DHCP Client** = *Enabled*.

### 7.1.1.1 Edit or New

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

Interfaces

(VLAN ID1)

**Basic Parameters**

Based on Ethernet Interface

Interface Mode  Untagged  Tagged (VLAN)

VLAN ID

MAC Address   Use built-in

**Basic IPv4 Parameters**

Security Policy  Untrusted  Trusted

Address Mode  Static  DHCP

IP Address / Netmask

**Basic IPv6 Parameters**

IPv6  Enabled

Advanced Settings

**Advanced IPv4 Settings**

Proxy ARP  Enabled

TCP-MSS Clamping  Enabled

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
<b>Based on Ethernet Interface</b>	This field is only displayed if you are editing a virtual routing interface.  Select the Ethernet interface for which the virtual interface is to be configured.
<b>Interface Mode</b>	Only for physical interfaces in routing mode and for virtual interfaces.



Field	Description
	<p>Select the configuration mode of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Untagged</i> (default value): The interface is not assigned for a specific purpose.</li> <li>• <i>Tagged (VLAN)</i>: This option only applies for routing interfaces.</li> </ul> <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 <b>MAC Address</b> is optional in this mode.</p>
<b>VLAN ID</b>	<p>Only for <b>Interface Mode</b> = <i>Tagged (VLAN)</i></p> <p>This option only applies for routing interfaces. Assign the interface to a VLAN by entering the VLAN ID of the relevant VLAN.</p> <p>Possible values are 1 (default value) to 4094.</p>
<b>MAC Address</b>	<p>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 <b>Use built-in</b>, 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).</p> <p>If <b>Use built-in</b> is active, the predefined MAC address of the allocated physical interface is used.</p> <p><b>Use built-in</b> is activated by default.</p>

#### Fields in the Basic IPv4 Parameters menu.

Field	Description
<b>Security Policy</b>	<p>Select the security settings to be used with the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i> (default value): All IP packets are allowed through except for those which are explicitly prohibited..</li> <li>• <i>Untrusted</i>: Only those packets are transmitted that can be attributed to a connection that has been initiated from a trus-</li> </ul>

Field	Description
	<p>ted zone.</p> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>
<b>Address Mode</b>	<p>Select how an IP address is assigned to the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Static</i> (default value): The interface is assigned a static IP address in <b>IP Address / Netmask</b>.</li> <li>• <i>DHCP</i>: An IP address is assigned to the interface dynamically via DHCP.</li> </ul>
<b>IP Address / Netmask</b>	<p>Only for <b>Address Mode</b> = <i>Static</i></p> <p>With <b>Add</b>, add a new address entry, enter the <b>IP Address</b> and the corresponding <b>Netmask</b> of the virtual interface.</p>

#### Fields in the **Basic IPv6 Parameters** menu.

Field	Description
<b>IPv6</b>	<p>Select whether this interface should use Internet Protocol version 6 (IPv6) for data transmission.</p> <p>The function is activated by selecting <i>Enabled</i>. The function is disabled by default.</p>
<b>Security Policy</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i></p> <p>Select the security settings to be used with the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i> (default value): All IP packets are allowed through except for those which are explicitly prohibited.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 on your LAN.</p> <ul style="list-style-type: none"> <li>• <i>Untrusted</i>: Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 outside of your LAN.</p>

Field	Description
	<p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>
<b>IPv6 Mode</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i></p> <p>Select whether the interface is to be operated in host or in router mode. Depending on your selection different parameters are presented for you to configure.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Router (Transmit Router Advertisement)</i> (default value): The interface connects different networks to each other.</li> <li>• <i>Host</i>: The interface is operated in host mode.</li> </ul>
<b>Transmit Router Advertisement</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Router (Transmit Router Advertisement)</i></p> <p>Select whether Router Advertisements are to be sent via the interface.</p> <p>Using Router Advertisements the list of prefixes is propagated and the router propagates itself as the standard gateway.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>DHCP Server</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Router (Transmit Router Advertisement)</i></p> <p>Specify if your device is to act as DHCP server, i.e., if it is to transmit DHCP options in order to distribute information about the DNS servers to the clients.</p> <p>Enable this option if hosts are to create IPv6 addresses through SLAAC.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>IPv6 Addresses</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i></p>

Field	Description
	<p>You can assign <b>IPv6 Addresses</b> to the selected interface..</p> <p><b>Add</b> allows you to create one or more address entries.</p> <p>A new windows opens that allows you to specify an IPv6 address consisting of a Link Prefix and a host identifier.</p> <p>If your device operates in host mode (<b>IPv6 Mode</b> = <i>Host</i>, <b>Accept Router Advertisement</b> = <i>Enabled</i> and <b>DHCP Client</b> = <i>Enabled</i>), its IPv6 addresses are determined through SLAAC. You need not configure an IPv6 address manually, but you can enter additional addresses if desired.</p> <p>If your device is operating in router mode (<b>IPv6 Mode</b> = <i>Router (Transmit Router Advertisement)</i>, <b>Transmit Router Advertisement</b> = <i>Enabled</i> and <b>DHCP Server</b> = <i>Enabled</i>), you need to configure its IPv6 addresses here.</p>
<b>Accept Router Advertisement</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Host</i></p> <p>Select if Router Advertisements are to be received on the selected interface. Router Advertisements are used, e.g., to create the prefix list.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>DHCP Client</b>	<p>Only for <b>IPv6</b> = <i>Aktiviert</i> and <b>IPv6 Mode</b> = <i>Host</i></p> <p>Select if your device is to act as DHCP client, i.e., if it is to receive DHCP options in order to obtain information about the DNS servers.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

Use **Add** to create more entries.

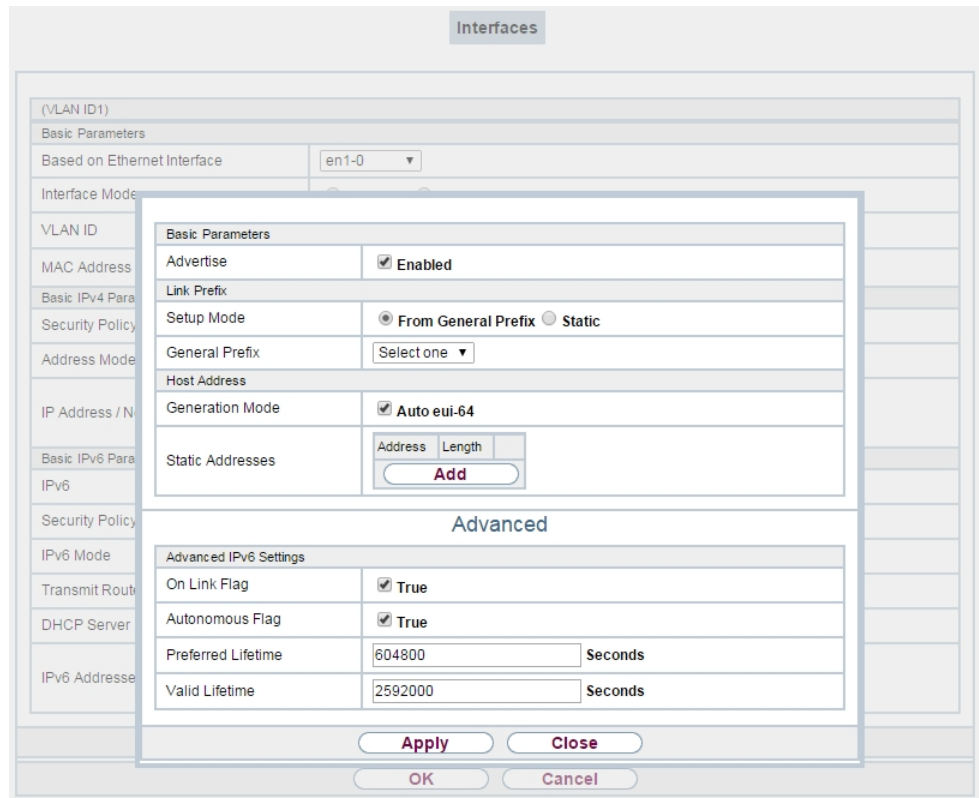


Fig. 57: LAN->IP Configuration->Interfaces->New->Add

**Fields in the Basic Parameters menu.**

Field	Description
<b>Advertise</b>	<p>Only for <b>IPv6 Mode = Router</b> (<i>Transmit Router Advertisement</i>)</p> <p>Here you can determine if the prefix being defined in the current window is propagated per Router Advertisement over the selected interface.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

**Fields in the Link Prefix menu.**

Field	Description
<b>Setup Mode</b>	Select in which way the Link Prefix is to be determined.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>From General Prefix</i> (default value): The Link Prefix is derived from a General Prefix.</li> <li>• <i>Static</i>: You can enter the link prefix.</li> </ul>
<b>General Prefix</b>	<p>Only for <b>Setup Mode</b> = <i>From General Prefix</i></p> <p>Select the General Prefix the Link Prefix is to be derived from. You can choose from the General Prefixes available under <b>Network-&gt;IPv6 General Prefixes-&gt;General Prefix Configuration-&gt;New</b>.</p>
<b>Auto Subnet Configuration</b>	<p>Only if <b>Setup Mode</b> = <i>From General Prefix</i> and if a General Prefix has been selected.</p> <p>Select if the subnet is to be created automatically. Automatic subnet creation will use ID <i>0</i> for the first subnet, ID <i>1</i> for the second, etc.</p> <p>Possible values for the sub net ID are: <i>0 - 65535</i>.</p> <p>The subnet ID describes the fourth of the four 16 bit fields of a Link Prefix. Upon subnet creation the decimal ID value is converted to a hexadecimal one.</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 disabled, you can define a subnet by entering a Subnet ID.</p>
<b>Subnet ID</b>	<p>Only if <b>Auto Subnet Configuration</b> is not active.</p> <p>Enter a Subnet ID in order to define a subnet. The subnet ID describes the fourth of the four 16 bit fields of a Link Prefix.</p> <p>Possible values are <i>0 - 65535</i>.</p> <p>Upon subnet creation the decimal ID value is converted to a hexadecimal one.</p>
<b>Link Prefix</b>	<p>Only for <b>Setup Mode</b> = <i>Static</i></p>

Field	Description
	You can specify the Link Prefix of an IPv6 address. This prefix must end with <code>::</code> . Its predetermined length is <code>64</code> .


#### Fields in the **Host Address** menu.

Field	Description
<b>Generation Mode</b>	<p>Determine if the Host Identifier of the IPv6 address is to be automatically derived from the MAC address through EUI-64.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p> <p>EUI-64 triggers the following process:</p> <ul style="list-style-type: none"> <li>• The hexadecimal 48 bit MAC address is split into 2 x 24 bit.</li> <li>• <code>FFFE</code> is inserted into the created gap in order to obtain 64 bit.</li> <li>• The hexadecimal notation of the 64 bit is converted to a binary notation.</li> <li>• Bit no. 7 of the first 8 bit field is set to <code>1</code>.</li> </ul>
<b>Static Addresses</b>	<p>Independently of the automatic creation described under <b>Generation Mode</b>, you can manually specify the Host Identifier of one or more IPv6 addresses with <b>Add</b>. Its predefined length is <code>64</code>. Start any entry with <code>::</code>.</p>

The fields in the **Advanced** menu are part of the prefix information sent inside of Router Advertisements if **Advertise** is enabled. The menu **Advanced** consists of the following fields:

#### Fields in the **Advanced IPv6 Settings** menu

Field	Description
<b>On Link Flag</b>	<p>Select whether the On-Link Flag (L-Flag) should be set. This allows the host to enter the prefix from the prefix list.</p> <p>The function is activated by selecting <i>True</i>.</p> <p>The function is enabled by default.</p>
<b>Autonomous Flag</b>	<p>Select whether the Autonomous Address Configuration Flag (A-Flag) should be set. This allows the host to use the prefix and the 64 bit interface ID, to derive its address.</p> <p>The function is activated by selecting <i>True</i>.</p>

Field	Description
	The function is enabled by default.
<b>Preferred Lifetime</b>	<p>Enter a time period in seconds. During this time, addresses derived from the prefix through SLAAC are preferred.</p> <p>The default value is <i>604800</i> seconds.</p>
<b>Valid Lifetime</b>	<p>Enter a time period in seconds, for which the prefix is valid.</p> <p>The default value is <i>2592000</i> seconds.</p>
	<p> <b>Note</b></p> <p>The value for the valid lifetime should be lower than the one configured for the option <b>Router Lifetime</b> under <b>Advanced IPv6 Settings</b>.</p>

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

#### Fields in the **Advanced IPv4 Settings** menu.



Field	Description
<b>DHCP MAC Address</b>	<p>Only for <b>Address Mode</b> = <i>DHCP</i></p> <p>If <b>Use built-in</b> 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 <b>Use built-in</b>, you enter a 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>
<b>DHCP Hostname</b>	<p>Only for <b>Address Mode</b> = <i>DHCP</i></p> <p>Enter the host name requested by the provider. The maximum length of the entry is 45 characters.</p>
<b>DHCP Broadcast Flag</b>	<p>Only for <b>Address Mode</b> = <i>DHCP</i></p> <p>Choose whether or not the BROADCAST bit is set in the DHCP</p>



Field	Description
	<p>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>
<b>Proxy ARP</b>	<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> <p>The function is disabled by default.</p>
<b>TCP-MSS Clamping</b>	<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>

#### Fields in the **Advanced IPv6 Settings** menu

Field	Description
<b>Router Lifetime</b>	<p>Only for <b>IPv6 = Enabled</b>, <b>IPv6 Mode = Router</b> (<i>Transmit Router Advertisement</i>) and <b>Transmit Router Advertisement = Enabled</b></p> <p>Enter a time period in seconds. The router remains in the default router list throughout this interval.</p> <p>The default value is <i>600</i> seconds. The maximum value is <i>65520</i> seconds. A value of <i>0</i> means that the router is not a default router, and will not be entered in the default router list.</p>

Field	Description
	<div data-bbox="541 211 1315 399" style="border: 1px solid #ccc; padding: 10px;">  <p><b>Note</b></p> <p>The value for the <b>Router Lifetime</b> should be higher than the shortest valid lifetime for a link prefix configured for this interface under <b>Basic IPv6 Parameters</b>.</p> </div>
<p><b>Router Preference</b></p>	<p>Only for <b>IPv6 = Enabled</b>, <b>IPv6 Mode = Router (Transmit Router Advertisement)</b> and <b>Transmit Router Advertisement = Enabled</b></p> <p>Select your router's preference for choice of default router. This is useful for cases where a node receives advertisements from multiple routers, or for back-up scenarios.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>High</i></li> <li>• <i>Medium</i> (default value)</li> <li>• <i>Low</i></li> </ul>
<p><b>DHCP Mode</b></p>	<p>Only for <b>IPv6 = Enabled</b>, <b>IPv6 Mode = Router (Transmit Router Advertisement)</b> and <b>Transmit Router Advertisement = Enabled</b></p> <p>Select the information to be forwarded to the DHCP client.</p> <div data-bbox="541 1069 1315 1226" style="border: 1px solid #ccc; padding: 10px;">  <p><b>Note</b></p> <p>To achieve this, your router must not be set up as a DHCP server.</p> </div> <p>By selecting <i>Other - DNS Servers, SIP Servers</i> (default value) no address- related information, such as i.e. DNS, VoIP, etc., is passed through.</p> <p>Enable this option if hosts inside of the network are to automatically create their IP addresses through SLAAC. In this case, the router sends only data via DHCP that are not address-related.</p> <p>By selecting <i>Managed - IPv6 Address Management</i> hosts receive IPv6 addresses as well as not address-related information through DHCP.</p>

Field	Description
<b>DNS Propagation</b>	<p>Only for <b>IPv6 Mode = Router</b> (<i>Transmit Router Advertisement</i>) and <b>Transmit Router Advertisement</b> <i>Enabled</i></p> <p>Select if and in which way DNS server addresses are to be propagated in Router Advertisements. A maximum of two DNS server addresses is propagated.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Off</i>: No DNS server address propagation</li> <li>• <i>Self</i>: The device sends its own IP addresses as DNS server address. If the device has multiple addresses, they are used in the following order: <ul style="list-style-type: none"> <li>• Global addresses</li> <li>• ULA (Unique Local Addresses)</li> <li>• Link local addresses</li> </ul> </li> <li>• <i>Other</i>: Statically configured as well as dynamically learned DNS server entries are propagated according to their priority. If there are no entries, no address is propagated.</li> </ul>

## 7.2 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.

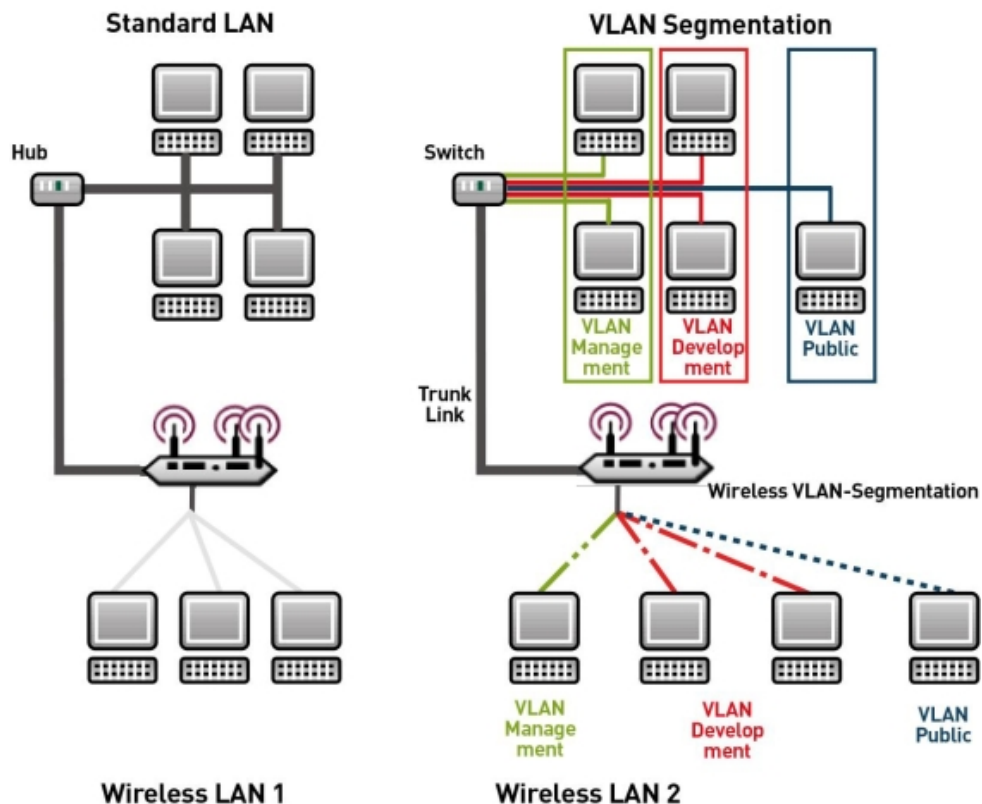


Fig. 58: VLAN segmenting

## 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**.

## 7.2.1 VLANs

In this menu, you can display all the VLANs already configured, edit your settings and create new VLANs. By default, the *Management* VLAN with **VLAN Identifier** = 1 is available, to which all interfaces are assigned.

### 7.2.1.1 Edit or New

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

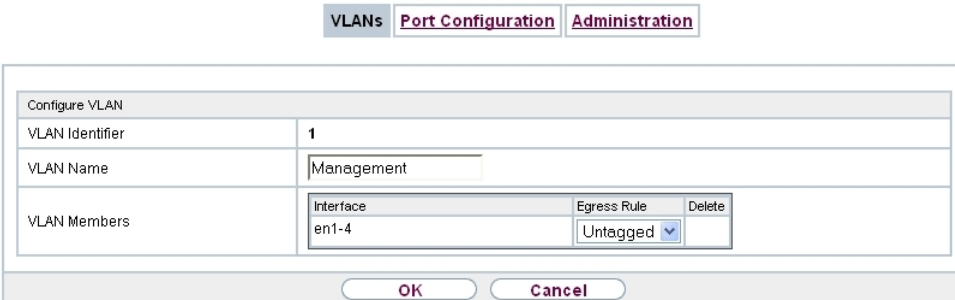



Fig. 59: LAN->VLAN->VLANs->New

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

#### Fields in the **Configure VLAN** menu.

Field	Description
<b>VLAN Identifier</b>	Enter the number that identifies the VLAN. In the  menu, you can no longer change this value.  Possible values are 1 (default value) to 4094.
<b>VLAN Name</b>	Enter a unique name for the VLAN. A character string of up to 32 characters is possible.  The predefined VLAN name is <i>Management</i> .
<b>VLAN Members</b>	Select the ports that are to belong to this VLAN. You can use the <b>Add</b> 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 in-

Field	Description
	formation) or <i>Untagged</i> (i.e. without VLAN information).

## 7.2.2 Port Configuration

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

[VLANs](#) | **Port Configuration** | [Administration](#)

View	20	per page	<<	>>	Filter in	None	>	equal	>	Go
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. 60: LAN->VLANs->Port Configuration

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

### Fields in the Port Configuration menu.

Field	Description
<b>Interface</b>	Shows the port for which you define the PVID and processing rules.
<b>PVID</b>	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.
<b>Drop untagged frames</b>	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.
<b>Drop non-members</b>	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.

## 7.2.3 Administration

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

Fig. 61: 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
<b>Enable VLAN</b>	<p>Enable or disable the specified bridge group for VLAN.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is not activated by default.</p>
<b>Management VID</b>	<p>Select the VLAN ID of the VLAN in which your device is to operate.</p>

## Chapter 8 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. Information on the modi contained in the standard and the correspondingly supported transmission speeds are, e.g., available at [Wikipedia](#).

### 8.1 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.

#### 8.1.1 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	Transmit Power	Status	
00:a0:f9:0b:cf:e0	Off	2.4 GHz	-	Max.	⬇️	🔧

Fig. 62: **Wireless LAN->WLAN->Radio Settings**




### 8.1.1.1 Radio Settings->

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

Select the  icon to edit the configuration.

Radio Settings	
<b>Wireless Settings</b>	
Operation Mode	Access-Point / Bridge Link Master
Operation Band	2.4 GHz In/Outdoor
Channel	Auto
Selected Channel	0
Transmit Power	Max.
<b>Performance Settings</b>	
Wireless Mode	802.11g
Airtime fairness	<input type="checkbox"/> Enabled
<b>Advanced Settings</b>	
Channel Plan	All
RTS Threshold	Always off
Short Guard Interval	<input checked="" type="checkbox"/> Enabled
Fragmentation Threshold	2346 Bytes
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 63: **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](#)

Fig. 64: **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
<b>Operation Mode</b>	Define the mode in which the wireless module of your device is to operate.  Possible values: <ul style="list-style-type: none"> <li>• <i>Off</i> (default value): The wireless module is not active.</li> <li>• <i>Access-Point / Bridge Link Master</i>: Your device is used as an access point in your network.</li> <li>• <i>Access Client</i>: Your device serves as an Access Client in your network.</li> <li>• <i>Bridge Link Client</i>: Your device is used as a wireless bridge link in your network.</li> </ul>
<b>Operation Band</b>	Select the operation band and, where applicable, the usage area of the wireless module.  <b>For Operation Mode = <i>Access-Point / Bridge Link Master</i> or <i>Bridge Link Client</i></b>  Possible values:

Field	Description
	<ul style="list-style-type: none"> <li>• <i>2.4 GHz In/Outdoor</i> (default value): Your device is operated at 2.4 GHz inside or outside buildings.</li> <li>• <i>5 GHz Indoor</i>: Your device runs in 5 GHz inside buildings.</li> <li>• <i>5 GHz Outdoor</i>: Your device runs in 5 GHz outside buildings.</li> <li>• <i>5 GHz In/Outdoor</i>: Your device is run with 5 GHz inside or outside buildings.</li> </ul>
<b>Usage Area</b>	<p>Only for <b>Operation Mode</b> = <i>Access Client</i> and <b>Operation Band</b> = <i>2.4 and 5 GHz</i> or <i>5 GHz</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Indoor-Outdoor</i> (default value)</li> <li>• <i>Indoor</i></li> <li>• <i>Outdoor</i></li> </ul>
<b>Channel</b>	<p>The number of channels you can select depends on the country setting. Please consult the data sheet for your device.</p> <p><b>Access Point Mode / Bridge Mode:</b></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"> <li>• For <b>Operation Band</b> = <i>2.4 GHz In/Outdoor</i></li> </ul> <p>Possible values are <i>1 to 13</i> and <i>Auto</i> (default value). <i>Auto</i> is not possible in bridge mode.</p> <ul style="list-style-type: none"> <li>• For <b>Operation Band</b> = <i>5 GHz Indoor</i></li> </ul>

Field	Description
	<p>Possible values are <i>36, 40, 44, 48</i> and <i>Auto</i> (standard value)</p> <ul style="list-style-type: none"> <li>For <b>Operation Band</b> = <i>5 GHz In/Outdoor</i> and <i>5 GHz Outdoor</i></li> </ul> <p>Only the <i>Auto</i> option is possible here.</p> <p><b>Access Client Mode:</b></p> <p>In the Access Client Mode no channel you can select. The used channel is shown.</p>
<b>Selected Channel</b>	Displays the channel used.
<b>Used Secondary Channel</b>	<p>Not for <b>Operation Mode</b> = <i>Access-Point / Bridge Link Master</i></p> <p>Displays the second channel used.</p>
<b>Transmit Power</b>	<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"> <li><i>Max.</i> (default value): The maximum antenna power is used.</li> <li><i>5 dBm</i></li> <li><i>8 dBm</i></li> <li><i>11 dBm</i></li> <li><i>14 dBm</i></li> <li><i>16 dBm</i></li> <li><i>17 dBm</i></li> </ul>

#### Fields in the menu Performance Settings

Field	Description
<b>Wireless Mode</b>	<p>Select the wireless technology that the access point is to use.</p> <p>Only for <b>Operation Mode</b> = <i>Access Point / Bridge Link Master</i> and <b>Operation Band</b> = <i>2.4 GHz In/Outdoor</i> or for</p>


Field	Description
	<p><b>Operation Mode = <i>Access Client</i> and Operation Band = 2.4 GHz</b></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>802.11g</i>: The device operates only in accordance with 802.11g. 802.11b clients have no access.</li> <li>• <i>802.11b</i>: Your device operates only in accordance with 802.11b and forces all clients to adapt to it.</li> <li>• <i>802.11 mixed (b/g)</i>: Your device adapts to the client technology and operates according to either <b>802.11b</b> or <b>802.11g</b>.</li> <li>• <i>802.11 mixed long (b/g)</i>: Your device adapts to the client technology and operates according to either <b>802.11b</b> or <b>802.11g</b>. 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.</li> <li>• <i>802.11 mixed short (b/g)</i>: Your device adapts to the client technology and operates according to either <b>802.11b</b> or <b>802.11g</b>. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates).</li> <li>• <i>802.11b/g/n</i>: Your device operates according to either 802.11b, 802.11g or 802.11n.</li> <li>• <i>802.11g/n</i>: Your device operates according to either 802.11g or 802.11n.</li> <li>• <i>802.11n</i>: Your device operates only according to 802.11n.</li> </ul> <p><b>For Operation Mode = <i>Access-Point / Bridge Link Master</i> and <i>Bridge Link Client</i> and Operation Band = 5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor and for Operation Mode = <i>Access Client</i> and Operation Band = 5.8 GHz</b></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>802.11a</i>: The device operates only in accordance with 802.11a.</li> <li>• <i>802.11n</i>: Your device operates only according to 802.11n.</li> <li>• <i>802.11a/n</i>: Your device operates according to either 802.11a or 802.11n.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>802.11ac/a/n</i>: Your device operates according to 802.11ac, 802.11a or 802.11n.</li> <li>• <i>802.11ac/n</i>: Your device operates according to either 802.11ac or 802.11n.</li> </ul>
<b>Bandwidth</b>	<p>For <b>Operation Mode</b> = <i>Access-Point / Bridge Link Master</i> or <i>Bridge Link Client</i></p> <p>Not for <b>Operation Band</b> = <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"> <li>• <i>20 MHz</i> (default value): One channel with 20 MHz bandwidth is used.</li> <li>• <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.</li> <li>• <i>80 MHz</i>: In 802.11 ac mode, a bandwidth of 80 MHz is additionally available.</li> </ul>
<b>Number of Spatial Streams</b>	<p>Not for <b>Wireless Mode</b> = <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"> <li>• <i>2</i>: Two traffic flows are used.</li> <li>• <i>1</i>: One traffic flow is used.</li> </ul>
<b>Airtime fairness</b>	<p>This function is not available for all devices.</p> <p>The <b>Airtime fairness</b> 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</p>

Field	Description
	Classe "Background".

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
<b>Channel Plan</b>	<p>Only for <b>Operation Mode</b> = <i>Access-Point / Bridge Link Master</i> and <b>Channel</b> = <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"> <li>• <i>All</i>: All channels can be dialled when a channel is selected.</li> <li>• <i>Auto</i>: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided.</li> <li>• <i>User defined</i>: Select the desired channels.</li> </ul>
<b>Selected Channels</b>	<p>Only for <b>Channel Plan</b> = <i>User defined</i></p> <p>The currently selected channels are displayed here.</p> <p>With <b>Add</b> 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>
<b>RTS Threshold</b>	<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</p>

Field	Description
	on/off independently of the data packet length by selecting the value <i>Always on</i> or <i>Always off</i> (default value).
<b>Short Guard Interval</b>	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.
<b>Fragmentation Threshold</b>	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.  Possible values are 256 to 2346.  The default value is 2346 bytes.

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

Fig. 65: Wireless LAN->WLAN->Radio Settings->  ->Advanced Settings for Operation Mode *Access Client*

#### Fields in the menu Advanced Settings for Access Client Mode.



Field	Description
<b>Scan channels</b>	Choose the channels which the WLAN client automatically scans for available wireless networks.  Possible values: <ul style="list-style-type: none"> <li>• <i>All</i> (default value): All channels are scanned.</li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• <i>Auto</i>: The channel is automatically selected.</li> <li>• <i>User defined</i>: The desired channels can therefore be defined.</li> </ul>
<b>User Defined Channel Plan</b>	<p>Only for <b>Scan channels</b> = <i>User defined</i></p> <p>Define the channels which the WLAN client automatically scans for available wireless networks.</p>
<b>Roaming Profile</b>	<p>Select the roaming profile. The options available include typical roaming functions.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Normal Roaming</i> (default value): Standard roaming.</li> <li>• <i>Slow Roaming</i>: The WLAN client searches for available wireless networks as soon as the radio signal of the existing radio connection becomes weaker.</li> <li>• <i>No Roaming</i>: The WLAN client searches for available wireless networks if it is no longer connected to a wireless network.</li> <li>• <i>Custom Roaming</i>: Specify the individual roaming parameters.</li> </ul>
<b>Scan Threshold</b>	<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 <b>Roaming Profile</b> = <i>Custom Roaming</i>. The default value is <i>-70 dBm</i>.</p>
<b>Scan Interval</b>	<p>Indicates the interval in milliseconds after which the system scans for available wireless networks.</p> <p>The value can only be modified for <b>Roaming Profile</b> = <i>Custom Roaming</i>. The default value is <i>5000 ms</i>.</p>
<b>Min. Period Active Scan</b>	<p>Displays the minimum active scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for <b>Roaming Profile</b> = <i>Custom</i></p>

Field	Description
	<i>Roaming</i> . The default value is <i>10 ms</i> .
<b>Max. Period Active Scan</b>	<p>Displays the maximum active scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for <b>Roaming Profile</b> = <i>Custom Roaming</i>. The default value is <i>40 ms</i>.</p>
<b>Min. Period Passive Scan</b>	<p>Displays the minimum passive scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for <b>Roaming Profile</b> = <i>Custom Roaming</i>. The default value is <i>20 ms</i>.</p>
<b>Max. Period Passive Scan</b>	<p>Displays the maximum passive scanning time for a frequency in milliseconds.</p> <p>The value can only be modified for <b>Roaming Profile</b> = <i>Custom Roaming</i>. The default value is <i>120 ms</i>.</p>
<b>Max. Scan Duration</b>	<p>Displays the maximum scanning duration for a frequency in milliseconds.</p> <p>The value can only be modified for <b>Roaming Profile</b> = <i>Custom Roaming</i>. The default value is <i>50000 ms</i>.</p>

## 8.1.2 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 offers 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 170).

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

### 8.1.2.1 Edit or New

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

Radio Settings
Wireless Networks (VSS)
Bridge Links

Service Set Parameters	
Network Name (SSID)	default <input type="checkbox"/> Visible
Intra-cell Repeating	<input checked="" type="checkbox"/> Enabled
U-APSD	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Enabled
Bandwidth limitation for each WLAN client	
Rx Shaping	No limit ▼
Tx Shaping	No limit ▼
Advanced Settings	
Beacon Period	100 ms
DTIM Period	2
IGMP Snooping	<input type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 66: **Wireless LAN->WLAN->Wireless Networks (VSS)->**  **->New**

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

#### Fields in the menu **Service Set Parameters**

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


Field	Description
	<p>be permitted within a radio cell.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>WMM</b>	<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>
<b>U-APSD</b>	<p>Select whether the Unscheduled Automatic Power Save Delivery (U-APSD) mode is to be enabled.</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
<b>Security Mode</b>	<p>Select the <b>Security Mode</b> (encryption and authentication) for the wireless network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Inactive</i> (default value): Neither encryption nor authentication</li> <li>• <i>WEP 40</i>: WEP 40 bits</li> <li>• <i>WEP 104</i>: WEP 104 bits</li> <li>• <i>WPA-PSK</i>: WPA Preshared Key</li> <li>• <i>WPA Enterprise</i>: 802.11i/TKIP</li> </ul>
<b>Transmit Key</b>	<p>Only for <b>Security Mode</b> = <i>WEP 40</i> or <i>WEP 104</i></p> <p>Select one of the keys configured in <b>WEP Key</b> &lt;1 - 4&gt; as a default key.</p> <p>The default value is <i>Key 1</i>.</p>

Field	Description
<b>WEP Key 1-4</b>	<p>Only for <b>Security Mode</b> = <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>
<b>WPA Mode</b>	<p>Only for <b>Security Mode</b> = <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"> <li>• <i>WPA and WPA 2</i> (default value): <b>WPA and WPA 2</b> can be applied.</li> <li>• <i>WPA</i>: Only <b>WPA</b> is applied.</li> <li>• <i>WPA 2</i>: Only <b>WPA 2</b> is applied.</li> </ul>
<b>WPA Cipher</b>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for <b>WPA Mode</b> = <i>WPA</i> and <i>WPA and WPA 2</i></p> <p>Select the type of encryption with which to apply <b>WPA</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>AES</i>: AES is used.</li> <li>• <i>TKIP</i>: TKIP is used.</li> <li>• <i>AES and TKIP</i> (default value): AES or TKIP is used.</li> </ul>
<b>WPA2 Cipher</b>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for <b>WPA Mode</b> = <i>WPA 2</i> and <i>WPA and WPA 2</i></p> <p>Select the type of encryption with which to apply <b>WPA 2</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>AES</i>: AES is used.</li> <li>• <i>AES and TKIP</i> (default value): AES or TKIP is used.</li> </ul>
<b>Preshared Key</b>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i></p>



Field	Description
	<p>Enter the WPA password.</p> <p>Enter an ASCII string with 8 - 63 characters.</p>
	<p> <b>Note</b></p> <p>Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!</p>
<b>EAP Preauthentication</b>	<p>Only for <b>Security Mode</b> = <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
<b>Max. number of clients - hard limit</b>	<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>
<b>Max. number of clients - soft limit</b>	<p>Not all devices support this function.</p> <p>To avoid a radio module being fully utilised, you can set a "soft"</p>

Field	Description
	<p>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 <b>Max. number of clients - hard limit</b> is reached.</p> <p>The value of the <b>Max. number of clients - soft limit</b> must be the same as or less than that of the <b>Max. number of clients - hard limit</b>.</p> <p>The default value is <i>28</i>.</p> <p>You can disable this function if you set <b>Max. number of clients - soft limit</b> and <b>Max. number of clients - hard limit</b> to identical values.</p>
<b>Client Band select</b>	<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 <b>Client Band select</b> 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"> <li>• <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.</li> <li>• <i>2,4 GHz band preferred</i>: Preference is given to accepting clients in the 2.4 GHz band.</li> <li>• <i>5 GHz band preferred</i>: Preference is given to accepting clients in the 5 GHz band.</li> </ul>

#### Fields in the menu **MAC-Filter**

Field	Description
<b>Access Control</b>	<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>
<b>Allowed Addresses</b>	Use <b>Add</b> to make entries and enter the MAC addresses ( <b>MAC Address</b> ) of the clients to be permitted.

#### Fields in the menu **Bandwidth limitation for each WLAN client**



Field	Description
<b>Rx Shaping</b>	<p>Select a bandwidth limitation in the receive direction.</p> <p>Possible values are</p> <ul style="list-style-type: none"> <li>• <i>No limit</i> (default value)</li> <li>• <i>0,25 Mbit/s, 0,5 Mbit/s, 1 Mbit/s up to 10 Mbit/s</i> in single Mbit/s steps, <i>15 Mbit/s, 20 Mbit/s, 30 Mbit/s, 40 Mbit/s</i> and <i>50 Mbit/s</i>.</li> </ul>
<b>Tx Shaping</b>	<p>Select a bandwidth limitation in the transmit direction.</p> <p>Possible values are</p> <ul style="list-style-type: none"> <li>• <i>No limit</i> (default value)</li> <li>• <i>0,25 Mbit/s, 0,5 Mbit/s, 1 Mbit/s up to 10 Mbit/s</i> in single Mbit/s steps, <i>15 Mbit/s, 20 Mbit/s, 30 Mbit/s, 40 Mbit/s</i> and <i>50 Mbit/s</i>.</li> </ul>

#### Fields in the menu **Advanced Settings**

Field	Description
<b>Beacon Period</b>	<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> ms.</p>
<b>DTIM Period</b>	Enter the interval for the Delivery Traffic Indication Message

Field	Description
	<p>(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>
<b>IGMP Snooping</b>	<p>IGMP snooping reduces the data traffic and thus the network load, as Multicast packets from the LAN are not forwarded. Only those Multicast packets will be forwarded that are requested by the respective clients. When you enable IGMP snooping, IGMP snooping, therefore, provides the framework in which Multicast is applied.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

### 8.1.3 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.

#### 8.1.3.1 Edit



Choose the  icon to edit existing entries.

Fig. 67: 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
<b>Network Name (SSID)</b>	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
<b>Security Mode</b>	Select the security mode (encryption and authentication) for the wireless network.  Possible values: <ul style="list-style-type: none"> <li>• <i>Inactive</i> (default value): Neither encryption nor authentication</li> <li>• <i>WEP 40</i>: WEP 40 bits</li> <li>• <i>WEP 104</i>: WEP 104 bits</li> <li>• <i>WPA-PSK</i>: WPA Preshared Key</li> </ul>
<b>Transmit Key</b>	Only for <b>Security Mode</b> = <i>WEP 104</i>  Select one of the keys configured in <b>WEP Key</b> <1 - 4> as a default key.  The default value is <i>Key 1</i> .
<b>WEP Key 1 - 4</b>	Only for <b>Security Mode</b> = <i>WEP 40</i> , <i>WEP 104</i>  Enter the WEP key.

Field	Description
	<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>
<p><b>WPA Mode</b></p>	<p>Only for <b>Security Mode</b> = <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"> <li>• <i>WPA</i> (default value): Only WPA is used.</li> <li>• <i>WPA 2</i>: Only WPA2 is used.</li> </ul>
<p><b>Preshared Key</b></p>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i></p> <p>Enter the WPA password.</p> <p>Enter an ASCII string with 8 - 63 characters.</p>
<p><b>WPA Cipher</b></p>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i> and <b>WPA Mode</b> = <i>WPA</i></p> <p>Select which encryption method should be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>TKIP</i> (default value): Temporal Key Integrity Protocol</li> <li>• <i>AES</i>: Advanced Encryption Standard.</li> </ul> <p>Both encryption methods are rated as secure, with AES offering better performance.</p>
<p><b>WPA2 Cipher</b></p>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i> and <b>WPA Mode</b> = <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"> <li>• <i>AES</i> (default value): Advanced Encryption Standard.</li> <li>• <i>TKIP</i> : Temporal Key Integrity Protocol</li> </ul> <p>Both encryption methods are rated as secure, with AES offering better performance.</p>

### 8.1.3.2 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.

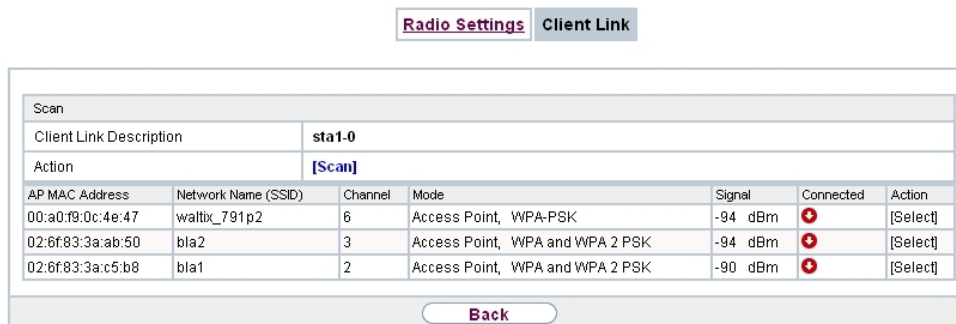




Fig. 68: Wireless LAN->WLAN->Client Link->Scan

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
<b>Client Link Description</b>	Displays the name of the client link you configured.
<b>Action</b>	<p>Start the scan by clicking on <b>Scan</b>.</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 <b>Scan</b>. The partner should then be found.</p>
<b>AP MAC Address</b>	Shows the MAC address of the remote client.
<b>Network Name (SSID)</b>	Displays the name of the remote client.
<b>Channel</b>	Shows the <b>Channel</b> used.

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

## 8.1.4 Bridge Links




### Note


Note that the Bridge Link function of this device series is incompatible with older Bridge Link or WDS implementations.

**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.

### 8.1.4.1 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

 **Make sure you change the standard preshared key! As long as the key remains unchanged, your device is not protected against unauthorised use.**

Basic Settings

Bridge Link Name (ID)	<input type="text"/>
Preshared Key	<input type="password" value="....."/>
Role	Master ▼

OK
Cancel

Fig. 69: 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
<b>Bridge Link Name (ID)</b>	<p>Depending on whether you operate the radio module as <b>Access-Point / Bridge Link Master</b> or as <b>Bridge Link Client</b> you create bridge links in master or slave mode.</p> <p>If the radio module is operated in <b>Access-Point / Bridge Link Master</b> mode, you can create bridge links in master as well as in slave mode; if it is operated in <b>Bridge Link Client</b> mode, only the slave mode is available.</p> <p>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>In <b>Bridge Link Client</b> mode, the bridge link is automatically set to slave mode. Enter the ID of the bridge link the device is to connect to.</p>
<b>Preshared Key</b>	<p>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.</p>
<b>Role</b>	<p>Here, you determine the role your device is to assume.</p> <p>Possible values:</p> <p><i>Master:</i> In master mode, clients connect to your device as slaves. In addition to the bridge link, your device can also assume the role of an access point for WLAN clients.</p> <p><i>Slave:</i> In slave mode, your device connects to one of the configured bridge links.</p>

## 8.2 Administration

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

## 8.2.1 Basic Settings

Fig. 70: **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
<b>Region</b>	<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> <p>The range of channels available for selection (<b>Channel</b> in the <b>Wireless LAN-&gt;WLAN-&gt;Radio Settings</b> menu) changes depending on the country setting.</p> <p>The default value is <i>Germany</i>.</p>

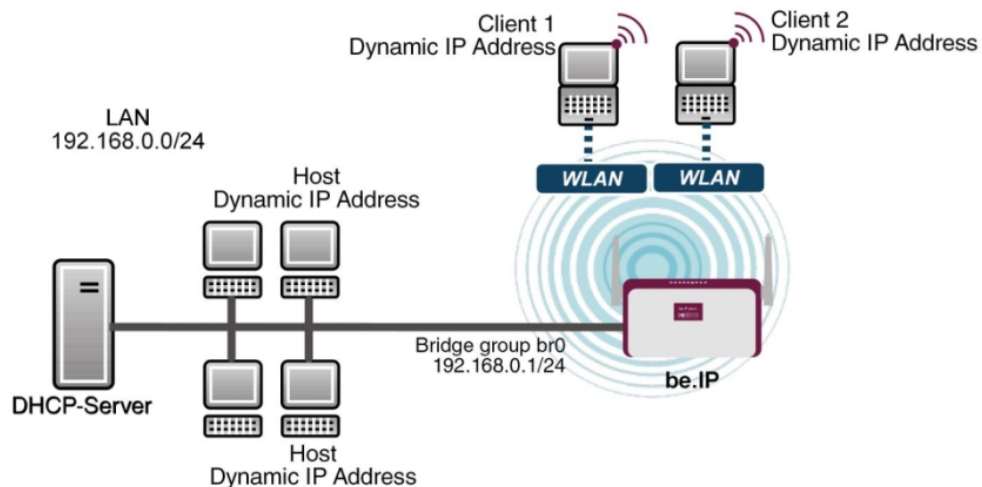
## 8.3 Configuration

### 8.3.1 WLAN - Configuration example

#### Requirements

- Your LAN is connected over the first Ethernet interface (Port **1**) of your device
- A client with Windows XP operating system and a WLAN card
- A DHCP server in the LAN distributes IP addresses from the network *192.168.0.0/24* for clients from the LAN and WLAN.
- A WAN connection.

### Example scenario



Example scenario WLAN with WPA-PSK

### Configuration target

Configuration of an additional WLANs (Guest-WLAN)

### Overview of Configuration Steps

#### Configuration Guest-WLAN



Field	Menu	Value
Network Name (SSID)	Wireless LAN->WLAN->Wireless Networks (VSS)->New	e.g. <i>Guest-WLAN</i>
Visible	Wireless LAN->WLAN->Wireless Networks (VSS)->New	Enabled
Security Mode	Wireless LAN->WLAN->Wireless Networks (VSS)->New	<i>WPA-PSK</i>
WPA Mode	Wireless LAN->WLAN->Wireless Networks (VSS)->New	<i>WPA2</i>
Preshared Key	Wireless LAN->WLAN->Wireless Networks (VSS)->New	e.g. <i>Super-Secret-2</i>

#### Enable WLAN Networks

Field	Menu	Value
Action	Wireless LAN->WLAN->Wireless	

Field	Menu	Value
	Networks (VSS)	

### Assign IP pool

Field	Menu	Value
Address Mode	LAN->IP Configuration->Interfaces->vss7-11 	Static
IP Address / Netmask	LAN->IP Configuration->Interfaces->vss7-11  ->Add	e.g. 192.168.0.10 / 255.255.255.0
IP Pool Name	Local Services->DHCP Server->IP Pool Configuration->New	e.g. Pool Guest
IP Address Range	Local Services->DHCP Server->IP Pool Configuration->New	e.g. 192.168.0.50 - 192.168.0.99
Interface	Local Services->DHCP Server->DHCP Configuration->New	vss7-11
IP Pool Name	Local Services->DHCP Server->DHCP Configuration->New	e.g. Pool Guest

### Setting up Firewall rules

Field	Menu	Value
Source	Firewall->Policies->IPv4 Filter Rules->New	WLAN_VSS7-11
Destination	Firewall->Policies->IPv4 Filter Rules->New	e.g. WAN_VDSL_TELEKOM
Service	Firewall->Policies->IPv4 Filter Rules->New	any
Action	Firewall->Policies->IPv4 Filter Rules->New	Access
Source	Firewall->Policies->IPv4 Filter Rules->New	WLAN_VSS7-11
Destination	Firewall->Policies->IPv4 Filter Rules->New	e.g. WAN
Service	Firewall->Policies->IPv4 Filter Rules->New	any
Action	Firewall->Policies->IPv4 Filter Rules->New	Deny

## Chapter 9 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.

### 9.1 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 recommend that you use the Wizard when initially configuring your WLAN infrastructure.

## 9.1.1 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 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.

## 9.1.2 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.

## 9.1.3 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.

### 9.1.3.1 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.

## 9.1.4 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.

## 9.2 Controller Configuration

In this menu, you make the basic settings for the wireless LAN controller.

### 9.2.1 General

**General**

Basic Settings	
Region	Germany <span style="float: right;">▼</span>
Interface	LAN_ENT-0 <span style="float: right;">▼</span>
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 <span style="float: right;">▼</span>

Fig. 71: 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
<b>Region</b>	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>
<b>Interface</b>	Select the interface to be used for the wireless controller.
<b>DHCP Server</b>	<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 bintec elmeg Gateway for example as a DHCP server, click on the <b>GUI</b> menu for this device under <b>Local Services-&gt;DHCP Server-&gt;DHCP Pool-&gt;New-&gt;Advanced Settings</b> in the <b>DHCP Options</b> field on the <b>Add</b> button. Select as <b>Option</b> <i>CAPWAP Controller</i> and in the <b>Value</b> 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 <b>System Management-&gt;Global Settings-&gt;System</b> menu in the <b>Manual WLAN Controller IP Address</b> field.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Internal</i>: Your device, on which the CAPWAP option 138 is active, assigns the IP addresses to the APs.</li> </ul>
<b>IP Address Range</b>	<p>Only for <b>DHCP Server</b> = <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
<b>Slave AP location</b>	<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"><li>• <i>Local (LAN)</i> (default value)</li><li>• <i>Remote (WAN)</i></li></ul> <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>
<b>Slave AP LED mode</b>	<p>Select the lighting scheme of the slave AP LEDs.</p> <p>Possible values:</p> <ul style="list-style-type: none"><li>• <i>State</i> (default value): All LEDs show their standard behavior.</li><li>• <i>Flashing</i>: Only the status LED flashes once per second.</li><li>• <i>Off</i>: All LEDs are deactivated.</li></ul>

## 9.2.2 Slave AP Autoprofile

The Wireless LAN Controller offers the option of automatically including and configuring an access point that is being integrated into the network accessible by the WLAN Controller. In order to be able to automatically assign a configuration to a new access point you have to configure a profile that is valid for all new access points that match certain criteria.

### 9.2.2.1 Edit or New

General Slave AP Autoprofile

Access Point Filter 2	
MAC Address	<input type="text"/> <input checked="" type="checkbox"/> All
IP Address / Netmask	<input type="text"/> / <input type="text"/>
Access Point Settings	
Location	<input type="text"/>
Description	<input type="text"/>
Radio 1	
Operation Mode	<input checked="" type="checkbox"/> Enabled
Active Radio Profile	2.4 GHz Radio Profile ▾
Assigned Wireless Network (VSS)	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <input style="width: 80%;" type="text"/> <input style="width: 20%;" type="button" value="Add"/> </div>
Radio 2	
Operation Mode	<input checked="" type="checkbox"/> Enabled
Active Radio Profile	2.4 GHz Radio Profile ▾
Assigned Wireless Network (VSS)	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <input style="width: 80%;" type="text"/> <input style="width: 20%;" type="button" value="Add"/> </div>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Fig. 72: Wireless LAN Controller->Controller Configuration->Slave AP Autoprofile->New**

The **Wireless LAN Controller->Controller Configuration->Slave AP Autoprofile->New** menu consists of the following fields:

#### Fields in the Access Point Filter menu

Field	Description
<b>MAC Address</b>	<p>Enter the MAC address of an access point that is to be configured automatically when it is integrated into the network.</p> <p>By default, <b>All</b> is activated so that the entry matches every new access point.</p>
<b>IP Address / Netmask</b>	<p>Enter an IP address and a netmask. You can enter host as well as network addresses so that you can filter for individual access points as well as for groups of access points from a specific subnet.</p>

#### Fields in the Access Point Settings menu

Field	Description
<b>Location</b>	Specify the location of the AP.
<b>Description</b>	Enter a unique description for the AP.

#### Fields in the Radio 1 or in the Radio 2

Field	Description
<b>Operating Mode</b>	<p>Wählen Sie aus, ob der Betriebsmodus vom verwendeten Funkmodulprofil bestimmt werden soll.</p> <p>The function is activated by selecting <i>Enabled</i>. The function is enabled by default.</p>
<b>Active Radio Profile</b>	<p>Only for <b>Operating Mode</b> = <i>Enabled</i></p> <p>Select a radio profile.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>2.4 GHz Radio Profile</i></li> <li>• <i>5 GHz Radio Profile</i></li> </ul>
<b>Assigned Wireless Network (VSS)</b>	<p>Only for <b>Operating Mode</b> = <i>Enabled</i></p> <p>Add a new radio profile with <b>Add</b>.</p>

## 9.3 Slave AP configuration

In this menu, you will find all of the settings that are required to manage the slave access points.



### 9.3.1 Slave Access Points

Slave Access Points
Radio Profiles
Wireless Networks (VSS)

Automatic Refresh Interval <input type="text" value="300"/> Seconds <span style="float: right;">Apply</span>							
View <input type="text" value="20"/> per page <span style="margin-left: 5px;">&lt;&lt; &gt;&gt;</span> Filter in <span style="margin-left: 5px;">None</span> <span style="margin-left: 5px;">equal</span> <span style="float: right;">Go</span>							
Location ▲	Name	IP Address	LAN MAC Address	Channel	Search Channel	Status	Action
		10.0.0.234	00:a0:f9:0b:cf:d8			❌ Discovered	🔄
INY	WI2040n	10.0.0.13	00:01:cd:06:76:fa	auto (Ch.6)/man.(Ch.1)	🟢	🟢 Managed	📶 ⬆️ ⬆️ 🗑️ 🔄
WNY	bintec W1002n	10.0.0.12	00:01:cd:0e:8f:04	auto (Ch.1)	🟢	🟢 Managed	📶 ⬆️ ⬆️ 🗑️ 🔄
Page: 1, Items: 1 - 3							
Actions							
Channel reallocation				<span style="border: 1px solid black; padding: 5px 15px;">START</span>			

Fig. 73: 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 Point 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
<b>Discovered</b>	The AP has registered at the wireless LAN controller. The controller has prompted the required parameters from the AP.
<b>Initialising</b>	The WLAN controller and the APs "communicate" via CAPWAP. The configuration is transferred and enabled to the APs.
<b>Managed</b>	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 <b>GUI</b> .
<b>No License Available</b>	The AP does not have an unassigned licence for this AP.



Status	Meaning
<b>Offline</b>	The AP is either administratively disabled or switched off or has its power supply cut off etc.

### 9.3.1.1 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	bintec W1002n						
Location	<input type="text"/>						
Name	bintec W1002n						
Description	<input type="text"/>						
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	<b>No Profile Selected!</b>						
Used Channel	1						
Transmit Power	Max. ▼						
Assigned Wireless Network (VSS)	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Profil</th> <th style="width: 40%;">MAC Address</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td>vss-1:Kefig</td> <td>02:6f:83:3a:af:98</td> <td></td> </tr> </tbody> </table>	Profil	MAC Address		vss-1:Kefig	02:6f:83:3a:af:98	
Profil	MAC Address						
vss-1:Kefig	02:6f:83:3a:af:98						
<input type="button" value="OK"/> <input type="button" value="Cancel"/>							

Fig. 74: 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
<b>Device</b>	Displays the type of device for the AP.

Field	Description
<b>Location</b>	Displays the locality of the AP. The locations are given numbers if no location has been entered. You can enter another locality.
<b>Name</b>	Displays the name of the AP. You can change the name.
<b>Description</b>	Enter a unique description for the AP.
<b>CAPWAP Encryption</b>	<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
<b>Operation Mode</b>	<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"> <li>• <i>On</i> (default value): The wireless module is used as an access point in your network.</li> <li>• <i>Off</i>: The wireless module is not active.</li> </ul>
<b>Active Radio Profile</b>	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.
<b>Channel</b>	<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</p>

Field	Description
	<p>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 APs actually support these channels.</p> <p>Possible values (according to the selected wireless module profile):</p> <ul style="list-style-type: none"> <li>• For <b>Active Radio Profile = 2.4 GHz Radio Profile</b> Possible values are <i>1</i> to <i>13</i> and <i>Auto</i> (default value).</li> <li>• For <b>Active Radio Profile = 5 GHz Radio Profile</b> Possible values are <i>36</i>, <i>40</i>, <i>44</i>, <i>48</i> and <i>Auto</i> (default value)</li> </ul>
<b>Used Channel</b>	<p>Only for managed APs.</p> <p>Displays the channel that is currently in use.</p>
<b>Transmit Power</b>	<p>Displays the transmission power. You can select another transmission power.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Max.</i> (default value): The maximum antenna power is used.</li> <li>• <i>5 dBm</i></li> <li>• <i>8 dBm</i></li> <li>• <i>11 dBm</i></li> <li>• <i>14 dBm</i></li> <li>• <i>16 dBm</i></li> <li>• <i>17 dBm</i></li> </ul>
<b>Assigned Wireless Network (VSS)</b>	<p>Displays the wireless networks that are currently assigned.</p>

## 9.3.2 Radio Profiles





Slave Access Points		Radio Profiles		Wireless Networks (VSS)	
Radio Profiles	Configured Radio Modules	Operation Band	Wireless Mode		
2.4 GHz Radio Profile	0	2.4 GHz In/Outdoor	802.11 b/g/n		
5 GHz Radio Profile	0	5 GHz Indoor	802.11 a/n		
<a href="#">New</a>					

Fig. 75: 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**).

### 9.3.2.1 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)	
<b>Radio Profile Definition</b>					
Description	<input type="text"/>				
Operation Mode	Access Point ▾				
Operation Band	2.4 GHz In/Outdoor ▾				
Number of Spatial Streams	3 ▾				
<b>Performance Settings</b>					
Wireless Mode	802.11b/g/n ▾				
Max. Transmission Rate	Auto ▾				
Burst Mode	<input type="checkbox"/> Enabled				
Airtime fairness	<input checked="" type="checkbox"/> Enabled				
<b>Advanced Settings</b>					
Channel Plan	All ▾				
Beacon Period	<input type="text" value="100"/> ms				
DTIM Period	<input type="text" value="2"/>				
RTS Threshold	<input type="text" value="2347"/>				
Short Guard Interval	<input type="checkbox"/> Enabled				
Short Retry Limit	<input type="text" value="7"/>				
Long Retry Limit	<input type="text" value="4"/>				
Fragmentation Threshold	<input type="text" value="2346"/> Bytes				
Cyclic Background Scanning	<input type="checkbox"/> Enabled				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>					

Fig. 76: 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
<b>Description</b>	Enter the desired description of the wireless module profile.
<b>Operation Mode</b>	<p>Define the mode in which the wireless module profile is to be operated.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Off</i> (default value): The wireless module profile is not active.</li> <li>• <i>Access Point</i>: Your device is used as an access point in</li> </ul>

Field	Description
	your network.
<b>Operation Band</b>	<p>Select the frequency band of the wireless module profile.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>2.4 GHz In/Outdoor</i> (default value): Your device is operated at 2.4 GHz inside or outside buildings.</li> <li>• <i>5 GHz Indoor</i>: Your device is operated at 5 GHz inside buildings.</li> <li>• <i>5 GHz Outdoor</i>: Your device is operated at 5 GHz outside buildings.</li> <li>• <i>5 GHz In/Outdoor</i>: Your device is operated at 5 GHz inside or outside buildings.</li> <li>• <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.</li> </ul>
<b>Bandwidth</b>	<p>Not for <b>Operation Band</b> = <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"> <li>• <i>20 MHz</i> (default value): One channel with 20 MHz bandwidth is used.</li> <li>• <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.</li> <li>• <i>80 MHz</i>: In 802.11 ac mode, a bandwidth of 80 MHz is additionally available.</li> </ul>

#### Fields in the menu Performance Settings

Field	Description
<b>Wireless Mode</b>	<p>Select the wireless technology that the access point is to use.</p> <p>For <b>Operation Band</b> = <i>2.4 GHz In/Outdoor</i></p> <p>Possible values:</p>


Field	Description
	<ul style="list-style-type: none"> <li>• <i>802.11g</i>: The device operates only in accordance with 802.11g. 802.11b clients have no access.</li> <li>• <i>802.11b</i>: Your device operates only in accordance with 802.11b and forces all clients to adapt to it.</li> <li>• <i>802.11 mixed (b/g)</i>: Your device adapts to the client technology and operates according to either 802.11b or 802.11g.</li> <li>• <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.</li> <li>• <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).</li> <li>• <i>802.11b/g/n</i>: Your device operates according to either 802.11b, 802.11g or 802.11n.</li> <li>• <i>802.11g/n</i>: Your device operates according to either 802.11g or 802.11n.</li> <li>• <i>802.11n</i>: Your device operates only according to 802.11n.</li> </ul> <p><b>For Operation Band</b> = 5 GHz Indoor, 5 GHz Outdoor, 5 GHz In/Outdoor or 5.8 GHz Outdoor</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>802.11a</i>: The device operates only in accordance with 802.11a.</li> <li>• <i>802.11n</i>: Your device operates only according to 802.11n.</li> <li>• <i>802.11a/n</i>: Your device operates according to either 802.11a or 802.11n.</li> <li>• <i>802.11a/n</i>: Your device operates according to 802.11ac, 802.11a or 802.11n.</li> <li>• <i>802.11a/n</i>: Your device operates according to either 802.11ac or 802.11n.</li> </ul>
<b>Number of Spatial Streams</b>	Select how many traffic flows are to be used in parallel.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• 3: Three traffic flows are used.</li> <li>• 2: Two traffic flows are used.</li> <li>• 1: One traffic flow is used.</li> </ul>
<b>Max. Transmission Rate</b>	<p>Select the transmission speed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Auto</i> (default value): The transmission speed is determined automatically.</li> <li>• <i>&lt;Value&gt;</i>: According to setting for <b>Operation Band, Bandwidth, Number of Spatial Streams</b> and <b>Wireless Mode</b> various fixed values in mbps are available.</li> </ul>
<b>Airtime fairness</b>	<p>This function is not available for all devices.</p> <p>The <b>Airtime fairness</b> 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 function is only applied to unprioritized frames of the WMM Classe "Background".</p>
<b>Cyclic Background Scanning</b>	<p>Not all devices support this function.</p> <p>You can enable the <b>Cyclic Background Scanning</b> 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 <b>Cyclic Background Scanning</b>.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is not activated by default.</p>



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

#### Fields in the menu **Advanced Settings**

Field	Description
<b>Channel Plan</b>	<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"> <li>• <i>All</i>: All channels can be dialled when a channel is selected.</li> <li>• <i>Auto</i>: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided.</li> <li>• <i>User defined</i>: You can select the desired channels yourself.</li> </ul>
<b>User Defined Channel Plan</b>	<p>Only for <b>Channel Plan</b> = <i>User defined</i></p> <p>The currently selected channels are displayed here.</p> <p>With <b>Add</b> 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>
<b>Beacon Period</b>	<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.</p>
<b>DTIM Period</b>	<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 multic-</p>

Field	Description
	<p>ast 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>
<b>RTS Threshold</b>	<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>
<b>Short Guard Interval</b>	<p>Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.</p>
<b>Short Retry Limit</b>	<p>Enter the maximum number of attempts to send a frame with length less than or equal to the value defined in <b>RTS Threshold</b>. 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>
<b>Long Retry Limit</b>	<p>Enter the maximum number of attempts to send a data packet of length greater than the value defined in <b>RTS Threshold</b>. 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>
<b>Fragmentation Threshold</b>	<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>

### 9.3.3 Wireless Networks (VSS)




Slave Access Points		Radio Profiles		Wireless Networks (VSS)			
VSS Description	Network Name (SSID)	Number of associated radio modules	Security	Status	Action		
vss-1	Funkwerk-ec	0	WPA-PSK				
Assign unassigned VSS to all radio modules		<input type="button" value="START"/>					
<input type="button" value="New"/>							


Fig. 77: 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.

#### 9.3.3.1 Edit or New

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

Slave Access Points
Radio Profiles
Wireless Networks (VSS)

Service Set Parameters	
Network Name (SSID)	<input type="text"/> <input checked="" type="checkbox"/> Visible
Intra-cell Repeating	<input checked="" type="checkbox"/> Enabled
ARP Processing	<input type="checkbox"/> Enabled
WMM	<input checked="" type="checkbox"/> Enabled
Security Settings	
Security Mode	Inactive <input type="button" value="v"/>
Client load balancing	
Max. number of clients - hard limit	<input type="text" value="32"/>
Max. number of clients - soft limit	<input type="text" value="28"/>
Client Band select	Disabled - optimized for fast roaming <input type="button" value="v"/>
MAC-Filter	
Access Control	<input type="checkbox"/> Enabled
Dynamic blacklisting	<input checked="" type="checkbox"/> Enabled
Failed attempts per Time	<input type="text" value="10"/> / <input type="text" value="60"/> Seconds
Blacklist blocktime	<input type="text" value="500"/> Seconds
VLAN	
VLAN	<input type="checkbox"/> Enabled
Bandwidth limitation	
Rx Shaping	No limit <input type="button" value="v"/>
Tx Shaping	No limit <input type="button" value="v"/>

**Fig. 78: 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
<b>Network Name (SSID)</b>	Enter the name of the wireless network (SSID).  Enter an ASCII string with a maximum of 32 characters.  Also select whether the <b>Network Name (SSID)</b> is to be transmitted.  The network name is displayed by selecting <i>Visible</i> .  It is visible by default.
<b>Intra-cell Repeating</b>	Select whether communication between the WLAN clients is to

Field	Description
	<p>be permitted within a radio cell.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>ARP Processing</b>	<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>
<b>WMM</b>	<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
<b>Security Mode</b>	<p>Select the security mode (encryption and authentication) for the wireless network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Inactive</i> (default value): Neither encryption nor authentication</li> <li>• <i>WEP 40</i>: WEP 40 bits</li> <li>• <i>WEP 104</i>: WEP 104 bits</li> <li>• <i>WPA-PSK</i>: WPA Preshared Key</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>WPA Enterprise</i>: 802.11x</li> </ul>
<b>Transmit Key</b>	<p>Only for <b>Security Mode</b> = <i>WEP 40</i> or <i>WEP 104</i></p> <p>Select one of the keys configured in <b>WEP Key</b> as a standard key.</p> <p>The default value is <i>Key 1</i>.</p>
<b>WEP Key 1-4</b>	<p>Only for <b>Security Mode</b> = <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>
<b>WPA Mode</b>	<p>Only for <b>Security Mode</b> = <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"> <li>• <i>WPA and WPA 2</i> (default value): WPA and WPA 2 can be used.</li> <li>• <i>WPA</i>: Only WPA is used.</li> <li>• <i>WPA 2</i>: Only WPA2 is used.</li> </ul>
<b>WPA Cipher</b>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for <b>WPA Mode</b> = <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"> <li>• <i>TKIP</i> (default value): TKIP is used.</li> <li>• <i>AES</i>: AES is used.</li> <li>• <i>AES and TKIP</i>: AES or TKIP is used.</li> </ul>
<b>WPA2 Cipher</b>	<p>Only for <b>Security Mode</b> = <i>WPA-PSK</i> and <i>WPA Enterprise</i> and for <b>WPA Mode</b> = <i>WPA 2</i> and <i>WPA and WPA 2</i></p>

Field	Description
	<p>Select the type of encryption you want to apply to WPA2.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>AES</i> (default value): AES is used.</li> <li>• <i>TKIP</i>: TKIP is used.</li> <li>• <i>AES and TKIP</i>: AES or TKIP is used.</li> </ul>
<b>Preshared Key</b>	<p>Only for <b>Security Mode</b> = <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>
<b>Radius Server</b>	<p>You can control access to a wireless network via a RADIUS server.</p> <p>With <b>Add</b>, you can create new entries. Enter the IP address and the password of the RADIUS server.</p>
<b>EAP Preauthentication</b>	<p>Only for <b>Security Mode</b> = <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
<b>Max. number of clients - hard limit</b>	<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 wire-</p>

Field	Description
	<p>less 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>
<p><b>Max. number of clients - soft limit</b></p>	<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 <b>Max. number of clients - hard limit</b> is reached.</p> <p>The value of the <b>Max. number of clients - soft limit</b> must be the same as or less than that of the <b>Max. number of clients - hard limit</b>.</p> <p>The default value is <i>28</i>.</p> <p>You can disable this function if you set <b>Max. number of clients - soft limit</b> and <b>Max. number of clients - hard limit</b> to identical values.</p>
<p><b>Client Band select</b></p>	<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 <b>Client Band select</b> 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"> <li>• <i>Disabled - optimized for fast roaming</i> (default)</li> </ul>



Field	Description
	<p>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.</p> <ul style="list-style-type: none"> <li>• <i>2,4 GHz band preferred</i>: Preference is given to accepting clients in the 2.4 GHz band.</li> <li>• <i>5 GHz band preferred</i>: Preference is given to accepting clients in the 5 GHz band.</li> </ul>

#### Fields in the menu **MAC-Filter**

Field	Description
<b>Access Control</b>	<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>
<b>Allowed Addresses</b>	<p>Use <b>Add</b> to make entries and enter the MAC addresses (<b>MAC Address</b>) of the clients to be permitted.</p>
<b>Dynamic blacklisting</b>	<p>You can use the <b>Dynamic blacklisting</b> 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 <b>Wireless LAN Controller-&gt;Monitoring-&gt;Rogue Clients</b> menu.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is activated by default.</p>
<b>Failed attempts per Time</b>	<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>

Field	Description
<b>Blacklist blocktime</b>	<p>Enter the time for which an entry in the dynamic blacklist remains valid.</p> <p>Default value is <i>500</i> seconds.</p>

#### Fields in the menu VLAN

Field	Description
<b>VLAN</b>	<p>Select whether the VLAN segmentation is to be used for this wireless network.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>VLAN ID</b>	<p>Enter the number that identifies the VLAN.</p> <p>Possible values are <i>2</i> to <i>4094</i>.</p> <p>VLAN ID <i>1</i> is not possible as it is already in use.</p>

#### Fields in the menu Bandwidth limitation for each WLAN client

Field	Description
<b>Rx Shaping</b>	<p>Select a bandwidth limitation in the receive direction.</p> <p>Possible values are</p> <ul style="list-style-type: none"> <li>• <i>No limit</i> (default value)</li> <li>• <i>0,25 Mbit/s, 0,5 Mbit/s, 1 Mbit/s up to 10 Mbit/s in single Mbit/s steps, 15 Mbit/s, 20 Mbit/s, 30 Mbit/s, 40 Mbit/s and 50 Mbit/s.</i></li> </ul>
<b>Tx Shaping</b>	<p>Select a bandwidth limitation in the transmit direction.</p> <p>Possible values are</p> <ul style="list-style-type: none"> <li>• <i>No limit</i> (default value)</li> <li>• <i>0,25 Mbit/s, 0,5 Mbit/s, 1 Mbit/s up to 10 Mbit/s in single Mbit/s steps, 15 Mbit/s, 20 Mbit/s, 30 Mbit/s, 40 Mbit/s and 50 Mbit/s.</i></li> </ul>

## 9.4 Monitoring

This menu is used to monitor your WLAN infrastructure.



### Note

In order to ensure adequate timing between the WLAN Controller and the connected Slave APs, the internal time server of the WLAN Controller should be enabled.

## 9.4.1 WLAN Controller

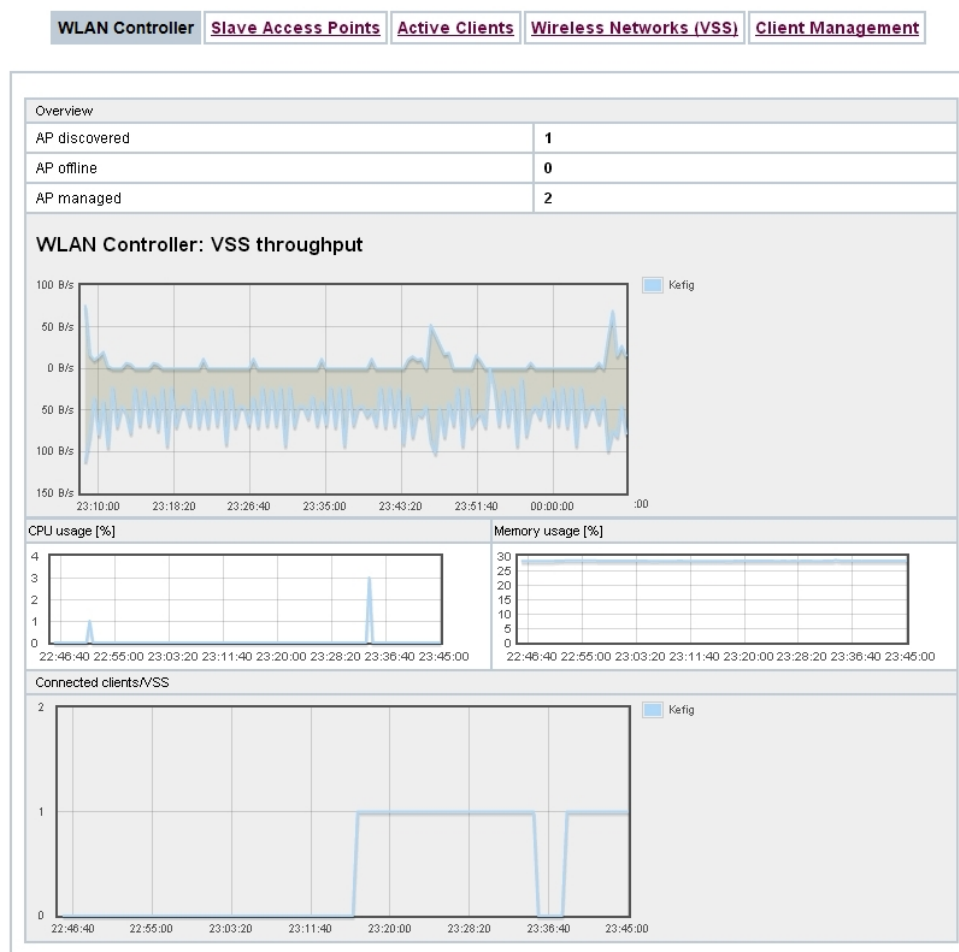


Fig. 79: Wireless LAN Controller->Monitoring->WLAN Controller

In the **Wireless LAN Controller->Monitoring->WLAN Controller** menu, an overview of the most relevant Wireless LAN Controller parameters is displayed. The display is refreshed every 30 seconds.

### Values in the Overview list

Status	Meaning
AP discovered	Displays the number of discovered access points.
AP offline	Displays the number of access points not connected to the Wireless LAN Controller.

Status	Meaning
<b>AP managed</b>	Displays the number of managed access points.
<b>WLAN Controller: VSS throughput</b>	Displays the data traffic in receive and transmit direction in bytes per second.
<b>CPU usage [%]</b>	Displays the percentaged CPU load over time.
<b>Memory usage [%]</b>	Displays the percentaged memory consumption over time.
<b>Connected clients/VSS</b>	Displays the number of connected clients per wireless network (VSS) over time.

## 9.4.2 Slave Access Points

[WLAN Controller](#)
[Slave Access Points](#)
[Active Clients](#)
[Wireless Networks \(VSS\)](#)
[Client Management](#)

Automatic Refresh Interval  Seconds

View  per page   Filter in

Location	Name	IP Address	LAN MAC Address	Channel	Tx Bytes	Rx Bytes		
INY	WI2040n	10.0.0.13	00:01:cd:06:76:fa	auto (Ch.6)/man.(Ch.1)	566634	60784		
WNY	bintec W1002n	10.0.0.12	00:01:cd:0e:8f:04	auto (Ch.1)	4832	6111		
		10.0.0.234	00:a0:f9:0b:cf:d8		0	0		

Page: 1, Items: 1 - 3

Fig. 80: Wireless LAN Controller->Monitoring->Slave Access Points

The menu **Wireless LAN Controller->Monitoring->Slave Access Points** shows a survey of all detected access points. Each access point is displayed along with the following parameters: **Location**, **Name**, **IP Address**, **LAN MAC Address**, **Channel**, **Tx Bytes** and **Rx Bytes**. Moreover, you can see if an access point is in *Managed* or *Discovered* state.

Via the icon, you can open a summary with additional details about the **Slave Access Points**.

### 9.4.2.1 Overview

In the **Overview** menu, additional information about the selected access point is displayed. The display is refreshed every 30 seconds.



Fig. 81: Wireless LAN Controller->Monitoring->Slave Access Points->Overview

#### Values in the Overview list

Status	Meaning
Throughput	Displays the received and transmitted data traffic per radio module over time.
Connected clients	Displays the number of connected clients per radio module over time.

#### 9.4.2.2 Radio 1

In the **Radio Module** menu, the received and transmitted data traffic per client is displayed over time. Each graph in the display is distinctly assigned to a client by its color and MAC address.

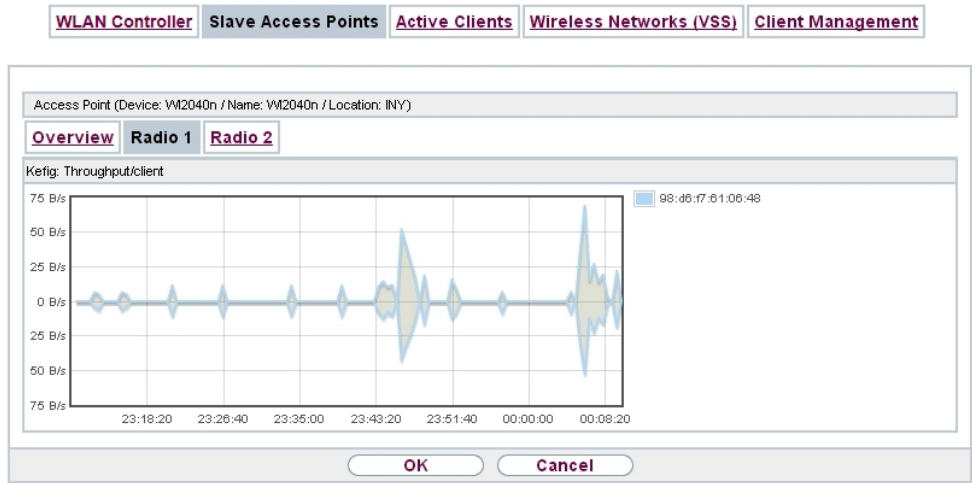


Fig. 82: Wireless LAN Controller->Monitoring->Slave Access Points->Radio

**Values in the Radio list**

Status	Meaning
Throughput/client	Displays the received and transmitted data traffic per client over time.

### 9.4.3 Active Clients

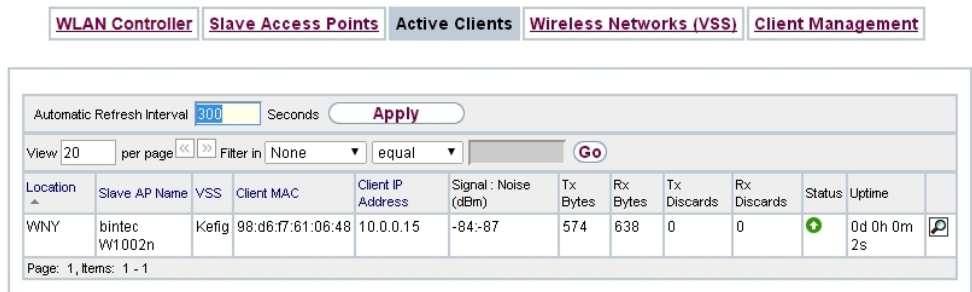



Fig. 83: Wireless LAN Controller->Monitoring->Active Clients

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, Slave AP Name, VSS, Client MAC, Client IP Address, Signal : Noise (dBm) , Tx Bytes, Rx Bytes, Tx Discards, Rx Discards, 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.

Via the  icon, you can open a summary with additional details about the **Active Clients**.

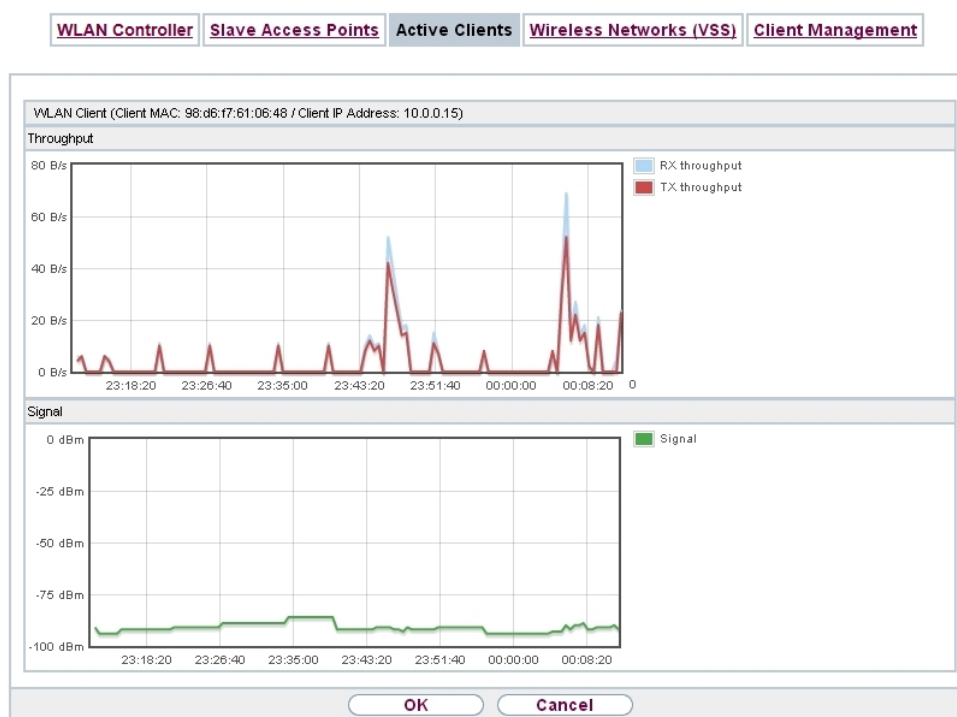



Fig. 84: Wireless LAN Controller->Monitoring->Active Clients-> 

## Value in the list WLAN Client list

Status	Meaning
Throughput	Displays the data traffic - separated into received and transmitted traffic - for the selected WLAN client over time.
Signal	Displays the signal strength of the selected WLAN client over time.



## 9.4.4 Wireless Networks (VSS)

WLAN Controller		Slave Access Points		Active Clients		Wireless Networks (VSS)		Client Management	
View	20	per page	<< >>	Filter in	None		equal		Go
Location	Slave AP Name	VSS	MAC Address (VSS)		Channel	Status			
INY	WI2040n	Kefig	02:6f:83:69:08:90		auto (Ch.6)	+			
INY	WI2040n	Kefig	02:6f:83:69:0c:58		man.(Ch.1)	+			
WNY	bintec WI1002n	Kefig	02:6f:83:3a:af:98		auto (Ch.1)	+			
Page: 1, Items: 1 - 3									

Fig. 85: Wireless LAN Controller->Monitoring->Wireless Networks (VSS)

In the **Wireless LAN Controller->Monitoring->Wireless Networks (VSS)** menu, 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**).

## 9.4.5 Client Management

WLAN Controller		Slave Access Points		Active Clients		Wireless Networks (VSS)		Client Management	
View	20	per page	<< >>	Filter in	None		equal		Go
Location	Slave AP Name	VSS	MAC Address (VSS)		Active Clients	2,4/5 GHz changeover	Denied Clients soft/hard		
INY	WI2040n	Kefig	02:6f:83:69:08:90		0	0	0/0	🗑️	
INY	WI2040n	Kefig	02:6f:83:69:0c:58		0	0	0/0	🗑️	
WNY	bintec WI1002n	Kefig	02:6f:83:3a:af:98		0	0	0/0	🗑️	
Page: 1, Items: 1 - 3									
Apply									

Fig. 86: Wireless LAN Controller->Monitoring->Client Management

The **Wireless LAN Controller->Monitoring->Client Management** menu displays information on the client management by the access points. You can, e.g., see the number of connected clients, 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.

## 9.5 Neighbor Monitoring

This menu serves the monitoring of remote access points.

### 9.5.1 Neighbor APs

Neighbor APs Rogue APs Rogue Clients

View 20	per page	Filter in: None	equal	Go			
SSID	MAC Address	Signal dBm	Channel	Security	Last seen	Strongest signal received by	Total detections
Page: 1							
Actions							
New Neighborscan				START			

Fig. 87: Wireless LAN Controller->Neighbor Monitoring->Neighbor APs

In the **Wireless LAN Controller->Neighbor 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.

## 9.5.2 Rogue APs

[Neighbor APs](#)   [Rogue APs](#)   [Rogue Clients](#)

View 20 per page << >> Filter in: None equal

SSID	MAC Address	Signal dBm	Channel	Last seen	Detected via AP	Accepted
Page: 1						
Actions						
New Neighborscan			<input type="button" value="START"/>			
<input type="button" value="OK"/>						

Fig. 88: Wireless LAN Controller->Neighbor 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->Neighbor 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.

### 9.5.3 Rogue Clients

Neighbor APs
Rogue APs
Rogue Clients


  

View <input type="text" value="20"/> per page << >> Filter in <span style="border: 1px solid black; padding: 2px;">None</span> equal <input type="text" value=""/> <span style="border: 1px solid black; padding: 2px; color: red;">Go</span>										
Rogue Client MAC Address	Network Name (SSID)	Attacked Access Point	Signal dBm	Type of attack	First seen	Last seen	Static Blacklist Select all/ Deselect all	Delete Select all/ Deselect all		
Page: 1										
<span style="border: 1px solid black; border-radius: 10px; padding: 5px 15px;">New</span>					<span style="border: 1px solid black; border-radius: 10px; padding: 5px 15px;">Apply</span>					

Fig. 89: Wireless LAN Controller->Neighbor Monitoring->Rogue Clients

The **Wireless LAN Controller->Neighbor 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
<b>Rogue Client MAC Address</b>	Displays the MAC address of the client on the blacklist.
<b>Network Name (SSID)</b>	Displays the SSID involved.
<b>Attacked Access Point</b>	Displays the AP concerned.
<b>Signal dBm</b>	Displays the signal strength of the client during the attempted access.
<b>Type of attack</b>	This displays the type of potential attack, e. g. an incorrect authentication.
<b>First seen</b>	Displays the time of the first registered attempted access.
<b>Last seen</b>	Displays the time of the last registered attempted access.
<b>Static Blacklist</b>	You can categorise a rogue client as untrustworthy by selecting the checkbox in the <b>Static Blacklist</b> column. The block on the client does not then end automatically, rather you need to lift it manually.
<b>Delete</b>	You can delete entries with the  symbol.

### 9.5.3.1 New

Choose the **New** button to configure additional blacklist entries.

Fig. 90: **Wireless LAN Controller->Neighbor Monitoring->Rogue Clients->New**

The menu consists of the following fields:

#### Fields in the New Blacklist Entry menu

Field	Description
<b>Rogue Client MAC Address</b>	Enter the MAC address of the client you intend to include in the static blacklist.
<b>Network Name (SSID)</b>	Pick the wireless network you want to exclude the rogue client from.

## 9.6 Maintenance

This menu is used for the maintenance of your managed APs.

## 9.6.1 Firmware Maintenance

**Firmware Maintenance**

**Managed Access Points**

View  per page << >> Filter in None equal Go

Update firmware Select all/ Deselect all	Location ▲	Device	IP Address	LAN MAC Address	Firmware Version	Status
<input type="checkbox"/>	INY	WI2040n	10.0.0.13	00:01:cd:06:76:fa	V.9.1 Rev. 7 (Beta 5) IPSec from 2013/09/20 00:00:00	
<input type="checkbox"/>	WNY	bintec WI1002n	10.0.0.12	00:01:cd:0e:8f:04	V.9.1 Rev. 7 (Patch 2) IPSec from 2014/01/20 00:00:00	

Page: 1, Items: 1 - 2

Action	<span style="border: 1px solid black; padding: 2px;">Update system software ▼</span>
Source Location	<span style="border: 1px solid black; padding: 2px;">HTTP server ▼</span>
URL	<input style="width: 90%;" type="text"/>

OK
Cancel

*Fig. 91: 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
<b>Image already exists.</b>	The software image already exists; no update is required.
<b>Error</b>	An error has occurred.
<b>Running</b>	The operation is currently in progress.
<b>Done</b>	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
<b>Action</b>	<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"> <li>• <i>Update system software</i>: You can also start an update of the system software.</li> <li>• <i>Save configuration with state information</i>: You can save a configuration which contains the AP status information.</li> </ul>
<b>Source Location</b>	<p>Select the source for the action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>HTTP server</i> (default value): The file is stored respectively on a remote server specified in the <b>URL</b>.</li> <li>• <i>Current Software from Update Server</i>: The file is on the official update server. (Only for <b>Action= Update system software</b>)</li> <li>• <i>TFTP server</i>: The file is stored respectively on a TFTP server specified in the <b>URL</b>.</li> </ul>
<b>URL</b>	<p>Only for <b>Source Location = HTTP server</b> or <b>TFTP server</b>  Enter the URL of the update server from which the system software file is loaded or on which the configuration file is saved.</p>

## Chapter 10 Networking

### 10.1 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**.

#### 10.1.1 IPv4 Route Configuration

A list of all configured routes is displayed in the **Network->Routes->IPv4 Route Configuration** menu.

In the ex works state, a predefined entry with the parameters **Destination IP Address** = *192.168.0.0*, **Netmask** = *255.255.255.0*, **Gateway** = *192.168.0.250*, **Interface** = *LAN\_EN1-0*, **Route Type** = *Network Route via Interface* is displayed.

##### 10.1.1.1 Edit or New

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



IPv4 Route Configuration		IPv6 Route Configuration	IPv4 Routing Table	IPv6 Routing Table	Options
<b>Basic Parameters</b>					
Route Type	Network Route via Interface ▼				
Interface	None ▼				
Route Class	<input checked="" type="radio"/> Standard <input type="radio"/> Extended				
<b>Route Parameters</b>					
Destination IP Address/Netmask	<input type="text"/> / <input type="text"/>				
Local IP Address	<input type="text" value="0.0.0.0"/>				
Metric	<input type="text" value="1"/> ▼				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>					

Fig. 92: Network->Routes->IPv4 Route Configuration->New with Route Class = Standard.

If the *Extended* option is selected for the **Route Class**, an extra configuration section opens.

IPv4 Route Configuration		IPv6 Route Configuration	IPv4 Routing Table	IPv6 Routing Table	Options
<b>Basic Parameters</b>					
Route Type	Network Route via Interface ▼				
Interface	None ▼				
Route Class	<input type="radio"/> Standard <input checked="" type="radio"/> Extended				
<b>Route Parameters</b>					
Destination IP Address/Netmask	<input type="text"/> / <input type="text"/>				
Local IP Address	<input type="text" value="0.0.0.0"/>				
Metric	<input type="text" value="1"/> ▼				
<b>Extended Route Parameters</b>					
Description	<input type="text"/>				
Source Interface	<input type="text" value="Any"/> ▼				
Source IP Address/Netmask	<input type="text" value="0.0.0.0"/> / <input type="text" value="0.0.0.0"/>				
Layer 4 Protocol	<input type="text" value="Any"/> ▼				
Source Port	<input type="text" value="Any"/> ▼ Port <input type="text" value="-1"/> to Port <input type="text" value="-1"/>				
Destination Port	<input type="text" value="Any"/> ▼ Port <input type="text" value="-1"/> to Port <input type="text" value="-1"/>				
DSCP / TOS Value	<input type="text" value="Ignore"/> ▼				
Mode	<input type="text" value="Dialup and wait"/> ▼				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>					


Fig. 93: Network->Routes->IPv4 Route Configuration->New with Route Class = Extended

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"> <li>• <i>Default Route via Interface</i>: Route via a specific interface which is to be used if no other suitable route is available.</li> <li>• <i>Default Route via Gateway</i>: Route via a specific gateway which is to be used if no other suitable route is available.</li> <li>• <i>Host Route via Interface</i>: Route to an individual host via a specific interface.</li> <li>• <i>Host Route via Gateway</i>: Route to an individual host via a specific gateway.</li> <li>• <i>Network Route via Interface</i> (default value): Route to a network via a specific interface.</li> <li>• <i>Network Route via Gateway</i>: Route to a network via a specific gateway.</li> </ul> <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"> <li>• <i>Default Route Template per DHCP</i>: The information of the gateway to be used is received via DHCP and integrated into the route.</li> <li>• <i>Host Route Template per DHCP</i>: The settings received by DHCP are supplemented by routing information about a particular host.</li> <li>• <i>Network Route Template per DHCP</i>: The settings received by DHCP are supplemented by routing information about a particular network.</li> </ul>

Field	Description
	<div style="border: 1px solid gray; padding: 10px; margin: 10px 0;">  <p><b>Note</b></p> <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>
<b>Interface</b>	Select the interface to be used for this route.
<b>Route Class</b>	<p>Select the type of <b>Route Class</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (default value): Defines a route with the default parameters.</li> <li>• <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.</li> </ul>

#### Fields in the menu **Route Parameters**

Field	Description
<b>Local IP Address</b>	<p>Only for <b>Route Type</b> = <i>Default Route via Interface</i>, <i>Host Route via Interface</i> or <i>Network Route via Interface</i></p> <p>Enter the own IP address of the router on the selected interface.</p>
<b>Destination IP Address/Netmask</b>	<p>Only for <b>Route Type</b> <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> <p>When <b>Route Type</b> = <i>Network Route via Interface</i></p> <p>Also enter the relevant netmask in the second field.</p>

Field	Description
<b>Gateway IP Address</b>	<p>Only for <b>Route Type</b> = <i>Default Route via Gateway, Host Route via Gateway</i> or <i>Network Route via Gateway</i></p> <p>Enter the IP address of the gateway to which your device is to forward the IP packets.</p>
<b>Metric</b>	<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 0 to 15. The default value is 1.</p>

#### Fields in the menu **Extended Route Parameters**

Field	Description
<b>Description</b>	Enter a description for the IP route.
<b>Source Interface</b>	<p>Select the interface over which the data packets are to reach the device.</p> <p>The default value is <i>None</i>.</p>
<b>Source IP Address/ Netmask</b>	Enter the IP address and netmask of the source host or source network.
<b>Layer 4 Protocol</b>	<p>Select a protocol.</p> <p>Possible values: <i>AH, Any, ESP, GRE, ICMP, IGMP, L2TP, OSPF, PIM, TCP, UDP</i>.</p> <p>The default value is <i>Any</i>.</p>
<b>Source Port</b>	<p>Only for <b>Layer 4 Protocol</b> = <i>TCP</i> or <i>UDP</i></p> <p>Enter the source port.</p> <p>First select the port number range.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The route is valid for all port numbers.</li> <li>• <i>Single</i>: Enables the entry of a port number.</li> </ul>


Field	Description
	<ul style="list-style-type: none"> <li>• <i>Range</i>: Enables the entry of a range of port numbers.</li> <li>• <i>Privileged</i>: Entry of privileged port numbers: 0 ... 1023.</li> <li>• <i>Server</i>: Entry of server port numbers: 5000 ... 32767.</li> <li>• <i>Clients 1</i>: Entry of client port numbers: 1024 ... 4999.</li> <li>• <i>Clients 2</i>: Entry of client port numbers: 32768 ... 65535.</li> <li>• <i>Not privileged</i>: Entry of unprivileged port numbers: 1024 ... 65535.</li> </ul> <p>Enter the appropriate values for the individual port or start port of a range in <b>Port</b> and, for a range, the end port in <b>to Port</b>.</p>
<b>Destination Port</b>	<p>Only for <b>Layer 4 Protocol</b> = <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"> <li>• <i>Any</i> (default value): The route is valid for all port numbers.</li> <li>• <i>Single</i>: Enables the entry of a port number.</li> <li>• <i>Range</i>: Enables the entry of a range of port numbers.</li> <li>• <i>Privileged</i>: Entry of privileged port numbers: 0 ... 1023.</li> <li>• <i>Server</i>: Entry of server port numbers: 5000 ... 32767.</li> <li>• <i>Clients 1</i>: Entry of client port numbers: 1024 ... 4999.</li> <li>• <i>Clients 2</i>: Entry of client port numbers: 32768 ... 65535.</li> <li>• <i>Not privileged</i>: Entry of unprivileged port numbers: 1024 ... 65535.</li> </ul> <p>Enter the appropriate values for the individual port or start port of a range in <b>Port</b> and, for a range, the end port in <b>to Port</b>.</p>
<b>DSCP / TOS Value</b>	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Ignore</i> (default value): The type of service is ignored.</li> <li>• <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).</li> <li>• <i>DSCP Decimal Value</i>: Differentiated Services Code Point</li> </ul>


Field	Description
	<p>according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format).</p> <ul style="list-style-type: none"> <li>• <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).</li> <li>• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.</li> <li>• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.</li> <li>• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.</li> </ul> <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>
<b>Mode</b>	<p>Select when the interface defined in <b>Route Parameters -&gt; Interface</b> is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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".</li> <li>• <i>Authoritative</i>: The route can always be used.</li> <li>• <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".</li> <li>• <i>Never dialup</i>: The route can be used when the interface is "up".</li> <li>• <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".</li> </ul>

## 10.1.2 IPv6 Route Configuration

A list of all configured IPv6 routes is displayed in the **Network->Routes->IPv6 Route Configuration** menu.

### 10.1.2.1 Edit or New

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

Routes without an  icon have been created by the router automatically and cannot be edited.

IPv4 Route Configuration
IPv6 Route Configuration
IPv4 Routing Table
IPv6 Routing Table
Options

Route Parameters	
Description	<input style="width: 90%;" type="text"/>
Route Active	<input checked="" type="checkbox"/> Enabled
Route Type	Network Route via Gateway ▾
Destination Interface	Select one ▾
Source Address / Length	<input style="width: 80%;" type="text"/> /64
Destination Address / Length	<input style="width: 80%;" type="text"/> /64
Gateway Address	<input style="width: 80%;" type="text"/>
Metric	1 ▾

Fig. 94: Network->Routes->IPv6 Route Configuration->New

The **Network->Routes->IPv6 Route Configuration->New** menu consists of the following fields:

#### Fields in the Route Parameters menu

Field	Description
<b>Description</b>	Enter a description for the IPv6 route.
<b>Route Active</b>	<p>Select if the route is to be active or inactive..</p> <p>With <i>Enabled</i> the status of the route will be set to active.</p> <p>The function is enabled by default.</p>
<b>Route Type</b>	<p>Select the type of route.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Default Route via Interface</i> : Route via a specific interface which is used if no other adequate route is available.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Default Route via Gateway</i>: Route via a specific gateway which is used if no other adequate route is available.</li> <li>• <i>Host Route via Interface</i>: Route to a single host via a specific interface.</li> <li>• <i>Host Route via Gateway</i>: Route to a single host via a specific gateway.</li> <li>• <i>Network Route via Interface</i>: Route to a network via a specific interface.</li> <li>• <i>Network Route via Gateway</i> (default value): Route to a network via a specific gateway.</li> </ul>
<b>Destination Interface</b>	<p>Select the IPv6 interface to be used for this route.</p> <p>You can choose from those interfaces available under <b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt;New</b> that are IPv6-enabled.</p>
<b>Source Address / Length</b>	<p>Enter the source IPv6 address along with the corresponding prefix length.</p> <p>: : describes an unspecific address.</p> <p>By default the prefix length <i>64</i> is predefined.</p>
<b>Destination Address / Length</b>	<p>Enter the destination IPv6 address along with the corresponding prefix length.</p> <p>: : describes an unspecific address.</p> <p>By default the prefix length <i>64</i> is predefined.</p>
<b>Gateway Address</b>	<p>Enter a the IPv6 address for the next hop.</p>
<b>Metric</b>	<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>



## 10.1.3 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.

In the ex works state, a predefined entry with the parameters **Destination IP Address** = *192.168.0.0*, **Netmask** = *255.255.255.0*, **Gateway** = *192.168.0.250*, **Interface** = *LAN\_EN1-0*, **Route Type** = *Network Route via Interface*, **Protocol** = *Local* is displayed.



IPv4 Route Configuration		IPv6 Route Configuration		IPv4 Routing Table		IPv6 Routing Table		Options	
View 20 per page << >> Filter in: None equal Go									
Destination IP Address	Netmask	Gateway	Interface	Metric	Route Type	Extended Route	Protocol		
10.0.0.0	255.255.255.0	10.0.0.185	LAN_EN1-0	0	Network Route via Interface	<input type="checkbox"/>	Local		
Page: 1, Items: 1 - 1									

Fig. 95: Network->Routes->IPv4 Routing Table

### Fields in the menu IPv4 Routing Table

Field	Description
<b>Destination IP Address</b>	Displays the IP address of the destination host or destination network.
<b>Netmask</b>	Displays the netmask of the destination host or destination network.
<b>Gateway</b>	Displays the gateway IP address. Nothing is displayed here when routes are received by DHCP.
<b>Interface</b>	Displays the interface used for this route.
<b>Metric</b>	Displays the route's priority.  The lower the value, the higher the priority of the route.
<b>Route Type</b>	Displays the route type.
<b>Extended Route</b>	Displays whether a route has been configured with advanced parameters.

Field	Description
<b>Protocol</b>	Displays how the entry has been created , e.g. manually ( <i>Local</i> ) or via one of the available protocols.
<b>Delete</b>	You can delete entries with the  symbol.

## 10.1.4 IPv6 Routing Table

A list of all configured IPv6 routes is displayed in the **Network->Routes->IPv6 Routing Table** menu.

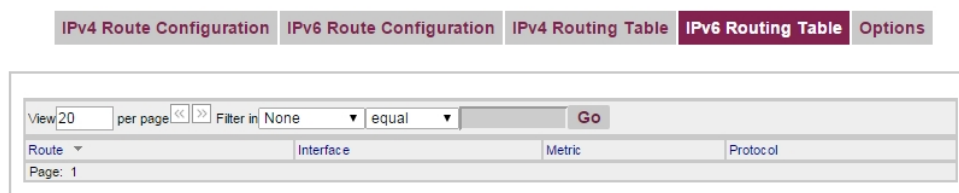


Fig. 96: **Network->Routes->IPv6 Routing Table**

### Fields in the IPv6 Routing Table menu

Field	Description
<b>Route</b>	Displays the source and destination address, which is used for this route, as well as the gateway IP address. Nothing is displayed here when routes are received by DHCP.
<b>Interface</b>	Displays the interface used for this route.
<b>Metric</b>	Displays the route's priority.  The lower the value, the higher the priority of the route.
<b>Protocol</b>	Displays how the entry has been created , e.g. manually ( <i>Local</i> ) or via one of the available protocols.

## 10.1.5 Options

### Back Route Verify

The term Back Route Verify describes a very simple but powerful function. If a check is ac-

tivated 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.

Back Route Verify

Mode

Enable for all interfaces  
 Enable for specific interfaces  
 Disable for all interfaces

View 20 per page Filter in None equal Go

No.	Interface	Back Route Verify
1	en1-0	<input checked="" type="checkbox"/> Enabled
2	en1-4	<input checked="" type="checkbox"/> Enabled

Page: 1, Items: 1 - 2

OK Cancel

Fig. 97: Networking->Routes->Options

In the ex works state, the two entries *en1-0* and *ethoa35-5* are displayed by default setting *Enable for specific interfaces*.

The **Networking->Routes->Options** menu consists of the following fields:

#### Fields in the Back Route Verify menu.

Field	Description
<b>Mode</b>	<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"> <li>• <i>Enable for all interfaces</i>: Back Route Verify is activated for all interfaces.</li> <li>• <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.</li> <li>• <i>Disable for all interfaces</i>: Back route verify is disabled for all interfaces.</li> </ul>
<b>No.</b>	<p>Only for <b>Mode</b> = <i>Enable for specific interfaces</i></p> <p>Displays the serial number of the list entry.</p>
<b>Interface</b>	<p>Only for <b>Mode</b> = <i>Enable for specific interfaces</i></p>

Field	Description
	Displays the name of the interface.
<b>Back Route Verify</b>	<p>Only for <b>Mode</b> = <i>Enable for specific interfaces</i></p> <p>Select whether <i>Back Route Verify</i> is to be activated for the interface.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>By default, the function is deactivated for all interfaces.</p>

## 10.2 IPv6 General Prefixes

**IPv6 General Prefixes** are usually distributed by IPv6 providers. They can be statically assigned or obtained through DHCP. In most cases, they define /48 or /56 networks. You can derive /64 subnets from these prefixes and have them distributed in your network.

General Prefixes have two key advantages:


- A single route is sufficient for all traffic between the provider and the customer.
- If your provider assigns a new General Prefix through DHCP or changes the static General Prefix assigned to you, there is little or no configuration to be done: In the case of DHCP you obtain the new General Prefix automatically; and in the case of a statically assigned General Prefix, you need to introduce it into your system once. All subnets and IPv6 addresses derived from the General Prefix change automatically after an update.

In order to IPv6 you need to configure how subnets and IPV6 addresses are created and distributed (see Configuring IPv6 addresses in [Interfaces](#) on page 134 and the menu **LAN->IP Configuration->Interfaces** for the IPv6-relevant parameters.

### 10.2.1 General Prefix Configuration

A list of all configured IPv6 prefixes is displayed in the **Networking->IPv6 General Prefixes->General Prefix Configuration** menu.

#### 10.2.1.1 Edit or New

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

**General Prefix Configuration**

Basic Parameters	
General Prefix active	<input checked="" type="checkbox"/> Enabled
Name	<input style="width: 100%;" type="text"/>
Type	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static
From Interface	Select one ▼

Fig. 98: Networking->IPv6 General Prefixes->General Prefix Configuration ->New

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>General Prefix active</b>	<p>Select if the prefix is to be active or inactive..</p> <p>With <i>Enabled</i> the status of the prefix will be set to active.</p> <p>The function is enabled by default.</p>
<b>Name</b>	<p>Enter a name for the General Prefix.</p> <p>A meaningful name helps selecting the General Prefix from a prefix list.</p>
<b>Type</b>	<p>Specify how the address range is to be assigned.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Dynamic</i> (default value): The general prefix will be set dynamically by DHCP transmission, e.g. from a provider.</li> <li>• <i>Static</i>: The prefix is fixed, e. g. by a provider.</li> </ul>
<b>From Interface</b>	<p>Only with <b>Type</b> = <i>Dynamic</i></p> <p>Select the IPv6 interface from which a General Prefix is to be obtained.</p> <p>You can choose from all interfaces that are available under <b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt;New</b> and that fulfill the following conditions:</p> <ul style="list-style-type: none"> <li>• <b>IPv6</b> is <i>Enabled</i>.</li> <li>• <b>IPv6 Mode</b> = <i>Host</i></li> <li>• <b>DHCP Client</b> is <i>Enabled</i>.</li> </ul>

Field	Description
<b>Used Prefix / Length</b>	<p>Only with <b>Type = Static</b></p> <p>Enter the prefix to be used. Enter the corresponding length. This prefix must end with ::.</p> <p>The default value is <i>48</i> .</p>

## 10.3 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 239).

### 10.3.1 NAT Interfaces

A list of all NAT interfaces is displayed in the **Networking->NAT->NAT Interfaces** menu.

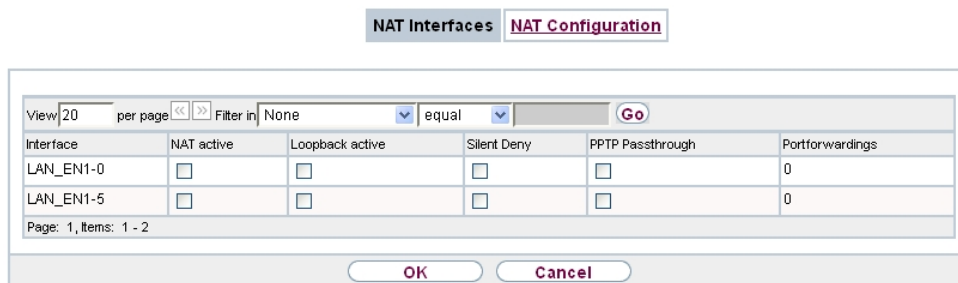


Fig. 99: **Networking->NAT->NAT Interfaces**

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
<b>NAT active</b>	<p>Select whether NAT is to be activated for the interface.</p> <p>The function is disabled by default.</p>

Field	Description
<b>Loopback active</b>	<p>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.</p> <p>The function is disabled by default.</p>
<b>Silent Deny</b>	<p>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.</p> <p>The function is disabled by default.</p>
<b>PPTP Passthrough</b>	<p>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.</p> <p>The function is disabled by default.</p> <p>If <b>PPTP Passthrough</b> is enabled, the device itself cannot be configured as a tunnel endpoint.</p>
<b>Portforwardings</b>	<p>Shows the number of portforwarding rules configured in <b>Networking-&gt;NAT-&gt;NAT Configuration</b>.</p>

## 10.3.2 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.

### 10.3.2.1 New

Choose the **New** button to set up NAT.

NAT Interfaces
NAT Configuration

Basic Parameters	
Description	<input type="text"/>
Interface	Any <input type="button" value="v"/>
Type of traffic	incoming (Destination NAT) <input type="button" value="v"/>
Specify original traffic	
Service	User-defined <input type="button" value="v"/>
Protocol	Any <input type="button" value="v"/>
Source IP Address/Netmask	Any <input type="button" value="v"/>
Original Destination IP Address/Netmask	Any <input type="button" value="v"/>
Replacement Values	
New Destination IP Address/Netmask	Host <input type="button" value="v"/> <input type="text" value="0.0.0.0"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 100: 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
<b>Description</b>	Enter a description for the NAT configuration.
<b>Interface</b>	Select the interface for which NAT is to be configured.  Possible values: <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): NAT is configured for all interfaces.</li> <li>• <i>&lt;Interface name&gt;</i>: Select one of the interfaces from the list.</li> </ul>
<b>Type of traffic</b>	Select the type of data traffic for which NAT is to be configured.  Possible values: <ul style="list-style-type: none"> <li>• <i>incoming (Destination NAT)</i> (default value): The data traffic that comes from outside.</li> <li>• <i>outgoing (Source NAT)</i>: Outgoing data traffic.</li> <li>• <i>excluding (Without NAT)</i>: Data traffic excluded from NAT.</li> </ul>
<b>NAT method</b>	Only for <b>Type of traffic</b> = <i>outgoing (Source NAT)</i>



Field	Description
	<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"> <li>• <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.</li> <li>• <i>restricted-cone</i> (UDP only): Like full-cone NAT; as external host, however, only the initial "external" destination host is allowed.</li> <li>• <i>port-restricted-cone</i> (UDP only): Like restricted-cone NAT; however, exclusively data from the initial destination port are allowed.</li> <li>• <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.</li> </ul>

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
<b>Service</b>	<p>Not for <b>Type of traffic</b> = <i>outgoing (Source NAT)</i> and <b>NAT method</b> = <i>full-cone, restricted-cone</i> or <i>port-restricted-cone</i>.</p> <p>Select one of the preconfigured services.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>User-defined</i> (default value)</li> <li>• <i>&lt;service name&gt;</i></li> </ul>
<b>Action</b>	<p>Only for <b>Type of traffic</b> = <i>excluding (Without NAT)</i></p>

Field	Description
	<p>Select which data packets are to be excluded by NAT.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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/network mask, etc.) are excluded by NAT.</li> <li>• <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/network mask, etc.) are excluded by NAT.</li> </ul>
<b>Protocol</b>	<p>Only for certain services.</p> <p>Not for <b>Type of traffic</b> = <i>outgoing (Source NAT)</i> and <b>NAT method</b> = <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 <b>Service</b>, different protocols are available.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value)</li> <li>• <i>AH</i></li> <li>• <i>Chaos</i></li> <li>• <i>EGP</i></li> <li>• <i>ESP</i></li> <li>• <i>GGP</i></li> <li>• <i>GRE</i></li> <li>• <i>HMP</i></li> <li>• <i>ICMP</i></li> <li>• <i>IGMP</i></li> <li>• <i>IGP</i></li> <li>• <i>IGRP</i></li> <li>• <i>IP</i></li> <li>• <i>IPinIP</i></li> <li>• <i>IPv6</i></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>IPX in IP</i></li> <li>• <i>ISO-IP</i></li> <li>• <i>Kryptolan</i></li> <li>• <i>L2TP</i></li> <li>• <i>OSPF</i></li> <li>• <i>PUP</i></li> <li>• <i>RDP</i></li> <li>• <i>RSVP</i></li> <li>• <i>SKIP</i></li> <li>• <i>TCP</i></li> <li>• <i>TLSP</i></li> <li>• <i>UDP</i></li> <li>• <i>VRRP</i></li> <li>• <i>XNS-IDP</i></li> </ul>
<b>Source IP Address/ Netmask</b>	<p>Only for <b>Type of traffic</b> = <i>incoming</i> (<i>Destination NAT</i>) or <i>excluding</i> (<i>Without NAT</i>)</p> <p>Enter the source IP address and corresponding netmask of the original data packets, as the case arises.</p>
<b>Original Destination IP Address/Netmask</b>	<p>Only for <b>Type of traffic</b> = <i>incoming</i> (<i>Destination NAT</i>)</p> <p>Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.</p>
<b>Original Destination Port/Range</b>	<p>Only for <b>Type of traffic</b> = <i>incoming</i> (<i>Destination NAT</i>), <b>Service</b> = <i>user-defined</i> and <b>Protocol</b> = <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>
<b>Original Source IP Ad- dress/Netmask</b>	<p>Only for <b>Type of traffic</b> = <i>outgoing</i> (<i>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
<b>Original Source Port/Range</b>	<p>Only for <b>Type of traffic</b> = <i>outgoing (Source NAT)</i>, <b>NAT method</b> = <i>symmetric</i>, <b>Service</b> = <i>user-defined</i> and <b>Protocol</b> = <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>
<b>Source Port/Range</b>	<p>Only for <b>Type of traffic</b> = <i>excluding (Without NAT)</i>, <b>Service</b> = <i>user-defined</i> and <b>Protocol</b> = <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>
<b>Destination IP Address/Netmask</b>	<p>Only for <b>Type of traffic</b> = <i>excluding (Without NAT)</i> or <i>outgoing (Source NAT)</i> and <b>NAT method</b> = <i>symmetric</i></p> <p>Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.</p>
<b>Destination Port/Range</b>	<p>Only for <b>Type of traffic</b> = <i>outgoing (Source NAT)</i>, <b>NAT method</b> = <i>symmetric</i>, <b>Service</b> = <i>user-defined</i> and <b>Protocol</b> = <i>TCP, UDP, TCP/UDP</i> or <b>Type of traffic</b> = <i>excluding (Without NAT)</i>, <b>Service</b> = <i>user-defined</i> and <b>Protocol</b> = <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
<b>New Destination IP Ad-</b>	Only for <b>Type of traffic</b> = <i>incoming (Destination NAT)</i>

Field	Description
<b>dress/Netmask</b>	Enter the destination IP address and corresponding netmask to which the original destination IP address is to be translated.
<b>New Destination Port</b>	<p>Only for <b>Type of traffic</b> = <i>incoming</i> (<i>Destination NAT</i>), <b>Service</b> = <i>user-defined</i> and <b>Protocol</b> = <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>
<b>New Source IP Address/Netmask</b>	<p>Only for <b>Type of traffic</b> = <i>outgoing</i> (<i>Source NAT</i>) and <b>NAT method</b> = <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>
<b>New Source Port</b>	<p>Only for <b>Type of traffic</b> = <i>outgoing</i> (<i>Source NAT</i>), <b>NAT method</b> = <i>symmetric</i>, <b>Service</b> = <i>user-defined</i>, <b>Protocol</b> = <i>TCP, UDP, TCP/UDP</i> and <b>Original Source Port/Range</b> = <i>-All- or Specify port</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 <b>Original Source Port/Range</b>, you can choose from the following options:</p> <ul style="list-style-type: none"> <li>• <i>Use Original Source Port/Range</i>: The range specified for <b>Original Source Port/Range</b> is not changed, all port numbers are retained.</li> <li>• <i>Use Source Port/Range starting with</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</li> </ul>

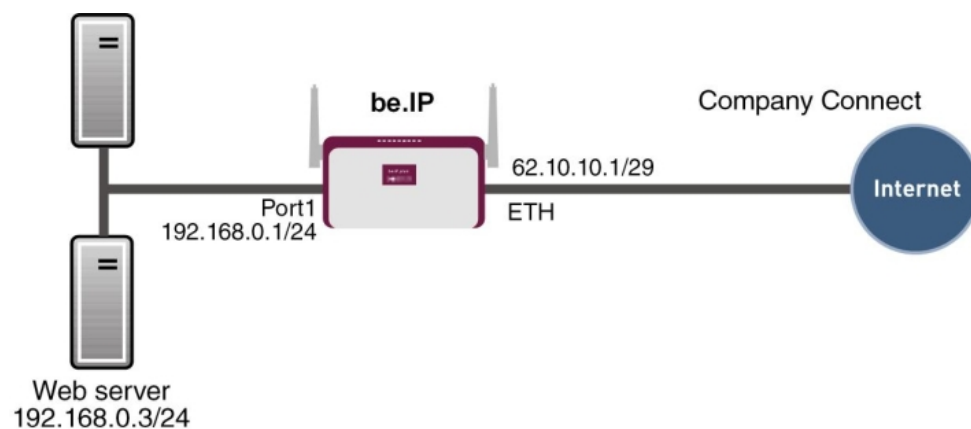
Field	Description
	count of ports is retained.

### 10.3.3 NAT - Configuration example

#### Requirements

- Basic configuration of the gateway
- A working Internet access. For example, **Company Connect** with 8 IP addresses.
- The Ethernet interface **ETH** is connected to the access router to the internet (IP address *62.10.10.1/29*)
- The IP address *62.10.10.2* to *62.10.10.6* are entered on Ethernet interface **ETH**.

#### Example scenario



#### Configuration target

- You configure NAT enables for accessing your gateway over HTTP.
- You also want to access your terminal server and the corporate web server over the Internet.

#### Overview of Configuration Steps

##### Enable NAT

Field	Menu	Value
NAT active	Network->NAT->NAT Interfaces	Enabled for <i>LAN_EN5-0</i>

Field	Menu	Value
Silent Deny	Network->NAT->NAT Interfaces	Enabled for LAN_EN5-0

#### Configured NAT enables

Field	Menu	Value
Description	Network->NAT->NAT Configuration->New	e.g. GUI
Interface	Network->NAT->NAT Configuration->New	LAN_EN5-0
Type of traffic	Network->NAT->NAT Configuration->New	incoming (Destination NAT)
Service	Network->NAT->NAT Configuration->New	User-defined
Protocol	Network->NAT->NAT Configuration->New	TCP
Original Destination IP Address/Netmask	Network->NAT->NAT Configuration->New	Host, e.g. 62.10.10.2
Original Destination Port/Range	Network->NAT->NAT Configuration->New	80
New Destination IP Address/Netmask	Network->NAT->NAT Configuration->New	127.0.0.1
New Destination Port	Network->NAT->NAT Configuration->New	Original disabled, 80

#### Web server

Field	Menu	Value
Description	Network->NAT->NAT Configuration->New	e.g. Webserver
Interface	Network->NAT->NAT Configuration->New	LAN_EN5-0
Type of traffic	Network->NAT->NAT Configuration->New	incoming (Destination NAT)
Service	Network->NAT->NAT Configuration->New	http
Protocol	Network->NAT->NAT Configuration->New	Host, e.g. 62.10.10.3
Original Destination IP Address/Netmask	Network->NAT->NAT Configuration->New	Host, e.g.

Field	Menu	Value
		192.168.0.3
<b>New Destination Port</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>Original</i>

### Terminal Server

Field	Menu	Value
<b>Description</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	e.g. <i>Terminal-Server</i>
<b>Interface</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>LAN_EN5-0</i>
<b>Type of traffic</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>incoming</i> <i>(Destination NAT)</i>
<b>Service</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>User-defined</i>
<b>Protocol</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>TCP</i>
<b>Original Destination IP Address/Netmask</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>96</i>
<b>Original Destination Port/Range</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>3389</i>
<b>New Destination IP Address/Netmask</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>Host, e.g.</i> <i>192.168.0.2</i>
<b>New Destination Port</b>	<b>Network-&gt;NAT-&gt;NAT Configuration-&gt;New</b>	<i>Original</i>

## 10.4 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.

### 10.4.1 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.

## 10.4.1.1 New

Choose the **New** button to create additional groups.

Fig. 101: **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
<b>Group Description</b>	Enter the desired description of the interface group.
<b>Distribution Policy</b>	Select the way the data traffic is to be distributed to the interfaces configured for the group.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Consider</b>	<p>Only for <b>Distribution Policy</b> = <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"> <li>• <i>Download</i>: Only the data rate in the receive direction is considered.</li> <li>• <i>Upload</i>: Only the data rate in the send direction is considered.</li> </ul> <p>By default, the <i>Download</i> and <i>Upload</i> options are disabled.</p>
<b>Distribution Mode</b>	<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"> <li>• <i>Always</i> (default value): Also includes idle interfaces.</li> <li>• <i>Only use active interfaces</i>: Only interfaces in the up state are included.</li> </ul>

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.

Load Balancing Groups Special Session Handling

Basic Parameters

Group Description

Distribution Policy Session-Round-Robin

Distribution

Interface Se

Interface

Ad

Basic Parameters

Group Description

Distribution Policy Session-Round-Robin

Interface Selection for Distribution

Interface None

Distribution Ratio 0 %

Advanced Settings

Route Selector None

Tracking IP Address None

Apply
Cancel

Fig. 102: Networking->Load Balancing->Load Balancing Groups->Add

#### Fields in the Basic Parameters menu.

Field	Description
Group Description	Shows the description of the interface group.
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 <b>Distribution Ratio</b> employed:</p> <ul style="list-style-type: none"> <li>For <i>Session-Round-Robin</i> is based on the number of distributed sessions.</li> <li>For <i>Load-dependent Bandwidth</i>, the data rate is the de-</li> </ul>

Field	Description
	cisive factor.

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Route Selector</b>	<p>The <b>Route Selector</b> 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"> <li>• If an interface is only assigned to one load balancing group, it is not necessary to configure the route selector.</li> <li>• If an interface is assigned to multiple load balancing groups, configuration of the route selector is essential.</li> <li>• The route selector must be configured identically for all interface entries within a load balancing group.</li> </ul> <p>Select the <b>Destination IP Address</b> of the desired route.</p> <p>You can choose between all routes and all extended routes.</p>
<b>Tracking IP Address</b>	<p>You can use the <b>Tracking IP Address</b> 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 <b>Local Services-&gt;Surveillance-&gt;Hosts</b> menu. Here, it is important that only the host surveillance entries with the action <b>Monitor</b> 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 <b>Tracking IP Address</b> in the <b>Load Balancing-&gt;Load Balancing Groups-&gt;Advanced Settings</b> menu. The interface's load bal-</p>

Field	Description
	<p>ancing 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 <b>Local Services-&gt;Surveillance-&gt;Hosts-&gt;New</b> menu under <b>Monitored IP Address</b> and which are monitored with the aid of the <b>Action to be executed</b> field (<b>Action</b> = <i>Monitor</i>).</p>

## 10.4.2 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.

### 10.4.2.1 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	<input type="text"/>
Service	User-defined <span style="float: right;">▼</span>
Protocol	Any <span style="float: right;">▼</span>
Destination IP Address/Netmask	Any <span style="float: right;">▼</span>
Source Interface	Any <span style="float: right;">▼</span>
Source IP Address/Netmask	Any <span style="float: right;">▼</span>
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. 103: 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
<b>Admin Status</b>	<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>
<b>Description</b>	<p>Enter a name for the entry.</p>
<b>Service</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>charge</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>The default value is <i>User defined</i>.</p>
<b>Protocol</b>	Select a protocol, if required. The <i>Any</i> option (default value) matches any protocol.
<b>Destination IP Address/Netmask</b>	<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"> <li>• <i>Any</i> (default value)</li> <li>• <i>Host</i>: Enter the IP address of the host.</li> <li>• <i>Network</i>: Enter the network address and the related netmask.</li> </ul>
<b>Destination Port/Range</b>	<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"> <li>• <i>-All-</i> (default value): The destination port is not specified.</li> <li>• <i>Specify port</i>: Enter a destination port.</li> <li>• <i>Specify port range</i>: Enter a destination port range.</li> </ul>
<b>Source Interface</b>	If required, select your device's source interface.
<b>Source IP Address/Netmask</b>	<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"> <li>• <i>Any</i> (default value)</li> <li>• <i>Host</i>: Enter the IP address of the host.</li> <li>• <i>Network</i>: Enter the network address and the related netmask.</li> </ul>

Field	Description
<b>Source Port/Range</b>	<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"> <li>• <i>-All-</i> (default value): The destination port is not specified.</li> <li>• <i>Specify port</i>: Enter a destination port.</li> <li>• <i>Specify port range</i>: Enter a destination port range.</li> </ul>
<b>Special Handling Timer</b>	<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
<b>Frozen Parameters</b>	<p>Specify whether, when data packets are subsequently sent, the two parameters <b>Destination Address</b> and <b>Destination Port</b> must have the same value as the first data packet, i. e. whether the subsequent data packets must be routed via the same <b>Destination Port</b> to the same <b>Destination Address</b>.</p> <p>The two parameters <b>Destination Address</b> and <b>Destination Port</b> 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 <b>Source IP Address</b> 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>

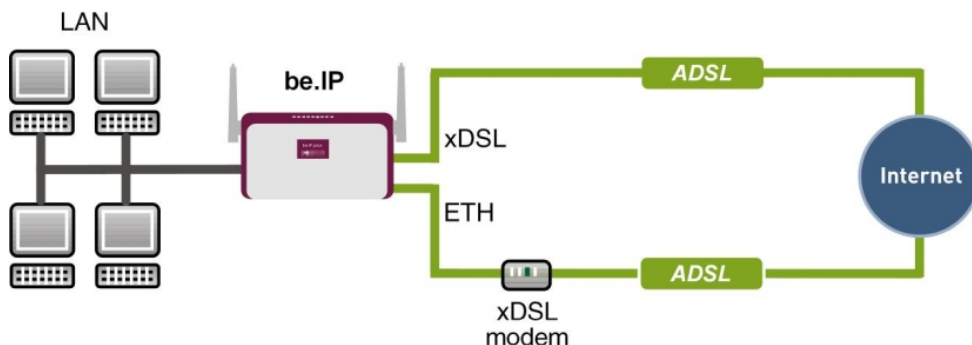
### 10.4.3 Load balancing - Configuration example

#### Requirements



- Gateway with the ADSL modem integrated
- An external ADSL modem
- Two independent ADSL Internet connections

### Example scenario



### Configuration target

- The data traffic is distributed half and half to the two ADSL lines based on IP sessions.
- We shall then take the example of encrypted HTTP connections (HTTPS) to describe how to effectively avoid any loss of connection that might occur when distributing to different Internet accesses.



#### Note

When creating the ADSL connections, besides the public IP address, the bintec R3002 also obtains the IP addresses of the DNS servers for resolving the name of the configured Internet provider. Particularly when using different Internet providers, the use of the DSN servers needs to be connection-specific.

The configuration of the DNS servers is automatically created when you create the ADSL connections and can be seen in the menu **Local SevicesDNSDNS Server**.

### Overview of Configuration Steps

#### Set up first Internet connection

Field	Menu	Value
Connection Type	Assistants->Internet Access->Internet Connections->New	Internal ADSL Modem

Field	Menu	Value
Description	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>ADSL-1</i>
Type	Assistants->Internet Access->Internet Connections->New->Next	<i>User-defined via PPP over Ethernet (PPPoE)</i>
Login Name	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>feste_ip@provider.de</i>
Password	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>test12345</i>



#### Note

The message you get when you create the second ADSL connection may be ignored. The IP load distribution avoids routing conflicts due to multiple standard routes!

#### Set up the second Internet connection

Field	Menu	Value
Connection Type	Assistants->Internet Access->Internet Connections->New	<i>External xDSL Modem</i>
Description	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>ADSL-2</i>
Physical Ethernet Port	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>ETH5</i>
Type	Assistants->Internet Access->Internet Connections->New->Next	<i>User-defined</i>
Login Name	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>#0001@t-online.de</i>
Password	Assistants->Internet Access->Internet Connections->New->Next	e.g. <i>test12345</i>

#### Create a load balancing group

Field	Menu	Value
Group Description	Network->Load Balancing->Load Balancing Groups->New	e.g. <i>Internet Access</i>
Distribution Policy	Network->Load Balancing->Load Balancing Groups->New	<i>Session-Round-Robin</i>

Field	Menu	Value
Distribution Mode	Network->Load Balancing->Load Balancing Groups->New	<i>Always</i>
Interface	Network->Load Balancing->Load Balancing Groups->New->Add	<i>WAN_ADSL-1</i>
Distribution Ratio	Network->Load Balancing->Load Balancing Groups->New->Add	<i>50</i>
Interface	Network->Load Balancing->Load Balancing Groups->New->Add	<i>WAN_ADSL-2</i>
Distribution Ratio	Network->Load Balancing->Load Balancing Groups->New->Add	<i>50</i>

### Special Session Handling

Field	Menu	Value
Description	Network->Load Balancing->Special Session Handling->New	e.g. <i>HTTPS</i>
Service	Network->Load Balancing->Special Session Handling->New	<i>http (SSL)</i>
Special Handling Timer	Network->Load Balancing->Special Session Handling->New	<i>900 seconds</i>

## 10.5 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

### 10.5.1 IPv4/IPv6 Filter

In the **Networking->IPv4/IPv6 Filter->QoS Filter** menu IP filters are configured.

The list also displays any configured entries from **Networking->Access Rules->Rule Chains**.

### 10.5.1.1 New

Choose the **New** button to define more IP filters.

Basic Parameters	
Description	<input type="text"/>
Service	any ▼
Destination IPv4 Address/Netmask	Any ▼
Destination IPv6 Address/Length	Any ▼
Source IPv4 Address/Netmask	Any ▼
Source IPv6 Address/Length	Any ▼
DSCP/Traffic Class Filter (Layer 3)	Ignore ▼
COS Filter (802.1p/Layer 2)	Ignore ▼

Fig. 104: **Networking->IPv4/IPv6 Filter->QoS Filter->New**

The **Networking->IPv4/IPv6 Filter->QoS Filter->New** menu consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>Description</b>	Enter the name of the filter.
<b>Service</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>charge</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>The default value is <i>User defined</i>.</p>

Field	Description
<b>Protocol</b>	<p>Select a protocol.</p> <p>The <i>Any</i> option (default value) matches any protocol.</p>
<b>Type</b>	<p>Only for <b>Protocol</b> = <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>
<b>Connection State</b>	<p>With <b>Protocol</b> = <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"> <li>• <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.</li> <li>• <i>Any</i> (default value): All TCP packets match the filter.</li> </ul>
<b>Destination IPv4 Address/Netmask</b>	<p>Enter the destination IPv4 address of the data packets and the corresponding netmask.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The destination IP address/netmask are not specified.</li> <li>• <i>Host</i>: Enter the destination IP address of the host.</li> <li>• <i>Network</i>: Enter the destination network address and the corresponding netmask.</li> </ul>
<b>Destination IPv6 Address/Length</b>	<p>Enter the destination IPv6 address of the data packets and the prefix length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The destination IP address/length are not specified.</li> <li>• <i>Host</i>: Enter the destination IP address of the host.</li> <li>• <i>Network</i>: Enter the destination network address and the pre-</li> </ul>

Field	Description
	fix length.
<b>Destination Port/Range</b>	<p>Only for <b>Protocol</b> = <i>TCP</i>, <i>UDP</i> or <i>TCP/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"> <li>• <i>-All-</i> (default value): The destination port is not specified.</li> <li>• <i>Specify port</i>: Enter a destination port.</li> <li>• <i>Specify port range</i>: Enter a destination port range.</li> </ul>
<b>Source IPv4 Address/Netmask</b>	<p>Enter the source IPv4 address of the data packets and the corresponding netmask.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The source IP address/netmask are not specified.</li> <li>• <i>Host</i>: Enter the source IP address of the host.</li> <li>• <i>Network</i>: Enter the source network address and the corresponding netmask.</li> </ul>
<b>Source IPv6 Address/Length</b>	<p>Enter the source IPv6 address of the data packets and the prefix length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The source IP address/length are not specified.</li> <li>• <i>Host</i>: Enter the source IP address of the host.</li> <li>• <i>Network</i>: Enter the source network address and the prefix length.</li> </ul>
<b>Source Port/Range</b>	<p>Only for <b>Protocol</b> = <i>TCP</i>, <i>UDP</i> or <i>TCP/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"> <li>• <i>-All-</i> (default value): The source port is not specified.</li> <li>• <i>Specify port</i>: Enter a source port.</li> <li>• <i>Specify port range</i>: Enter a source port range.</li> </ul>

Field	Description
<b>DSCP/TOS Filter (Layer 3)</b>	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Ignore</i> (default value): The type of service is ignored.</li> <li>• <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).</li> <li>• <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).</li> <li>• <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).</li> <li>• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.</li> <li>• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.</li> <li>• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.</li> </ul>
<b>COS Filter (802.1p/Layer 2)</b>	<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> <p>The default value is <i>Ignore</i>.</p>

## 10.5.2 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.

### 10.5.2.1 New

Choose the **New** button to create additional data classes.

IPv4/IPv6 Filter
QoS Classification
QoS Interfaces/Policies

Basic Parameters	
Class map	New ▼
Description	<input type="text"/>
Filter	Select one ▼
Direction	Outgoing ▼
High Priority Class	<input type="checkbox"/>
Class ID	1 ▼
Set DSCP/Traffic Class Filter (Layer 3)	Preserve ▼
Set COS value (802.1p/Layer 2)	Preserve ▼
Interfaces	<div style="border: 1px solid gray; padding: 2px;"> <input type="text" value="Interface"/> </div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Add"/> </div>


Fig. 105: **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
<b>Class map</b>	Choose the class plan you want to create or edit.  Possible values: <ul style="list-style-type: none"> <li><i>New</i> (default value): You can create a new class plan with this setting.</li> <li><i>&lt;Name of class plan&gt;</i>: Shows a class plan that has already been created, which you can select and edit. You can add new filters.</li> </ul>
<b>Description</b>	Only for <b>Class map</b> = <i>New</i>  Enter the name of the class plan.
<b>Filter</b>	Select an IP filter.  If the class plan is new, select the filter to be set at the first point of the class plan.  If the class plan already exists, select the filter to be attached to the class plan.



Field	Description
	To select a filter, at least one filter must be configured in the <b>Networking-&gt;QoS-&gt;QoS Filter</b> menu.
<b>Direction</b>	<p>Select the direction of the data packets to be classified.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Incoming</i>: Incoming data packets are assigned to the class (<b>Class ID</b>) that is then to be defined.</li> <li>• <i>Outgoing</i> (default value): Outgoing data packets are assigned to the class (<b>Class ID</b>) that is then to be defined.</li> <li>• <i>Both</i>: Incoming and outgoing data packets are assigned to the class (<b>Class ID</b>) that is then to be defined.</li> </ul>
<b>High Priority Class</b>	<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>
<b>Class ID</b>	<p>Only for <b>High Priority Class</b> not active.</p> <p>Choose a number which assigns the data packets to a class.</p>
	<p> <b>Note</b></p> <p>The class ID is a label to assign data packets to specific classes. (The class ID does not define the priority.)</p>
	Possible values are whole numbers between <i>1</i> and <i>254</i> .
<b>Set DSCP/Traffic Class Filter (Layer 3)</b>	<p>Here you can set or change the DSCP/TOS value of the IP data packets, based on the class (<b>Class ID</b>) that has been defined.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Preserve</i> (default value): The DSCP/TOS value of the IP data packets remains unchanged.</li> <li>• <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).</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <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).</li> <li>• <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).</li> <li>• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.</li> <li>• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.</li> <li>• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.</li> </ul>
<b>Set COS value (802.1p/Layer 2)</b>	<p>In the header of the Ethernet packets filtered by the selected filter, you can here set/change the service class (Layer 2 priority).</p> <p>Possible values are whole numbers between 0 and 7.</p> <p>The default value is <i>Preserve</i>.</p>
<b>Interfaces</b>	<p>Only for <b>Class map = New</b></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>

### 10.5.3 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.

### 10.5.3.1 New

Choose the **New** button to create additional prioritisations.

Fig. 106: **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
<b>Interface</b>	Select the interface for which QoS is to be configured.
<b>Prioritisation Algorithm</b>	<p>Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>Priority Queueing</i>: QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority.</li> <li><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 packets are always handled with priority.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Disabled</i> (default value): QoS is deactivated on the interface. The existing configuration is not deleted, but can be activated again if required.</li> </ul>
<b>Traffic shaping</b>	<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>
<b>Maximum Upload Speed</b>	<p>Only for <b>Traffic shaping</b> = enabled.</p> <p>Enter a maximum data rate for the selected interface in the send direction in kbit per second.</p> <p>Possible values are 0 to 1000000.</p> <p>The default value is 0, i.e. no limits are set, the selected interface can occupy its maximum bandwidth.</p>
<b>Protocol Header Size below Layer 3</b>	<p>Only for <b>Traffic shaping</b> = 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"> <li>• <i>User defined</i>: Value in byte.</li> </ul> <p>Possible values are 0 to 100.</p> <ul style="list-style-type: none"> <li>• <i>Undefined (Protocol Header Offset=0)</i> (default value)</li> </ul> <p>Can only be selected for Ethernet interfaces</p> <ul style="list-style-type: none"> <li>• <i>Ethernet</i></li> <li>• <i>Ethernet and VLAN</i></li> <li>• <i>PPP over Ethernet</i></li> <li>• <i>PPP over Ethernet and VLAN</i></li> </ul>

Field	Description
	<p>Can only be selected for IPSec interfaces:</p> <ul style="list-style-type: none"> <li>• <i>IPSec over Ethernet</i></li> <li>• <i>IPSec over Ethernet and VLAN</i></li> <li>• <i>IPSec via PPP over Ethernet</i></li> <li>• <i>IPSec via PPPoE and VLAN</i></li> </ul>
<p><b>Encryption Method</b></p>	<p>Only if an IPSec Peers is selected as <b>Interface</b>, <b>Traffic shaping</b> is <i>Active</i> and <b>Protocol Header Size below Layer 3</b> 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"> <li>• <i>DES, 3DES, Blowfish, Cast - (cipher block size = 64 Bit)</i></li> <li>• <i>AES128, AES192, AES256, Twofish - (cipher block size = 128 Bit)</i></li> </ul>
<p><b>Real Time Jitter Control</b></p>	<p>Only for <b>Traffic shaping</b> = 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 (&lt; 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>
<p><b>Control Mode</b></p>	<p>Only for <b>Real Time Jitter Control</b> = enabled.</p> <p>Select the mode for optimising voice transmission.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>All RTP Streams</i>: All RTP streams are optimised. The function activates the RTP stream detection mechanism for</li> </ul>

Field	Description
	<p>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.</p> <ul style="list-style-type: none"> <li>• <i>Inactive</i>: Voice data transmission is not optimised.</li> <li>• <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.</li> <li>• <i>Always</i>: Real Time Jitter Control is always active, even if no real time data is routed.</li> </ul>
<b>Queues/Policies</b>	<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 <b>Add</b>. The <b>Edit Queue/Policy</b> 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
<b>Description</b>	Enter the name of the queue/policy.
<b>Outbound Interface</b>	Shows the interface for which the QoS queues are being configured.
<b>Prioritisation queue</b>	<p>Select the queue priority type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Class Based</i> (default value): Queue for data classified as “normal”.</li> <li>• <i>High Priority</i>: Queue for data classified as “high priority”.</li> <li>• <i>Default</i>: Queue for data that has not been classified or data of a class for which no queue has been configured.</li> </ul>

Field	Description
<b>Class ID</b>	<p>Only for <b>Prioritisation queue</b> = <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 <b>Networking-&gt;QoS-&gt;QoS Classification</b> menu.</p>
<b>Priority</b>	<p>Only for <b>Prioritisation queue</b> = <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>
<b>Weight</b>	<p>Only for <b>Prioritisation Algorithm</b> = <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>
<b>RTT Mode (Realtime Traffic Mode)</b>	<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>
<b>Traffic Shaping</b>	<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> <p>The function is disabled by default.</p>
<b>Maximum Upload</b>	<p>Only for <b>Traffic Shaping</b> = enabled.</p>

Field	Description
<b>Speed</b>	<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>
<b>Overbooking allowed</b>	<p>Only for <b>Traffic Shaping</b> = enabled.</p> <p>Enable or disable the function. The function controls the bandwidth limit.</p> <p>If <b>Overbooking allowed</b> is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface.</p> <p>If <b>Overbooking allowed</b> 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>
<b>Burst size</b>	<p>Only for <b>Traffic Shaping</b> = 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
<b>Dropping Algorithm</b>	<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> <ul style="list-style-type: none"> <li>• <i>Tail Drop</i> (default value): The newest packet received is dropped.</li> <li>• <i>Head Drop</i>: The oldest packet in the queue is dropped.</li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• <i>Random Drop</i>: A randomly selected packet is dropped from the queue.</li> </ul>
<b>Congestion Avoidance (RED)</b>	<p>Enable or disable preventative deletion of data packets.</p> <p>Packets which have a data size of between <b>Min. queue size</b> and <b>Max. queue size</b> 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>
<b>Min. queue size</b>	<p>Enter the lower threshold value for the process <b>Congestion Avoidance (RED)</b> in bytes.</p> <p>Possible values are <i>0</i> to <i>262143</i>.</p> <p>The default value is <i>0</i>.</p>
<b>Max. queue size</b>	<p>Enter the upper threshold value for the process <b>Congestion Avoidance (RED)</b> in bytes.</p> <p>Possible values are <i>0</i> to <i>262143</i>.</p> <p>The default value is <i>16384</i>.</p>

## 10.6 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 (not available for all devices) interface or ISDN Login.

## 10.6.1 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.

The screenshot shows the 'Access Filter' configuration menu. At the top, there are three tabs: 'Access Filter' (selected), 'Rule Chains', and 'Interface Assignment'. Below the tabs is a search and filter bar with 'View: 20 per page', navigation arrows, 'Filter in: None', a dropdown menu set to 'equal', and a 'Go' button. Below this is a table with columns: Index, Description, Source, Destination, and TOS Decimal Value. The table is currently empty. At the bottom of the menu is a 'New' button.

Fig. 107: **Networking->Access Rules->Access Filter**

### 10.6.1.1 Edit or New

Choose the  icon to edit existing entries. To configure access filters, select the **New** button.

The screenshot shows the 'New' configuration dialog for an Access Filter. At the top, there are three tabs: 'Access Filter' (selected), 'Rule Chains', and 'Interface Assignment'. Below the tabs is a 'Basic Parameters' section with the following fields:

Description	<input type="text"/>
Service	any ▼
Destination IPv4 Address/Netmask	Any ▼
Destination IPv6 Address/Length	Any ▼
Source IPv4 Address/Netmask	Any ▼
Source IPv6 Address/Length	Any ▼
DSCP/Traffic Class Filter (Layer 3)	Ignore ▼
COS Filter (802.1p/Layer 2)	Ignore ▼

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Fig. 108: **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
<b>Description</b>	Enter a description for the filter.
<b>Service</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>charge</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>The default value is <i>User defined</i>.</p>
<b>Protocol</b>	<p>Select a protocol.</p> <p>The <i>Any</i> option (default value) matches any protocol.</p>
<b>Type</b>	<p>Only if <b>Protocol</b> = <i>ICMP</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i></li> <li>• <i>Echo reply</i></li> <li>• <i>Destination unreachable</i></li> <li>• <i>Source quench</i></li> <li>• <i>Redirect</i></li> <li>• <i>Echo</i></li> <li>• <i>Time exceeded</i></li> <li>• <i>Timestamp</i></li> <li>• <i>Timestamp reply</i></li> </ul> <p>The default value is <i>Any</i>.</p>

Field	Description
	See RFC 792.
<b>Connection State</b>	<p>Only if <b>Protocol</b> = <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"> <li>• <i>Any</i> (default value): All TCP packets match the filter.</li> <li>• <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.</li> </ul>
<b>Destination IPv4 Address/Netmask</b>	<p>Enter the destination IPv4 address of the data packets and the corresponding netmask.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The destination IP address/netmask are not specified.</li> <li>• <i>Host</i>: Enter the destination IP address of the host.</li> <li>• <i>Network</i>: Enter the destination network address and the corresponding netmask.</li> </ul>
<b>Destination IPv6 Address/Length</b>	<p>Enter the destination IPv6 address of the data packets and the prefix length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The destination IP address/length are not specified.</li> <li>• <i>Host</i>: Enter the destination IP address of the host.</li> <li>• <i>Network</i>: Enter the destination network address and the prefix length.</li> </ul>
<b>Destination Port/Range</b>	<p>Only if <b>Protocol</b> = <i>TCP, UDP</i></p> <p>Enter a destination port number or a range of destination port numbers that matches the filter.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>-All-</i> (default value): The filter is valid for all port numbers</li> <li>• <i>Specify port</i>: Enables the entry of a port number.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Specify port range</i>: Enables the entry of a range of port numbers.</li> </ul>
<b>Source IPv4 Address/Netmask</b>	<p>Enter the source IPv4 address of the data packets and the corresponding netmask.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The source IP address/netmask are not specified.</li> <li>• <i>Host</i>: Enter the source IP address of the host.</li> <li>• <i>Network</i>: Enter the source network address and the corresponding netmask.</li> </ul>
<b>Source IPv6 Address/Length</b>	<p>Enter the source IPv6 address of the data packets and the prefix length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The source IP address/length are not specified.</li> <li>• <i>Host</i>: Enter the source IP address of the host.</li> <li>• <i>Network</i>: Enter the source network address and the prefix length.</li> </ul>
<b>Source Port/Range</b>	<p>Only if <b>Protocol</b> = <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"> <li>• <i>-All-</i> (default value): The filter is valid for all port numbers</li> <li>• <i>Specify port</i>: Enables the entry of a port number.</li> <li>• <i>Specify port range</i>: Enables the entry of a range of port numbers.</li> </ul>
<b>DSCP/TOS Filter (Layer 3)</b>	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Ignore</i> (default value): The type of service is ignored.</li> <li>• <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).</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <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).</li> <li>• <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).</li> <li>• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.</li> <li>• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.</li> <li>• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.</li> </ul>
<b>COS Filter (802.1p/Layer 2)</b>	<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>

## 10.6.2 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.

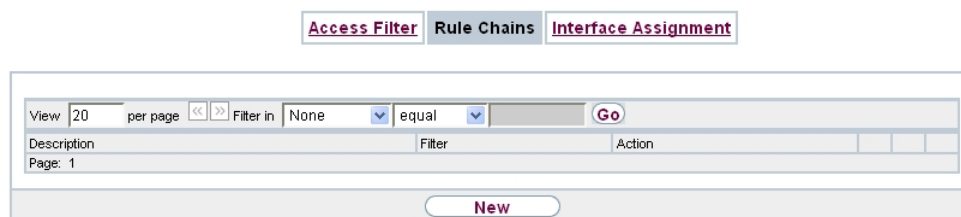



Fig. 109: **Networking->Access Rules->Rule Chains**

### 10.6.2.1 Edit or New

Choose the  icon to edit existing entries. To configure access lists, select the **New** button.

[Access Filter](#) | [Rule Chains](#) | [Interface Assignment](#)

Basic Parameters	
Rule Chain	New ▾
Description	<input type="text"/>
Access Filter	Select one ▾
Action	Allow if filter matches ▾

Fig. 110: 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
<b>Rule Chain</b>	<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"> <li><i>New</i> (default value): You can create a new rule chain with this setting.</li> <li><i>&lt;Name of the rule chain&gt;</i>: Select an already existing rule chain, and thus add another rule to it.</li> </ul>
<b>Description</b>	Enter the name of the rule chain.
<b>Access Filter</b>	<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>
<b>Action</b>	<p>Define the action to be taken for a filtered data packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>Allow if filter matches</i> (default value): Allow packet if it matches the filter.</li> <li><i>Allow if filter does not match</i>: Allow packet if it</li> </ul>



Field	Description
	<p>does not match the filter.</p> <ul style="list-style-type: none"> <li>• <i>Deny if filter matches</i>: Deny packet if it matches the filter.</li> <li>• <i>Deny if filter does not match</i>: Deny packet if it does not match the filter.</li> <li>• <i>Ignore</i>: Use next rule.</li> </ul>

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.

### 10.6.3 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.

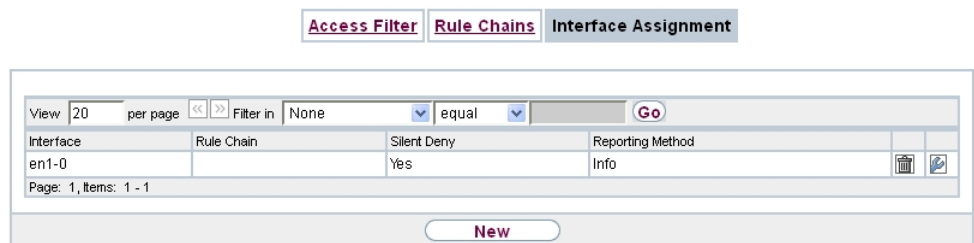



Fig. 111: Networking->Access Rules->Interface Assignment

#### 10.6.3.1 Edit or New

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

Access Filter
Rule Chains
Interface Assignment

Basic Parameters	
Interface	Select one ▼
Rule Chain	Select one ▼
Silent Deny	<input checked="" type="checkbox"/> Enabled
Reporting Method	Info ▼

OK
Cancel

Fig. 112: **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
<b>Interface</b>	Select the interface for which a configured rule chain is to be assigned.
<b>Rule Chain</b>	Select a rule chain.
<b>Silent Deny</b>	Define whether the sender is to be informed if an IP packet is denied. <ul style="list-style-type: none"> <li>• <i>Enabled</i> (default value): The sender is not informed.</li> <li>• <i>Disabled</i>: The sender receives an ICMP message.</li> </ul>
<b>Reporting Method</b>	Define whether a syslog message is to be generated if a packet is denied. <p style="margin-top: 5px;">Possible values:</p> <ul style="list-style-type: none"> <li>• <i>No report</i>: No syslog message.</li> <li>• <i>Info</i> (default value): A syslog message is generated with the protocol number, source IP address and source port number.</li> <li>• <i>Dump</i>: A syslog message is generated with the contents of the first 64 bytes of the denied packet.</li> </ul>

## 10.7 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.

### 10.7.1 Drop In Groups

The **Networking->Drop In->Drop In Groups** menu displays a list of all the configured **Drop In Groups**. Each **Drop In** group represents a network.

#### 10.7.1.1 New

Select the **New** button to set up other **Drop In Groups**.

**Drop In Groups**

Basic Parameters	
Group Description	<input type="text"/>
Mode	Transparent <input type="button" value="v"/>
Exclude from NAT (DMZ)	<input type="checkbox"/> Enabled
Network Configuration	Static <input type="button" value="v"/>
Network Address	<input type="text"/>
Netmask	<input type="text"/>
Local IP Address	<input type="text"/>
ARP Lifetime	3600 Seconds
DNS assignment via DHCP	Unchanged <input type="button" value="v"/>
Interface Selection	<div style="border: 1px solid gray; padding: 2px;">           Interface <input type="text"/> </div> <input type="button" value="Add"/>

Fig. 113: **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
<b>Group Description</b>	Enter a unique name for the <b>Drop In</b> group.
<b>Mode</b>	<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"> <li>• <i>Transparent</i> (default value): ARP packets and IP packets belonging to the drop-in network are routed transparently (unchanged).</li> <li>• <i>Proxy</i>: ARP packets and IP packets related to the drop-in network are forwarded with the MAC address of the corresponding interface.</li> </ul>
<b>Exclude from NAT (DMZ)</b>	<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> <p>The function is disabled by default.</p>
<b>Network Configuration</b>	<p>Select how an IP address / netmask is assigned to the <b>Drop In</b> network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Static</i> (default value)</li> <li>• <i>DHCP</i></li> </ul>
<b>Network Address</b>	<p>Only for <b>Network Configuration</b> = <i>Static</i></p> <p>Enter the network address of the <b>Drop In</b> network.</p>
<b>Netmask</b>	<p>Only for <b>Network Configuration</b> = <i>Static</i></p> <p>Enter the corresponding netmask.</p>
<b>Local IP Address</b>	<p>Only for <b>Network Configuration</b> = <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>

Field	Description
<b>DHCP Client on Interface</b>	<p>Only for <b>Network Configuration</b> = <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>
<b>ARP Lifetime</b>	<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>
<b>DNS assignment via DHCP</b>	<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"> <li>• <i>Unchanged</i> (default value)</li> <li>• <i>Own IP Address</i></li> </ul>
<b>Interface Selection</b>	<p>Select all the ports which are to be included in the <b>Drop In</b> group (in the network).</p> <p>Add new entries with <b>Add</b>.</p>

## Chapter 11 Routing Protocols

### 11.1 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.

#### 11.1.1 RIP Interfaces

A list of all RIP interfaces is displayed in the **Routing Protocols->RIP->RIP Interfaces** menu.


RIP Interfaces RIP Filter RIP Options

No.	Interface	Send Version	Receive Version	Route Announce	
1	en1-0	None	None	Up only	
2	en1-4	None	None	Up only	

Page: 1, Items: 1 - 2

Fig. 114: Routing Protocols->RIP->RIP Interfaces

##### 11.1.1.1 Edit

For every RIP interface, go to the  menu to select the options *Send Version*, *Receive Version* and *Route Announce*.

[RIP Interfaces](#)   [RIP Filter](#)   [RIP Options](#)

RIP Parameters for: en1-0	
Send Version	None ▾
Receive Version	None ▾
Route Announce	Up only ▾

Fig. 115: 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
<b>Send Version</b>	<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"> <li>• <i>None</i> (default value): RIP is not enabled.</li> <li>• <i>RIP V1</i>: Enables sending and receiving of version 1 RIP packets.</li> <li>• <i>RIP V2</i>: Enables sending and receiving of version 2 RIP packets.</li> <li>• <i>RIP V1/V2</i>: Enables sending and receiving RIP packets of both version 1 and 2.</li> <li>• <i>RIP V2 Multicast</i>: For sending RIP V2 messages over multicast address 224.0.0.9.</li> <li>• <i>RIP V1 Triggered</i>: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP).</li> <li>• <i>RIP V2 Triggered</i>: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).</li> </ul>
<b>Receive Version</b>	<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"> <li>• <i>None</i> (default value): RIP is not enabled.</li> <li>• <i>RIP V1</i>: Enables sending and receiving of version 1 RIP packets.</li> <li>• <i>RIP V2</i>: Enables sending and receiving of version 2 RIP packets.</li> <li>• <i>RIP V1/V2</i>: Enables sending and receiving RIP packets of both version 1 and 2.</li> <li>• <i>RIP V1 Triggered</i>: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP).</li> <li>• <i>RIP V2 Triggered</i>: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).</li> </ul>
<b>Route Announce</b>	<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"> <li>• <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.</li> <li>• <i>Up only</i> (default value): Routes are only propagated if the interface status is up.</li> <li>• <i>Always</i>: Routes are always propagated independently of operational status.</li> </ul>

### 11.1.2 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. 116: **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.

### 11.1.2.1 New

Choose the **New** button to set up more RIP filters.



Fig. 117: **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
<b>Interface</b>	Select the interface to which the rule to be configured applies.
<b>IP Address / Netmask</b>	<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>
<b>Direction</b>	<p>Select whether the filter applies to the export or import of routes.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Import</i> (default value)</li> <li>• <i>Export</i></li> </ul>
<b>Metric Offset for Active Interfaces</b>	<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 <math>-16</math> to <math>16</math>.</p> <p>The default value is <math>0</math>.</p>
<b>Metric Offset for Inactive Interfaces</b>	<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 <math>-16</math> to <math>16</math>.</p> <p>The default value is <math>0</math>.</p>

## 11.1.3 RIP Options

RIP Interfaces RIP Filter **RIP 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

OK Cancel

Fig. 118: 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
<b>RIP UDP Port</b>	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 <i>520</i> should be retained.
<b>Default Route Distribution</b>	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.
<b>Poisoned Reverse</b>	Select the procedure for preventing routing loops.  With standard RIP, the routes learnt are propagated over all interfaces with RIP SEND activated. With <b>Poisoned Reverse</b> , 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>
<b>RFC 2453 Variable Timer</b>	<p>For the timers described in RFC 2453, select whether the same values that you can configure in the <b>Timer for RIP V2 (RFC 2453)</b> 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>
<b>RFC 2091 Variable Timer</b>	<p>For the timers described in RFC 2091, select whether the same values that you can configure in the <b>Timer for Triggered RIP (RFC 2091)</b> 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
<b>Update Timer</b>	<p>Only for <b>RFC 2453 Variable Timer</b> = <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>
<b>Route Timeout</b>	<p>Only for <b>RFC 2453 Variable Timer</b> = <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
<b>Garbage Collection Timer</b>	<p>Only for <b>RFC 2453 Variable Timer</b> = <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
<b>Hold Down Timer</b>	<p>Only for <b>RFC 2091 Variable Timer</b> = <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 be deleted once this period has elapsed.</p> <p>The default value is <i>120</i> (seconds).</p>
<b>Retransmission Timer</b>	<p>Only for <b>RFC 2091 Variable Timer</b> = <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>

## Chapter 12 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.

## 12.1 General

## 12.1.1 General

In the **Multicast->General->General** menu you can disable or enable the multicast function.

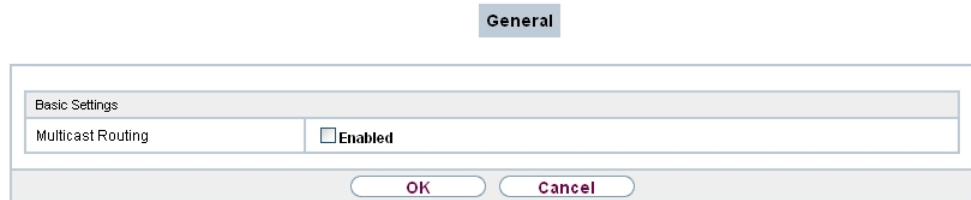


Fig. 119: **Multicast->General->General**

The **Multicast->General->General** menu consists of the following fields:

### Fields in the **Basic Settings** menu.

Field	Description
<b>Multicast Routing</b>	<p>Select whether <b>Multicast Routing</b> should be used.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

## 12.2 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.



## 12.2.1 IGMP

In this menu, you configure the interfaces on which IGMP is to be enabled.

### 12.2.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to configure IGMP on other interfaces.

IGMP Options

IGMP Settings	
Interface	None <span style="float: right;">▼</span>
Query Interval	125 <span style="float: right;">Seconds</span>
Maximum Response Time	10,0 <span style="float: right;">Seconds</span>
Robustness	2 <span style="float: right;">▼</span>
Last Member Query Interval	1,0 <span style="float: right;">Seconds</span>
IGMP State Limit	0 <span style="float: right;">Messages per Second</span>
Mode	<input type="radio"/> Host <input checked="" type="radio"/> Routing

Advanced Settings

IGMP Proxy	<input type="checkbox"/> Enabled
------------	----------------------------------

OK Cancel

Fig. 120: Multicast->IGMP->IGMP->New

The **Multicast->IGMP->IGMP->New** menu consists of the following fields:

#### Fields in the IGMP Settings menu.

Field	Description
<b>Interface</b>	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
<b>Query Interval</b>	Enter the interval in seconds in which IGMP queries are to be sent.  Possible values are 0 to 600.  The default value is 125.
<b>Maximum Response</b>	For the sending of queries, enter the time interval in seconds

Field	Description
<b>Time</b>	<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>
<b>Robustness</b>	<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>
<b>Last Member Query Interval</b>	<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>
<b>IGMP State Limit</b>	<p>Limit the number of reports/queries per second for the selected interface.</p>
<b>Mode</b>	<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"> <li>• <i>Routing</i> (default value): The interface is operated in Routing mode.</li> <li>• <i>Host</i>: The interface is only operated in host mode.</li> </ul>

### 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 IGMP Proxy interface.

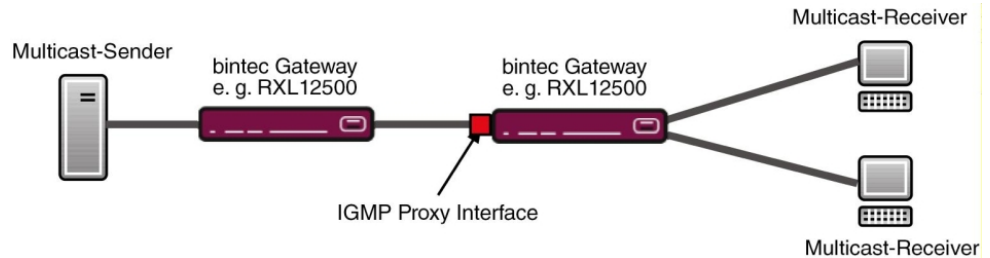


Fig. 121: IGMP Proxy

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>IGMP Proxy</b>	Select whether your device is to forward the hosts' IGMP messages in the subnet via its defined <b>Proxy Interface</b> .
<b>Proxy Interface</b>	Only for <b>IGMP Proxy</b> = enabled  Select the interface on your device via which queries are to be received and collected.

### 12.2.2 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	<input type="radio"/> Up <input type="radio"/> Down <input checked="" type="radio"/> Auto
Mode	<input checked="" type="radio"/> Compatibility Mode <input type="radio"/> Version 3 only
Maximum Groups	<input style="width: 100%;" type="text" value="64"/>
Maximum Sources	<input style="width: 100%;" type="text" value="64"/>
IGMP State Limit	<input style="width: 100%;" type="text" value="0"/> Messages per Second

OK
Cancel

Fig. 122: Multicast->IGMP->Options

The **Multicast->IGMP->Options** menu consists of the following fields:

#### Fields in the Basic Settings menu.

Field	Description
<b>IGMP Status</b>	Select the IGMP status.  Possible values: <ul style="list-style-type: none"> <li>• <i>Auto</i> (default value): Multicast is activated automatically for hosts if the hosts open applications that use multicast.</li> <li>• <i>Up</i>: Multicast is always on.</li> <li>• <i>Down</i>: Multicast is always off.</li> </ul>
<b>Mode</b>	Only for <b>IGMP Status</b> = <i>Up</i> or <i>Auto</i>  Select Multicast Mode.  Possible values: <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Version 3 only</i>: Only IGMP version 3 is used.</li> </ul>
<b>Maximum Groups</b>	Enter the maximum number of groups to be permitted, both internally and in reports.  The default value is <i>64</i> .
<b>Maximum Sources</b>	Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed

Field	Description
	sources per group. The default value is 64.
<b>IGMP State Limit</b>	Enter the maximum permitted total number of incoming queries and messages per second. The default value is 0, i.e. the number of IGMP status messages is not limited.

## 12.3 Forwarding

### 12.3.1 Forwarding

In this menu, you specify which multicast groups are always passed between the interfaces of your device.

#### 12.3.1.1 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 style="width: 100%;" type="text"/>
Source Interface	None <span style="font-size: small;">▼</span>
Destination Interface	None <span style="font-size: small;">▼</span>

Fig. 123: Multicast->Forwarding->Forwarding->New

The **Multicast->Forwarding->Forwarding->New** menu consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>All Multicast Groups</b>	Select whether all multicast groups, i.e. the complete multicast address range 224.0.0.0/4, are to be forwarded from the defined <b>Source Interface</b> to the defined <b>Destination Interface</b> . To do

Field	Description
	<p>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> <p>The option is deactivated by default.</p>
<b>Multicast Group Address</b>	<p>Only for <b>All Multicast Groups</b> = not active.</p> <p>Enter here the address of the multicast group you want to forward from a defined <b>Source Interface</b> to a defined <b>Destination Interface</b>.</p>
<b>Source Interface</b>	<p>Select the interface on your device to which the selected multicast group is sent.</p>
<b>Destination Interface</b>	<p>Select the interface on your device to which the selected multicast group is to be forwarded.</p>

## Chapter 13 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.

### 13.1 Internet + Dialup

In this menu, you can set up Internet access or dialup connections.

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 specified number of seconds)

Field	Description
	administratively set to down (deactivated); connection setup not possible for leased lines:

## Authentication

When a call is received, 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. First 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.

## 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, be aware of differing values for **Metric**.

## 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.

## Callback

The callback mechanism can be used for every connection 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.

## 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.

## Channel Bundling

Your device supports dynamic and static channel bundling for dialup connections. 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.

### 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.

Channel bundling can only be used for ISDN connections for a bandwidth increase or as a backup. 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.

## 13.1.1 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 AD-

SL access. However, PPPoE is now offered here too by some providers.

### 13.1.1.1 New

Choose the **New** button to set up new PPPoE interfaces.

PPPoE PPTP PPPoA ISDN AUX IP Pools

Basic Parameters	
Description	<input type="text"/>
PPPoE Mode	<input checked="" type="radio"/> Standard <input type="radio"/> Multilink
PPPoE Ethernet Interface	Select one ▾
User Name	<input type="text"/>
Password	<input type="password" value="*****"/>
Always on	<input type="checkbox"/> Enabled
Connection Idle Timeout	300 <input type="text"/> Seconds
IPv4 Settings	
Security Policy	<input checked="" type="radio"/> Untrusted <input type="radio"/> Trusted
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
IPv6 Settings	
IPv6	<input type="checkbox"/> Enabled
Advanced Settings	
Block after connection failure for	60 <input type="text"/> Seconds
Maximum Number of Dialup Retries	5 <input type="text"/>
Authentication	PAP/CHAP ▾
DNS Negotiation	<input checked="" type="checkbox"/> Enabled
Prioritize TCP ACK Packets	<input type="checkbox"/> Enabled
LCP Alive Check	<input checked="" type="checkbox"/> Enabled
IPv4 Advanced Settings	
MTU	<input checked="" type="checkbox"/> Automatic
<input type="button" value="OK"/> <input type="button" value="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
<b>Description</b>	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number No special charac-

Field	Description
	ters or umlauts must be used.
<b>PPPoE Mode</b>	<p>Select whether you want to use a standard Internet connection over PPPoE ( <i>Standard</i>) or your Internet access is to be set 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>
<b>PPPoE Ethernet Interface</b>	<p>Only for <b>PPPoE Mode</b> = <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 <b>WAN-&gt;ATM-&gt;Profiles-&gt;New</b>.</p> <p>Select <i>Automatic</i> in order to enable the automatic VDSL/ADSL mode. In this mode, the interface for the Internet connection is selected automatically. Note that there has to be an interface entry in the <b>ATM</b> menu. This is not required for a VDSL connection.</p>
<b>PPPoE Interfaces for Multilink</b>	<p>Only for <b>PPPoE Mode</b> = <i>Multilink</i></p> <p>Select the interfaces you want to use for your Internet connection. Click the <b>Add</b> button to create new entries.</p>
<b>User Name</b>	Enter the user name.
<b>Password</b>	Enter the password.
<b>VLAN</b>	Certain Internet service providers require a VLAN-ID. Activate

Field	Description
	this function to be able to enter a value under <b>VLAN ID</b> .
<b>VLAN ID</b>	<p>Only if <b>VLAN</b> is enabled.</p> <p>Enter the VLAN-ID that you received from your provider.</p>
<b>Always on</b>	<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>
<b>Connection Idle Timeout</b>	<p>Only if <b>Always on</b> 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 IPv4 Settings menu.

Field	Description
<b>Security Policy</b>	<p>Select the security settings to be used with the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i> : All IP packets are allowed through except for those which are explicitly prohibited.</li> <li>• <i>Untrusted</i> (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone.</li> </ul> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>

Field	Description
<b>IP Address Mode</b>	<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"> <li>• <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.</li> <li>• <i>Static</i>: You enter a static IP address.</li> </ul>
<b>Default Route</b>	<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>
<b>Create NAT Policy</b>	<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>
<b>Local IP Address</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Enter the static IP address of the connection partner.</p>
<b>Route Entries</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <p>Add new entries with <b>Add</b>.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or network.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b> If no entry is made, your device uses a default netmask.</li> <li>• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.</li> </ul>

#### Fields in the IPv6 Settings menu

Field	Description
<b>IPv6</b>	Select whether the selected PPPoE interface should use Inter-

Field	Description
	<p>net Protocol version 6 (IPv6) for data transmission.</p> <p>The function is activated by selecting <i>Enabled</i> .</p> <p>The function is disabled by default.</p>
<b>Security Policy</b>	<p>Select the security settings to be used with the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Untrusted</i> (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 outside of your LAN.</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i>: All IP packets are allowed through except for those which are explicitly prohibited.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 on your LAN.</p> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>
<b>IPv6 Mode</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i></p> <p>The selected PPPoE interface is operated in host mode.</p>
<b>Accept Router Advertisement</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Host</i></p> <p>Select if Router Advertisements are to be received on the selected interface. Router Advertisements are used, e.g., to create the prefix list.</p> <p>The function is activated by selecting <i>Enabled</i> .</p> <p>The function is enabled by default.</p>
<b>DHCP Client</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Host</i></p> <p>Determine if your device is to act as DHCP client.</p> <p>The function is activated by selecting <i>Enabled</i> .</p> <p>The function is enabled by default.</p>

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Block after connection failure for</b>	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> .
<b>Maximum Number of Dialup Retries</b>	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> .
<b>Authentication</b>	Select the authentication protocol for this connection partner. Select the authentication specified by your provider.  Possible values:  <ul style="list-style-type: none"> <li>• <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <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.)</li> <li>• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>DNS Negotiation</b>	Select whether your device receives IP addresses for <b>Primary DNS Server</b> and <b>Secondary DNS Server</b> 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.

Field	Description
<b>Prioritize TCP ACK Packets</b>	<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>
<b>LCP Alive Check</b>	<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>

#### Fields in the IPv4 Advanced Settings menu

Field	Description
<b>MTU</b>	<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> <p>The default value is <i>0</i>.</p>

## 13.1.2 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.

### 13.1.2.1 New

Choose the **New** button to set up new PPTP interfaces.



PPPoE **PPTP** PPPoA ISDN AUX IP Pools

Basic Parameters	
Description	<input type="text"/>
PPTP Ethernet Interface	Select one ▾
User Name	<input type="text"/>
Password	..... <input type="text"/>
Always on	<input type="checkbox"/> Enabled
Connection Idle Timeout	<input type="text" value="300"/> Seconds
IPv4 Settings	
Security Policy	<input checked="" type="radio"/> Untrusted <input type="radio"/> Trusted
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	<input type="text" value="60"/> Seconds
Maximum Number of Dialup Retries	<input type="text" value="5"/>
Authentication	PAP ▾
DNS Negotiation	<input checked="" type="checkbox"/> Enabled
Prioritize TCP ACK Packets	<input type="checkbox"/> Enabled
PPTP Address Mode	Static
Local PPTP IP Address	<input type="text" value="10.0.0.140"/>
Remote PPTP IP Address	<input type="text" value="10.0.0.138"/>
LCP Alive Check	<input checked="" type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="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
<b>Description</b>	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.
<b>PPTP Ethernet Interface</b>	Select the IP interface over which packets are to be transported to the remote PPTP terminal.  If you want to use an external DSL modem, select the Ethernet port to which the modem is connected.

Field	Description
	When using the internal DSL modem, select here the EthoA interface configured in <b>Physical Interfaces-&gt;ATM-&gt;Profiles-&gt;New</b> , e.g. <i>ethoa50-0</i> .
<b>User Name</b>	Enter the user name.
<b>Password</b>	Enter the password.
<b>Always on</b>	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.
<b>Connection Idle Timeout</b>	Only if <b>Always on</b> is disabled.  Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection.  Possible values are 0 to 3600 (seconds). 0 deactivates the timeout.  The default value is 300.  Example: 10 for FTP transmission, 20 for LAN-to-LAN transmission, 90 for Internet connections.

#### Fields in the IPv4 Settings menu.

Field	Description
<b>Security Policy</b>	Select the security settings to be used with the interface.  Possible values: <ul style="list-style-type: none"> <li>• <i>Trusted</i>: All IP packets are allowed through except for those which are explicitly prohibited..</li> <li>• <i>Untrusted</i> (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone.</li> </ul>

Field	Description
	You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.
<b>IP Address Mode</b>	<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"> <li>• <i>Get IP Address</i> (default value): Your device is automatically assigned a temporarily valid IP address from the provider.</li> <li>• <i>Static</i> : You enter a static IP address.</li> </ul>
<b>Default Route</b>	<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>
<b>Create NAT Policy</b>	<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>
<b>Local IP Address</b>	<p>Only for <b>IP Address Mode</b> = <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>
<b>Route Entries</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Define other routing entries for this PPTP partner.</p> <p>Add new entries with <b>Add</b>.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or network.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b> If no entry is made, your device uses a default netmask.</li> <li>• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.</li> </ul>

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Block after connection failure for</b>	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> .
<b>Maximum Number of Dialup Retries</b>	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> .
<b>Authentication</b>	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider.  Possible values:  <ul style="list-style-type: none"> <li>• <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <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.)</li> <li>• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>DNS Negotiation</b>	Select whether your device receives IP addresses for <b>Primary DNS Server</b> and <b>Secondary DNS Server</b> 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.

Field	Description
<b>Prioritize TCP ACK Packets</b>	<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>
<b>PPTP Address Mode</b>	<p>Displays the address mode. The value cannot be changed.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Static</i>: The <b>Local PPTP IP Address</b> will be assigned to the selected Ethernet port.</li> </ul>
<b>Local PPTP IP Address</b>	<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>
<b>Remote PPTP IP Address</b>	<p>Enter the IP address of the PPTP partner.</p> <p>The default value is <i>10.0.0.138</i>.</p>
<b>LCP Alive Check</b>	<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>

### 13.1.3 PPPoA

A list of all PPPoA interfaces is displayed in the **WAN->Internet + Dialup->PPPoA** menu.

In this menu, you configure a xDSL connection used to set up PPPoA connections. With PPPoA, the connection is configured so that the PPP data flow is transported directly over an ATM network (RFC 2364). This is required by some providers. Note your provider's specifications.

When using the internal DSL modem, a PPPoA interface must be configured with **Client Type = On Demand** for this connection in **WAN->ATM->Profiles->New**.

### 13.1.3.1 New

Choose the **New** button to set up new PPPoA interfaces.

PPPoE PPTP PPPoA ISDN AUX IP Pools

Basic Parameters	
Description	<input type="text"/>
ATM PVC	<input type="text" value="Select one"/>
User Name	<input type="text"/>
Password	<input type="password" value="....."/>
Always on	<input type="checkbox"/> Enabled
Connection Idle Timeout	<input type="text" value="300"/> Seconds
IPv4 Settings	
Security Policy	<input checked="" type="radio"/> Untrusted <input type="radio"/> Trusted
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
IPv6 Settings	
IPv6	<input type="checkbox"/> Enabled
Advanced Settings	
Block after connection failure for	<input type="text" value="60"/> Seconds
Maximum Number of Dialup Retries	<input type="text" value="5"/>
Authentication	<input type="text" value="PAP"/>
DNS Negotiation	<input checked="" type="checkbox"/> Enabled
Prioritize TCP ACK Packets	<input type="checkbox"/> Enabled
LCP Alive Check	<input checked="" type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 126: WAN->Internet + Dialup->PPPoA->New

The menu **WAN->Internet + Dialup->PPPoA->New** consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>Description</b>	Enter a name for uniquely identifying the connection partner. The first character in this field must not be a number No special characters or umlauts must be used.
<b>ATM PVC</b>	Select an ATM profile created in the <b>ATM-&gt;Profiles</b> menu, indicated by the global identifiers VPI and VCI specified by the

Field	Description
	provider.
<b>User Name</b>	Enter the user name.
<b>Password</b>	Enter the password for the PPPoA connection.
<b>Always on</b>	<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>
<b>Connection Idle Timeout</b>	<p>Only if <b>Always on</b> 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 IPv4 Settings menu.

Field	Description
<b>Security Policy</b>	<p>Select the security settings to be used with the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i>: All IP packets are allowed through except for those which are explicitly prohibited..</li> <li>• <i>Untrusted</i> (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone.</li> </ul> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>

Field	Description
<b>IP Address Mode</b>	<p>Choose whether your device has a static IP address or is assigned one dynamically.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.</li> <li>• <i>Static</i>: You enter a static IP address.</li> </ul>
<b>Default Route</b>	<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>
<b>Create NAT Policy</b>	<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>
<b>Local IP Address</b>	<p>Only for <b>IP Address Mode</b> = <i>Static</i></p> <p>Enter the static IP address you received from your provider.</p>
<b>Route Entries</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <p>Add new entries with <b>Add</b>.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or network.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b> If no entry is made, your device uses a default netmask.</li> <li>• <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>.</li> </ul>

#### Fields in the IPv6 Settings menu

Field	Description
<b>IPv6</b>	Select whether the selected ATM profile should use Internet



Field	Description
	<p>Protocol version 6 (IPv6) for data transmission.</p> <p>The function is activated by selecting <i>Enabled</i> .</p> <p>The function is disabled by default.</p>
<b>Security Policy</b>	<p>Select the security settings to be used with the ATM profile.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Untrusted</i> (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 outside of your LAN.</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i>: All IP packets are allowed through except for those which are explicitly prohibited.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 on your LAN.</p> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>
<b>IPv6 Mode</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i></p> <p>The selected PPPoE interface is operated in host mode.</p>
<b>Accept Router Advertisement</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Host</i></p> <p>Determine if Router Advertisements are to be received over this ATM profile. Router Advertisements are used to create the default router list as well as the prefix list.</p> <p>The function is activated by selecting <i>Enabled</i> .</p> <p>The function is enabled by default.</p>
<b>DHCP Client</b>	<p>Only for <b>IPv6</b> = <i>Enabled</i> and <b>IPv6 Mode</b> = <i>Host</i></p> <p>Determine if your device is to act as DHCP client.</p> <p>The function is activated by selecting <i>Enabled</i> .</p> <p>The function is enabled by default.</p>

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Block after connection failure for</b>	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> .
<b>Maximum Number of Dialup Retries</b>	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> .
<b>Authentication</b>	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider.  Possible values:  <ul style="list-style-type: none"> <li>• <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <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.)</li> <li>• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>DNS Negotiation</b>	Select whether your device receives IP addresses for <b>Primary DNS Server</b> and <b>Secondary DNS Server</b> 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.

Field	Description
<b>Prioritize TCP ACK Packets</b>	<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>
<b>LCP Alive Check</b>	<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>

### 13.1.4 ISDN

A list of all ISDN interfaces is displayed in the **WAN->Internet + Dialup->ISDN** menu.

In this menu, you configure the following ISDN connections:

- Internet access over ISDN
- LAN to LAN connection over ISDN
- Remote (Mobile) dial-in
- Use of the ISDN Callback function

#### 13.1.4.1 New

Choose the **New** button to set up new ISDN interfaces.

<a href="#">PPPoE</a> <a href="#">PPTP</a> <a href="#">PPPoA</a> <a href="#">ISDN</a> <a href="#">AUX</a> <a href="#">IP Pools</a>							
<b>Basic Parameters</b>							
Description	<input type="text"/>						
Connection Type	ISDN 64 kbps <input type="button" value="v"/>						
User Name	<input type="text"/>						
Remote User (for Dialin only)	<input type="text"/>						
Password	••••••••						
Always on	<input type="checkbox"/> Enabled						
Connection Idle Timeout	20 <b>Seconds</b>						
<b>IP Mode and Routes</b>							
IP Address Mode	<input checked="" type="radio"/> Static <input type="radio"/> Provide IP Address <input type="radio"/> Get IP Address						
Default Route	<input type="checkbox"/> Enabled						
Create NAT Policy	<input type="checkbox"/> Enabled						
Local IP Address	<input type="text"/>						
Route Entries	<table border="1"> <thead> <tr> <th>Remote IP Address</th> <th>Netmask</th> <th>Metric</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td>1 <input type="button" value="v"/></td> </tr> </tbody> </table> <input type="button" value="Add"/>	Remote IP Address	Netmask	Metric	<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>
Remote IP Address	Netmask	Metric					
<input type="text"/>	<input type="text"/>	1 <input type="button" value="v"/>					
<b>Advanced Settings</b>							
Block after connection failure for	300 <b>Seconds</b>						
Maximum Number of Dialup Retries	5						
Usage Type	<input checked="" type="radio"/> Standard <input type="radio"/> Dialin only <input type="radio"/> Multi-User (Dialin only)						
Authentication	PAP/CHAP/MS-CHAP <input type="button" value="v"/>						
Callback Mode	<input checked="" type="radio"/> None <input type="radio"/> Active <input type="radio"/> Passive						
<b>Bandwith on Demand Options</b>							
Channel Bundling	None <input type="button" value="v"/>						
<b>Dial Numbers</b>							
Entries	<table border="1"> <thead> <tr> <th>Mode</th> <th>Number</th> <th>Number of Used Ports</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table> <input type="button" value="Add"/>	Mode	Number	Number of Used Ports	<input type="text"/>	<input type="text"/>	<input type="text"/>
Mode	Number	Number of Used Ports					
<input type="text"/>	<input type="text"/>	<input type="text"/>					
<b>IP Options</b>							
OSPF Mode	<input checked="" type="radio"/> Passive <input type="radio"/> Active <input type="radio"/> Inactive						
Proxy ARP Mode	<input checked="" type="radio"/> Inactive <input type="radio"/> Up or Dormant <input type="radio"/> Up only						
DNS Negotiation	<input checked="" type="checkbox"/> Enabled						
<input type="button" value="OK"/> <input type="button" value="Cancel"/>							

Fig. 127: WAN->Internet + Dialup->ISDN->New

The menu **WAN->Internet + Dialup->ISDN->New** consists of the following fields:

**Fields in the Basic Parameters menu.**

Field	Description
<b>Description</b>	<p>Enter a name for uniquely identifying the connection partner.</p> <p>The first character in this field must not be a number No special characters or umlauts must be used.</p>
<b>Connection Type</b>	<p>Select which layer 1 protocol your device should use.</p> <p>This setting applies for outgoing connections to the connection partner and only for incoming connections from the connection partner if they could be identified on the basis of the calling party number.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>ISDN 64 kbps</i>: For 64-kbps ISDN data connections.</li> <li>• <i>ISDN 56 kbps</i>: For 56-kbps ISDN data connections.</li> </ul>
<b>User Name</b>	Enter your device code (local PPP user name).
<b>Remote User (for Dial-in only)</b>	Enter the code of the remote terminal (remote PPP user name).
<b>Password</b>	Enter the password.
<b>Always on</b>	<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>
<b>Connection Idle Timeout</b>	<p>Only if <b>Always on</b> 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 0 to 3600 (seconds). 0 deactivates the timeout. The default value is 20.</p>

**Fields in the IP Mode and Routes menu.**

Field	Description
<b>IP Address Mode</b>	<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"> <li>• <i>Static</i> (default value): You enter a static IP address.</li> <li>• <i>Provide IP Address</i>: Your device dynamically assigns an IP address to the remote terminal.</li> <li>• <i>Get IP Address</i>: Your device is dynamically assigned an IP address.</li> </ul>
<b>Default Route</b>	<p>Only for <b>IP Address Mode</b> = <i>Static</i> and <i>Get IP Address</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>
<b>Create NAT Policy</b>	<p>Only for <b>IP Address Mode</b> = <i>Static</i> and <i>Get IP Address</i></p> <p>When you configure an ISDN Internet connection, 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 disabled by default.</p>
<b>Local IP Address</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Assign the IP address from your LAN to the ISDN interface which is to be used as your device's internal source address.</p>
<b>Route Entries</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or network.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b> If no entry is made, your device uses a default netmask.</li> <li>• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.</li> </ul>

Field	Description
<b>IP Assignment Pool</b>	<p>Only if <b>IP Address Mode</b> = <i>Provide IP Address</i></p> <p>Select IP pools configured in the <b>WAN-&gt;Internet + Dialup-&gt;IP Pools</b> 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
<b>Block after connection failure for</b>	<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>
<b>Maximum Number of Dialup Retries</b>	<p>Enter the number of unsuccessful attempts to setup a connection before the interface is blocked.</p> <p>Possible values are <i>0</i> to <i>100</i>.</p> <p>The default value is <i>5</i>.</p>
<b>Usage Type</b>	<p>If necessary, select a special interface use.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (default value): No special type is selected.</li> <li>• <i>Dialin only</i>: The interface is used for incoming dialup connections and callbacks initiated externally.</li> <li>• <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.</li> </ul>
<b>Authentication</b>	<p>Select the authentication protocol for this PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>PAP</i> (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <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.)</li> <li>• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>Encryption</b>	<p>Only for <b>Authentication</b> = <i>MS-CHAPv2</i></p> <p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If <b>Encryption</b> 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"> <li>• <i>None</i> (default value): MPP encryption is not used.</li> <li>• <i>Enabled</i>: MPP encryption V2 with 128 bit is used to RFC 3078.</li> <li>• <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.</li> </ul>
<b>Callback Mode</b>	<p>Select the Callback Mode function.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>None</i> (default value): Your device does not call back.</li> <li>• <i>Active</i>: Select one of the following options: <ul style="list-style-type: none"> <li>• <i>No PPP negotiation</i>: Your device calls the connection partner to request a callback.</li> <li>• <i>Windows Client Mode</i>: Your device calls the connection partner to request a callback via CBCP (Callback Control Protocol). Needed for Windows clients.</li> </ul> </li> <li>• <i>Passive</i>: Select one of the following options: <ul style="list-style-type: none"> <li>• <i>PPP Negotiation or CLID</i>: Your device calls back immediately when requested to do so by the connection partner.</li> </ul> </li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• <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 (<b>Entries-&gt;Call Number</b>) with the <b>Mode</b> <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. At present, this cannot be avoided when connecting mobile Microsoft clients via a DCN.</li> <li>• <i>Delayed, CLID only</i>: Your device calls back after approx. four seconds if your device is requested to do so by the connection partner. Only makes sense for CLID.</li> <li>• <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 closing the dialog box that appears with <b>Cancel</b>.</li> </ul>

#### Fields in the **Bandwith on Demand Options** menu.

Field	Description
<b>Channel Bundling</b>	<p>Select whether channel bundling is to be used for ISDN connections with the connection partner, and if so, what type.</p> <p>Your device supports dynamic and static channel bundling for dialup connections. Only one B-channel is initially opened when a connection is set up. 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. In static channel bundling, you specify right from the start how many B-channels your device is to use, regardless of the transferred data rate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>None</i> (default value): No channel bundling, only one B-channel is ever available for connections.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Static</i>: Static channel bundling.</li> <li>• <i>Dynamic</i>: Dynamic channel bundling.</li> </ul>

#### Fields in the **Dial Numbers** menu

Field	Description
<b>Entries</b>	Add new entries with <b>Add</b> .

#### Fields in menu **Dial Number Configuration** (appears only for **Entries = Add**)

Field	Description
<b>Mode</b>	<p>Only if <b>Entries = Add</b></p> <p>The calling party number of the call is compared with the number entered under <b>Call Number</b>. Defines whether <b>Call Number</b> should be used for incoming or outgoing calls or for both. Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Both</i> (default value): For incoming and outgoing calls.</li> <li>• <i>Incoming</i>: For incoming calls, where your connection partner dials in to your device.</li> <li>• <i>Outgoing</i>: For outgoing calls, where you dial your connection partner.</li> </ul> <p>The calling party number of the incoming call is compared with the number entered under <b>Call Number</b>.</p>
<b>Call Number</b>	Enter the connection partner's numbers.
<b>Number of Used Ports</b>	Select which port is used.

#### Fields in the **IP Options** menu.

Field	Description
<b>OSPF Mode</b>	<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"> <li>• <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.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface.</li> <li>• <i>Inactive</i>: OSPF is disabled for this interface.</li> </ul>
<b>Proxy ARP Mode</b>	<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"> <li>• <i>Inactive</i> (default value): Deactivates Proxy ARP for this connection partner.</li> <li>• <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>Dormant</i>, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route.</li> <li>• <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.</li> </ul>
<b>DNS Negotiation</b>	<p>Select whether your device receives IP addresses for <b>Primary DNS Server</b> and <b>Secondary DNS Server</b> and <b>WINS Server Primary</b> and <b>Secondary</b> 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>

### 13.1.5 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.

### 13.1.5.1 New

Choose the **New** button to create additional connections.

PPPoE PPTP **UMTS/LTE** IP Pools

Basic Parameters	
Description	<input type="text"/>
UMTS/LTE Interface	UMTS-6-0 <span style="float: right;">▼</span>
User Name	<input type="text"/>
Password	<input type="password" value="••••••"/>
Always on	<input type="checkbox"/> Enabled
Connection Idle Timeout	<input type="text" value="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	<input type="text" value="60"/> Seconds
Maximum Number of Dialup Retries	<input type="text" value="5"/>
Authentication	PAP <span style="float: right;">▼</span>
DNS Negotiation	<input checked="" type="checkbox"/> Enabled
Prioritize TCP ACK Packets	<input type="checkbox"/> Enabled
LCP Alive Check	<input checked="" type="checkbox"/> Enabled
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 128: 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
<b>Description</b>	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.
<b>UMTS/LTE Interface</b>	Select the UMTS/LTE interface. In <b>RS120wu</b> the integrated modem with slot 6 unit 0 UMTS is preselected; for devices with an optional plug-in UMTS/LTE stick the USB port of the device is

Field	Description
	preselected.
<b>User Name</b>	Enter the user name.
<b>Password</b>	Enter the password.
<b>Always on</b>	<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>
<b>Connection Idle Timeout</b>	<p>Only if <b>Always on</b> 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>

#### Fields in the IP Mode and Routes menu.

Field	Description
<b>IP Address Mode</b>	<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"> <li>• <i>Get IP Address</i> (default value): Your device is dynamically assigned an IP address.</li> <li>• <i>Static</i>: You enter a static IP address.</li> </ul>
<b>Default Route</b>	<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>

Field	Description
<b>Create NAT Policy</b>	<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>
<b>Local IP Address</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Enter the static IP address of the connection partner.</p>
<b>Route Entries</b>	<p>Only if <b>IP Address Mode</b> = <i>Static</i></p> <p>Define other routing entries for this connection partner.</p> <p>Add new entries with <b>Add</b>.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or network.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b> If no entry is made, your device uses a default netmask.</li> <li>• <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>.</li> </ul>

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Block after connection failure for</b>	<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>
<b>Maximum Number of Dialup Retries</b>	<p>Enter the number of unsuccessful attempts to setup a connection before the interface is blocked.</p> <p>Possible values are <i>0</i> to <i>100</i>.</p> <p>The default value is <i>5</i>.</p>
<b>Authentication</b>	<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"> <li>• <i>PAP</i> (default value): Only run <i>PAP</i> (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run <i>CHAP</i> (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <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.)</li> <li>• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>DNS Negotiation</b>	<p>Select whether your device receives IP addresses for <b>DNS Server</b> primary domain name server <b>Primary</b> and <b>DNS Server</b> secondary domain name server <b>Secondary</b> 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>
<b>Prioritize TCP ACK Packets</b>	<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>
<b>LCP Alive Check</b>	<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>


## 13.1.6 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.

### 13.1.6.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

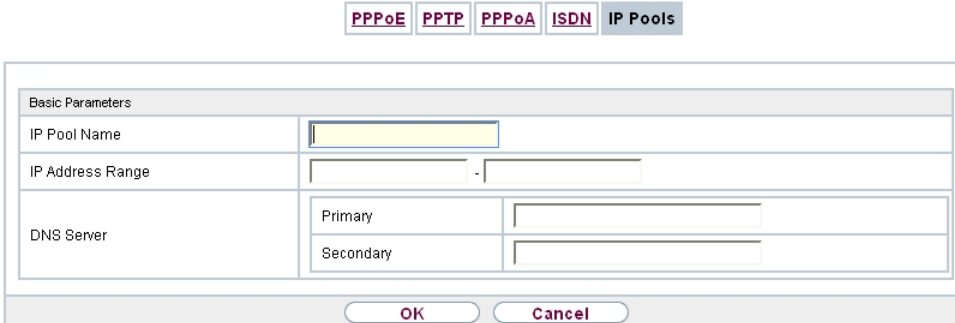


Fig. 129: WAN->Internet + Dialup->IP Pools->New

#### Fields in the menu Basic Parameters

Field	Description
<b>IP Pool Name</b>	Enter any description to uniquely identify the IP pool.
<b>IP Address Range</b>	Enter the first (first field) and last (second field) IP address of the IP address pool.



Field	Description
<b>DNS Server</b>	<p><b>Primary:</b> Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p><b>Secondary:</b> Optionally, enter the IP address of an alternative DNS server.</p>

## 13.2 ATM

ATM (Asynchronous Transfer Mode) is a data transmission procedure that was originally designed for broadband ISDN.

ATM is currently used in high-speed networks. You will need ATM, for example, if you want high-speed access to the Internet via the integrated ADSL or SHDSL modem.

In an ATM network, different applications such as speech, video and data, can be transmitted side-by-side in the asynchronous time multiplex procedure. Each transmitter is provided with time sections for transmitting data. With asynchronous transmission, unused time sections of a transmitter are used by another transmitter.

With ATM, the packet switching procedure is connected-based. A virtual connection is used for data transmission that negotiates between the transmitter and recipient or is configured on both sides. This determines the route that the data should take, for example. Multiple virtual connections can be set up over a single physical interface.

The data is transmitted in so-called cells or slots of constant size. Each cell consists of 48 bytes of usage data and 5 bytes of control information. The control information contains, amongst other things, the ATM address which is similar to the Internet address. The ATM address is made up of the Virtual Path Identifier (VPI) and the Virtual Connection Identifier (VCI); this identifies the virtual connection.

Various types of traffic flows are transported over ATM. To take account of the various demands of these traffic flows on the networks, e.g. in terms of cell loss and delay time, suitable values can be defined using the service categories. Uncompressed video data, for example, requires different parameters to time-uncritical data.

In ATM networks Quality of Service (QoS) is available, i.e. the size of various network parameters, such as bit rate, delay and jitter can be guaranteed.

OAM (Operation, Administration and Maintenance) is used to monitor the data transmission in ATM. OAM includes configuration management, error management and performance measurement.

## 13.2.1 Profiles

A list of all ATM profiles is displayed in the **WAN->ATM->Profiles** menu.

If the connection for your Internet access is set up using the internal modem, the ATM connection parameters must be set for this. An ATM profile combines a set of parameters for a specific provider.

By default an ATM profile with the description *AUTO-CREATED* is preconfigured. Its values (VPI 1 and VCI 32) are suitable for a Telekom ATM connection, for example.



### Note

The ATM encapsulations are described in RFCs 1483 and 2684. You will find the RFCs on the relevant pages of the IETF ([www.ietf.org/rfc.html](http://www.ietf.org/rfc.html)).

### 13.2.1.1 New

Choose the **New** button to set up new ATM profiles.

Profiles
Service Categories
OAM Controlling

ATM Profiles Parameter					
Provider	- User-defined - <span style="float: right;">▼</span>				
Description	<input type="text"/>				
Type	Ethernet over ATM <span style="float: right;">▼</span>				
Virtual Path Identifier (VPI)	<input type="text" value="8"/>				
Virtual Channel Identifier (VCI)	<input type="text" value="32"/>				
Encapsulation	LLC Bridged no FCS <span style="float: right;">▼</span>				
Ethernet over ATM Settings					
Default Ethernet for PPPoE Interfaces	<input type="checkbox"/> Enabled				
Address Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP				
IP Address/Netmask	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; padding: 2px;">IP Address</td> <td style="width: 40%; padding: 2px;">Netmask</td> </tr> <tr> <td colspan="2" style="text-align: center; padding: 2px;"><span style="border: 1px solid gray; padding: 2px 5px;">Add</span></td> </tr> </table>	IP Address	Netmask	<span style="border: 1px solid gray; padding: 2px 5px;">Add</span>	
IP Address	Netmask				
<span style="border: 1px solid gray; padding: 2px 5px;">Add</span>					
MAC Address	<input type="text"/> <input checked="" type="checkbox"/> Use built-in				
<span style="border: 1px solid gray; border-radius: 10px; padding: 5px 15px; margin-right: 20px;">OK</span> <span style="border: 1px solid gray; border-radius: 10px; padding: 5px 15px;">Cancel</span>					

Fig. 130: **WAN->ATM->Profiles->New**

The menu **WAN->ATM->Profiles->New** consists of the following fields:

**Fields in the ATM Profiles Parameter menu.**

Field	Description
<b>Provider</b>	Select one of the preconfigured ATM profiles for your provider from the list or manually define the profile using <code>-- User-defined --</code> .
<b>Description</b>	Only for <b>Provider</b> = <code>-- User-defined --</code> Enter the desired description for the connection.
<b>ATM Interface</b>	Only if several ATM interfaces are available, e.g. if several interfaces are separately configured in devices with SHDSL. Select the ATM interface that you wish to use for the connection.
<b>Type</b>	Only for <b>Provider</b> = <code>-- User-defined --</code> Select the protocol for the ATM connection. Possible values: <ul style="list-style-type: none"> <li>• <i>Ethernet over ATM</i> (default value): Ethernet over ATM (EthoA) is used for the ATM connection (Permanent Virtual Circuit, PVC).</li> <li>• <i>Routed Protocols over ATM</i>: Routed Protocols over ATM (RPoA) is used for the ATM connection (Permanent Virtual Circuit, PVC).</li> <li>• <i>PPP over ATM</i>: PPP over ATM (PPPoA) is used for the ATM connection (Permanent Virtual Circuit, PVC).</li> </ul>
<b>Virtual Path Identifier (VPI)</b>	Only for <b>Provider</b> = <code>-- User-defined --</code> Enter the VPI value of the ATM connection. The VPI is the identification number of the virtual path to be used. Note your provider's instructions. Possible values are 0 to 255. The default value is 8.
<b>Virtual Channel Identifier (VCI)</b>	Only for <b>Provider</b> = <code>-- User-defined --</code> Enter the VCI value of the ATM connection. The VCI is the iden-

Field	Description
	<p>tification number of the virtual channel. A virtual channel is the logical connection for the transport of ATM cells between two or more points. Note your provider's instructions.</p> <p>Possible values are <i>32</i> to <i>65535</i>.</p> <p>The default value is <i>32</i>.</p>
<b>Encapsulation</b>	<p>Only for <b>Provider</b> = <i>-- User-defined --</i></p> <p>Select the encapsulation to be used. Note your provider's instructions.</p> <p>Possible values (in accordance with RFC 2684):</p> <ul style="list-style-type: none"> <li>• <i>LLC Bridged no FCS</i> (Default value for Ethernet over ATM : Is only displayed for <b>Type</b> = <i>Ethernet over ATM</i>. Bridged Ethernet with LLC/SNAP encapsulation without Frame Check Sequence (checksums).</li> <li>• <i>LLC Bridged FCS</i>: only displayed for <b>Type</b> = <i>Ethernet over ATM</i>. Bridged Ethernet with LLC/SNAP encapsulation with Frame Check Sequence (checksums).</li> <li>• <i>Non ISO</i> (default value for Routed Protocols over ATM): Is only displayed for <b>Type</b> = <i>Routed Protocols over ATM</i>. Encapsulation with LLC/SNAP header, suitable for IP routing.</li> <li>• <i>LLC</i>: only displayed for <b>Type</b> = <i>PPP over ATM</i>. Encapsulation with LLC header.</li> <li>• <i>VC Multiplexing</i> (default value for PPP over ATM): Bridged Ethernet without additional encapsulation (Null Encapsulation) with Frame Check Sequence (checksums).</li> </ul>

**Fields in menu Ethernet over ATM Settings (appears only for Type = Ethernet over ATM)**

Field	Description
<b>Default Ethernet for PPPoE Interfaces</b>	<p>Only for <b>Type</b> = <i>Ethernet over ATM</i></p> <p>Select whether this Ethernet-over-ATM interface is to be used for all PPPoE connections</p>

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>Address Mode</b>	<p>Only for <b>Type</b> = <i>Ethernet over ATM</i></p> <p>Select how an IP address is to be assigned to the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Static</i> (default value): The interface is assigned a static IP address in <b>IP Address / Netmask</b>.</li> <li>• <i>DHCP</i>: An IP address is assigned to the interface dynamically via DHCP.</li> </ul>
<b>IP Address/Netmask</b>	<p>Only for <b>Address Mode</b> = <i>Static</i></p> <p>Enter the IP addresses (<b>IP Address</b>) and the corresponding netmasks (<b>Netmask</b>) of the ATM interfaces. Add new entries with <b>Add</b>.</p>
<b>MAC Address</b>	<p>Enter a MAC address for the internal router interface of ATM connection, e.g. <i>00:a0:f9:06:bf:03</i>. An entry is only required in special cases.</p> <p>For Internet connections, it is sufficient to select the option <b>Use built-in</b> (default setting). An address is used which is derived from the MAC address of the <i>en1-0</i>.</p>
<b>DHCP MAC Address</b>	<p>Only for <b>Address Mode</b> = <i>DHCP</i></p> <p>Enter the MAC address of the internal router interface of ATM connection, e.g. <i>00:e1:f9:06:bf:03</i>.</p> <p>If your provider has assigned you a MAC address for DHCP, enter this here.</p> <p>You can also select the <b>Use built-in</b> option (default setting) An address is used which is derived from the MAC address of the <i>en1-0</i>.</p>
<b>DHCP Hostname</b>	<p>Only for <b>Address Mode</b> = <i>DHCP</i></p> <p>If necessary, enter the host name registered with the provider to be used by your device for DHCP requests.</p>

Field	Description
	The maximum length of the entry is 45 characters.

**Fields in menu Routed Protocols over ATM Settings (appears only for Type = Routed Protocols over ATM)**

Field	Description
<b>IP Address/Netmask</b>	Enter the IP addresses ( <b>IP Address</b> ) and the corresponding netmasks ( <b>Netmask</b> ) of the ATM interface. Add new entries with <b>Add</b> .
<b>Prioritize TCP ACK Packets</b>	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).  The function is enabled with <i>Enabled</i> .  The function is disabled by default.

**Field in menu PPP over ATM Settings (appears only for Type = PPP over ATM)**

Field	Description
<b>Client Type</b>	Select whether the PPPoA connection is to be set up permanently or on demand.  Possible values:  <ul style="list-style-type: none"> <li>• <i>On Demand</i> (default value): The PPPoA is only set up on demand, e.g. for Internet access.</li> </ul> You'll find additional information on PPP over ATM under <a href="#">PPPoA</a> on page 317.

## 13.2.2 Service Categories

In the **WAN->ATM->Service Categories** menu is displayed a list of already configured ATM connections (PVC, Permanent Virtual Circuit) to which specific data traffic parameters were assigned.

Your device supports QoS (Quality of Service) for ATM interfaces.



### Caution

ATM QoS should only be used if your provider specifies a list of data traffic parameters (traffic contract).

The configuration of ATM QoS requires extensive knowledge of ATM technology and the way the bintec elmegbintec elmeg devices function. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

### 13.2.2.1 New

Choose the **New** button to create additional categories.

Fig. 131: WAN->ATM->Service Categories->New

The menu **WAN->ATM->Service Categories->New** consists of the following fields:

#### Fields in the Basic Parameters menu.

Field	Description
<b>Virtual Channel Connection (VCC)</b>	Select the already configured ATM connection (displayed by the combination of VPI and VCI) for which the service category is to be defined.
<b>ATM Service Category</b>	Select how the data traffic of the ATM connection is to be controlled. A priority is implicitly assigned when you select the ATM service category: from CBR (highest priority) through VBR.1 /VBR.3 to VBR (lowest priority).  Possible settings:

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Unspecified Bit Rate (UBR)</i> (default value): No specific data rate is guaranteed for the connection. The <b>Peak Cell Rate (PCR)</b> specifies the limit above which data is discarded. This category is suitable for non-critical applications.</li> <li>• <i>Constant Bit Rate (CBR)</i>: (Constant Bit Rate) The connection is assigned a guaranteed data rate determined by the <b>Peak Cell Rate (PCR)</b>. This category is suitable for critical (real-time) applications that require a guaranteed data rate.</li> <li>• <i>Variable Bit Rate V.1 (VBR.1)</i>: A guaranteed data rate is assigned to the connection - <b>Sustained Cell Rate (SCR)</b>. This may be exceeded by the volume configured in <b>Maximum Burst Size (MBS)</b>. Any additional ATM traffic is discarded. The <b>Peak Cell Rate (PCR)</b> constitutes the maximum possible data rate. This category is suitable for non-critical applications with burst data traffic.</li> <li>• <i>Variable Bit Rate V.3 (VBR.3)</i>: A guaranteed data rate is assigned to the connection - <b>Sustained Cell Rate (SCR)</b>. This may be exceeded by the volume configured in <b>Maximum Burst Size (MBS)</b>. Additional ATM traffic is marked and handled with low priority based on the utilisation of the destination network, i.e. is discarded if necessary. The <b>Peak Cell Rate (PCR)</b> constitutes the maximum possible data rate. This category is suitable for critical applications with burst data traffic.</li> </ul>
<b>Peak Cell Rate (PCR)</b>	<p>Enter a value for the maximum data rate in bits per second.</p> <p>Possible values: 0 to 10000000.</p> <p>The default value is 0.</p>
<b>Sustained Cell Rate (SCR)</b>	<p>Only for <b>ATM Service Category</b> = <i>Variable Bit Rate V.1 (VBR.1)</i> or <i>Variable Bit Rate V.3 (VBR.3)</i></p> <p>Enter a value for the minimum available, guaranteed data rate in bits per second.</p> <p>Possible values: 0 to 10000000.</p> <p>The default value is 0.</p>
<b>Maximum Burst Size (MBS)</b>	<p>Only for <b>ATM Service Category</b> = <i>Variable Bit Rate V.1 (VBR.1)</i> or <i>Variable Bit Rate V.3 (VBR.3)</i></p>



Field	Description
	<p>Enter a value for the maximum number of bits per second by which the PCR can be exceeded briefly.</p> <p>Possible values: 0 to 100000.</p> <p>The default value is 0.</p>

### 13.2.3 OAM Controlling

OAM is a service for monitoring ATM connections. A total of five hierarchies (flow level F1 to F5) are defined for OAM information flow. The most important information flows for an ATM connection are F4 and F5. The F4 information flow concerns the virtual path (VP) and the F5 information flow the virtual channel (VC). The VP is defined by the VPI value, the VC by VPI and VCI.



#### Note

Generally, monitoring is not carried out by the terminal but is initiated by the ISP. Your device then only needs to react correctly to the signals received. This is ensured without a specific OAM configuration for both flow level 4 and flow level 5.

Two mechanisms are available for monitoring the ATM connection: Loopback Tests and OAM Continuity Check (OAM CC). These can be configured independently of each other.



#### Caution

The configuration of OAM requires extensive knowledge of ATM technology and the way the bintec elmegbintec elmeg devices functions. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

In the **WAN->ATM->OAM Controlling** menu, a list of all monitored OAM flow levels is displayed.

#### 13.2.3.1 New

Choose the **New** button to set up monitoring for other flow levels.

[Profiles](#) | [Service Categories](#) | **OAM Controlling**

OAM Flow Configuration	
OAM Flow Level	F5
Virtual Channel Connection (VCC)	VPI1, VCI32
Loopback	
Loopback End-to-End	<input type="checkbox"/> Enabled
Loopback Segment	<input type="checkbox"/> Enabled
CC Activation	
Continuity Check (CC) End-to-End	Passive Direction Both
Continuity Check (CC) Segment	Passive Direction Both

Fig. 132: WAN->ATM->OAM Controlling->New

The menu **WAN->ATM->OAM Controlling->New** consists of the following fields:

#### Fields in the OAM Flow Configuration menu.

Field	Description
<b>OAM Flow Level</b>	<p>Select the OAM flow level to be monitored.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>F5</i>: (virtual channel level) The OAM settings are used for the virtual channel (default value).</li> <li>• <i>F4</i> : (virtual path level) The OAM settings are used on the virtual path.</li> </ul>
<b>Virtual Channel Connection (VCC)</b>	<p>Only for <b>OAM Flow Level</b> = <i>F5</i></p> <p>Select the already configured ATM connection to be monitored (displayed by the combination of VPI and VCI).</p>
<b>Virtual Path Connection (VPC)</b>	<p>Only for <b>OAM Flow Level</b> = <i>F4</i></p> <p>Select the already configured virtual path connection to be monitored (displayed by the VPI).</p>

#### Fields in the Loopback menu.

Field	Description
<b>Loopback End-to-End</b>	Select whether you activate the loopback test for the connection between the endpoints of the VCC or VPC.

Field	Description
	<p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>End-to-End Send Interval</b>	<p>Only if <b>Loopback End-to-End</b> is enabled.</p> <p>Enter the time in seconds after which a loopback cell is to be sent.</p> <p>Possible values are <i>0</i> to <i>999</i>.</p> <p>The default value is <i>5</i>.</p>
<b>End-to-End Pending Requests</b>	<p>Only if <b>Loopback End-to-End</b> is enabled.</p> <p>Enter the number of directly consecutive loopback cells that may fail to materialise before the connection is regarded as interrupted ("down"). Possible values are <i>1</i> to <i>99</i>.</p> <p>The default value is <i>5</i>.</p>
<b>Loopback Segment</b>	<p>Select whether you want to activate the loopback test for the segment connection (segment = connection of the local endpoint to the next connection point) of the VCC or VPC.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>Segment Send Interval</b>	<p>Only if <b>Loopback Segment</b> is enabled.</p> <p>Enter the time in seconds after which a loopback cell is sent.</p> <p>Possible values are <i>0</i> to <i>999</i>.</p> <p>The default value is <i>5</i>.</p>
<b>Segment Pending Requests</b>	<p>Only if <b>Loopback Segment</b> is enabled.</p> <p>Enter the number of directly consecutive loopback cells that may fail to materialise before the connection is regarded as interrupted ("down").</p> <p>Possible values are <i>1</i> to <i>99</i>.</p> <p>The default value is <i>5</i>.</p>

## Fields in the CC Activation menu.

Field	Description
<b>Continuity Check (CC) End-to-End</b>	<p>Select whether you activate the OAM-CC test for the connection between the endpoints of the VCC or VPC.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Passive</i> (default value): OAM CC requests are responded to after CC negotiation (CC activation negotiation).</li> <li>• <i>Active</i>: OAM CC requests are sent after CC negotiation (CC activation negotiation).</li> <li>• <i>Both</i>: OAM CC requests are sent and answered after CC negotiation (CC activation negotiation).</li> <li>• <i>No negotiation</i>: Depending on the setting in the <b>Direction</b> field, OAM CC requests are either sent and/or responded to. There is no CC negotiation.</li> <li>• <i>Passive</i>: The function is disabled.</li> </ul> <p>Also select whether the test cells of the OAM CC are to be sent or received.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Both</i> (default value): CC data is both received and generated.</li> <li>• <i>Sink</i>: CC data is received.</li> <li>• <i>Source</i>: CC data is generated.</li> </ul>
<b>Continuity Check (CC) Segment</b>	<p>Select whether you want to activate the OAM-CC test for the segment connection (segment = connection of the local endpoint to the next connection point) of the VCC or VPC.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Passive</i> (default value): OAM CC requests are responded to after CC negotiation (CC activation negotiation).</li> <li>• <i>Active</i>: OAM CC requests are sent after CC negotiation (CC activation negotiation).</li> <li>• <i>Both</i>: OAM CC requests are sent and answered after CC negotiation (CC activation negotiation).</li> <li>• <i>No negotiation</i>: Depending on the setting in the <b>Direction</b> field, OAM CC requests are either sent and/or responded to.</li> </ul>

Field	Description
	<p>There is no CC negotiation.</p> <ul style="list-style-type: none"> <li>• <i>None</i>: The function is disabled.</li> </ul> <p>Also select whether the test cells of the OAM CC are to be sent or received.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> <li>• <i>Both</i> (default value): CC data is both received and generated.</li> <li>• <i>Sink</i>: CC data is received.</li> <li>• <i>Source</i>: CC data is generated.</li> </ul>

## 13.3 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.

### 13.3.1 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.

#### 13.3.1.1 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	<input style="width: 80%;" type="text" value="0"/> kbps

Fig. 133: 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
<b>Interface</b>	Define for which interfaces voice transmission is to be optimised.
<b>Control Mode</b>	Select the mode for the optimisation.  Possible values: <ul style="list-style-type: none"> <li>• <i>Controlled RTP Streams only</i> (default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission.</li> <li>• <i>All RTP Streams</i>: All RTP streams are optimised.</li> <li>• <i>Inactive</i>: Voice data transmission is not optimised.</li> <li>• <i>Always</i>: Voice data transmission is always optimised.</li> </ul>
<b>Maximum Upload Speed</b>	Enter the maximum available upstream bandwidth in kbp/s for the selected interface.

## Chapter 14 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.

### 14.1 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 99). 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 IPv4 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 IPv4 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 IPv4 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 IPv4 Traffic Filter**, it is rejected.

If an IP packet meets the requirements in an **Additional IPv4 Traffic Filter**, IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

**Note**

The parameter **Additional IPv4 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.

### 14.1.1 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 sorted by priority displayed in the **VPN->IPSec->IPSec Peers** menu.



[IPSec Peers](#)
[Phase-1 Profiles](#)
[Phase-2 Profiles](#)
[XAUTH Profiles](#)
[IP Pools](#)
[Options](#)

Internet Key Exchange Version 1 (IKEv1)

View  per page << >> Filter in None equal Go

Prio	Description	Peer Address	Peer ID	Phase-1 Profile	Phase-2 Profile	Status	Action

Page: 1

Internet Key Exchange Version 2 (IKEv2)

View  per page << >> Filter in None equal Go


Prio	Description	Peer Address	Peer ID	Phase-1 Profile	Phase-2 Profile	Status	Action

Page: 1

New

Fig. 134: 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 567.

### 14.1.1.1 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	<input checked="" type="radio"/> Up <input type="radio"/> Down															
Description	<input type="text" value="Peer-1"/>															
Peer Address	IP Version <input type="text" value="IPv4 Preferred"/> <input type="text"/>															
Peer ID	Fully Qualified Domain Name (FQDN) <input type="text" value="Peer-1."/>															
Internet Key Exchange	<input type="text" value="IKEv1"/>															
IP Version of the tunneled Networks	<input type="text" value="IPv4"/>															
IPv4 Interface Routes																
Security Policy	<input type="radio"/> Untrusted <input checked="" type="radio"/> Trusted															
IPv4 Address Assignment	<input type="text" value="Static"/>															
Default Route	<input type="checkbox"/> Enabled															
Local IP Address	<input type="text"/>															
Route Entries	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Remote IP Address</th> <th style="width: 20%;">Netmask</th> <th style="width: 10%;">Metric</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text" value="1"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Remote IP Address	Netmask	Metric		<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="button" value="Add"/>						
Remote IP Address	Netmask	Metric														
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>													
<input type="button" value="Add"/>																
Additional IPv4 Traffic Filter																
Additional IPv4 Traffic Filter	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">Description</th> <th style="width: 10%;">Protocol</th> <th style="width: 20%;">Src. IP/Mask:Port</th> <th style="width: 20%;">Dest. IP/Mask:Port</th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="5" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Description	Protocol	Src. IP/Mask:Port	Dest. IP/Mask:Port		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>				
Description	Protocol	Src. IP/Mask:Port	Dest. IP/Mask:Port													
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>												
<input type="button" value="Add"/>																


Advanced Settings

Advanced IPSec Options	
Phase-1 Profile	<input type="text" value="None (use default profile)"/>
Phase-2 Profile	<input type="text" value="None (use default profile)"/>
XAUTH Profile	<input type="text" value="Select one"/>
Number of Admitted Connections	<input checked="" type="radio"/> One User <input type="radio"/> Multiple Users
Start Mode	<input checked="" type="radio"/> On Demand <input type="radio"/> Always up
Advanced IP Options	
Public Interface	<input type="text" value="Chosen by Routing"/>
Public Source IPv4 Address	<input type="checkbox"/> Enabled
IPv4 Back Route Verify	<input type="checkbox"/> Enabled
IPv4 Proxy ARP	<input checked="" type="radio"/> Inactive <input type="radio"/> Up or Dormant <input type="radio"/> Up only
IPv4 IPSec Callback	
Mode	<input type="text" value="Inactive"/>

Fig. 135: 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
<b>Administrative Status</b>	<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"> <li>• <i>Up</i> (default value): The peer is available for setting up a tunnel immediately after saving the configuration.</li> <li>• <i>Down</i>: The peer is initially not available after the configuration has been saved.</li> </ul>
<b>Description</b>	<p>Enter a description of the peer that identifies it.</p> <p>The maximum length of the entry is 255 characters.</p>
<b>Peer Address</b>	<p>Select the <b>IP Version</b>. You can choose if IPv4 or IPv6 is to be preferred or if only one IP version is to be permitted.</p> <div data-bbox="539 777 1316 935" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p> <b>Note</b></p> <p>This selection is only relevant if an IP address is entered as host name.</p> </div> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>IPv4 Preferred</i></li> <li>• <i>IPv6 Preferred</i></li> <li>• <i>IPv4 Only</i></li> <li>• <i>IPv6 Only</i></li> </ul> <p>Enter the public IP address of the peer or a resolvable host name.</p> <p>This entry can be omitted in certain configurations, but in that case your device cannot initiate an IPSec connection.</p>
<b>Peer ID</b>	<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>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Fully Qualified Domain Name (FQDN)</i>: Any string</li> <li>• <i>E-mail Address</i></li> <li>• <i>IPV4 Address</i></li> <li>• <i>ASN.1-DN (Distinguished Name)</i></li> <li>• <i>Key ID</i>: Any string</li> </ul> <p>On the peer device, this ID corresponds to the <b>Local ID Value</b>.</p>
<b>Internet Key Exchange</b>	<p>Select the version of the Internet Exchange Protocol to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>IKEv1</i> (default value): Internet Key Exchange Protocol Version 1</li> <li>• <i>IKEv2</i>: Internet Kex Exchange Protocol Version 2</li> </ul>
<b>Authentication Method</b>	<p>Only for <b>Internet Key Exchange = IKEv2</b></p> <p>Select the authentication method.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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 <b>IPSec Peers</b>. The preshared key is the shared password.</li> <li>• <i>RSA Signature</i>: Phase 1 key calculations are authenticated using the RSA algorithm.</li> </ul>
<b>Local ID Type</b>	<p>Only for <b>Internet Key Exchange = IKEv2</b></p> <p>Select the local ID type.</p> <p>Possible ID types:</p> <ul style="list-style-type: none"> <li>• <i>Fully Qualified Domain Name (FQDN)</i></li> <li>• <i>E-mail Address</i></li> <li>• <i>IPV4 Address</i></li> <li>• <i>ASN.1-DN (Distinguished Name)</i></li> <li>• <i>Key ID</i>: Any string</li> </ul>
<b>Local ID</b>	<p>Only for <b>Internet Key Exchange = IKEv2</b></p>

Field	Description
	<p>Enter the ID of your device.</p> <p>For <b>Authentication Method</b> = <i>DSA Signature</i> or <i>RSA Signature</i> the option <b>Use Subject Name from certificate</b> is displayed.</p> <p>When you enable the option <b>Use Subject Name from certificate</b>, 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 <a href="#">Certificates</a> on page 99), 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>
<b>Preshared Key</b>	<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>
<b>IP Version of the tunneled Networks</b>	<p>Select if IPv4, IPv6 or both versions are allowed for the VPN tunnel.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>IPv4</i></li> <li>• <i>IPv6</i></li> <li>• <i>IPv4 and IPv6</i></li> </ul>

**Fields in the menu IPv4 Interface Routes (appears only for IP Version of the tunneled Networks = IPv4 or IPv4 and IPv6)**

Field	Description
<b>Security Policy</b>	<p>Select the security settings to be used with the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i>: All IP packets are allowed through except for those which are explicitly prohibited.</li> <li>• <i>Untrusted</i> (default value): Only those packets are transmit-</li> </ul>

Field	Description
	<p>ted that can be attributed to a connection that has been initiated from a trusted zone.</p> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>
<b>IP Address Assignment</b>	<p>Select the configuration mode of the interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Static</i> (default value): Enter a static IP address.</li> <li>• <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.</li> <li>• <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 <b>IP Assignment Pool</b>.</li> </ul>
<b>Config Mode</b>	<p>Only where <b>IP Address Assignment</b> = <i>IKE Config Mode Server</i> or <i>IKE Config Mode Client</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Pull</i> (default value): The client requests the IP address and the gateway answers the request.</li> <li>• <i>Push</i>: The gateway suggests an IP address to the client and the client must either accept or reject this.</li> </ul> <p>This value must be identical for both sides of the tunnel.</p>
<b>IP Assignment Pool</b>	<p>Only if <b>IP Address Assignment</b> = <i>IKE Config Mode Server</i></p> <p>Select an IP pool configured in the <b>VPN-&gt;IPSec-&gt;IP Pools</b> menu. If an IP pool has not been configured here yet, the message <i>Not yet defined</i> appears in this field.</p>
<b>Default Route</b>	<p>Only for <b>IP Address Assignment</b> = <i>Static</i> or <i>IKE Config 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>

Field	Description
	The function is disabled by default.
<b>Local IP Address</b>	<p>Only for <b>IP Address Assignment</b> = <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>
<b>Metric</b>	<p>Only for <b>IP Address Assignment</b> = <i>Static</i> or <i>IKE Config Mode Client</i> and <b>Default Route</b> = <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 0 to 15. The default value is 1.</p>
<b>Route Entries</b>	<p>Only for <b>IP Address Assignment</b> = <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"> <li>• <i>Remote IP Address</i>: IP address of the destination host or LAN.</li> <li>• <i>Netmask</i>: Netmask for <i>Remote IP Address</i>.</li> <li>• <i>Metric</i>: The lower the value, the higher the priority of the route (possible values 0..15). The default value is 1.</li> </ul>

**Fields in the menu Additional IPv4 Traffic Filter (appears only for IP Version of the tunneled Networks = IPv4 or IPv4 and IPv6)**

Field	Description
<b>Additional IPv4 Traffic Filter</b>	<p>Only for <b>Internet Key Exchange</b> = <i>IKEv1</i></p> <p>Use <b>Add</b> to create a new filter.</p>

**Fields in the IPv6 Interface Routes menu (appears only for IP Version of the tunneled Networks = IPv6 or IPv4 and IPv6)**

Field	Description
<b>Security Policy</b>	Select the security settings to be used with the interface..

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Untrusted</i>: IP packets are only allowed through if the connection has been initiated from "inside".</li> </ul> <p>We recommend you use this setting if you want to use IPv6 outside of your LAN.</p> <ul style="list-style-type: none"> <li>• <i>Trusted</i> (default value): All IP packets are allowed through except for those which are explicitly prohibited.</li> </ul> <p>We recommend you use this setting if you want to use IPv6 on your LAN.</p> <p>You can configure exceptions for the selected setting in the <a href="#">Firewall</a> on page 415 menu.</p>
<b>Local IPv6 Network</b>	<p>Select a network. You can choose from the Link Prefixes available under <b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt;New</b>.</p> <p>Enter the Local IPv6 address and the corresponding prefix length. The default prefix length is /64. This prefix must end with ::.</p>
<b>Remote IPv6 Network</b>	<p>Add a new prefix. Enter the address of the other tunnel endpoint. The default prefix <b>Length</b> is 64 and the default <b>Priority</b> is 1. The lower the value entered for <b>Priority</b>, the higher the priority of the route.</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 IPv4 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 IPv4 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 IPv4 Traffic Filter** it is discarded.

If an IP packet meets the requirements in an **Additional IPv4 Traffic Filter** , IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

**Note**

The parameter **Additional IPv4 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**.

The screenshot shows the 'IPsec Peers' configuration page with a modal dialog box open for adding a new peer. The dialog box is titled 'Basic Parameters' and contains the following fields:

- Description:** A text input field.
- Protocol:** A dropdown menu currently set to 'Any'.
- Source IP Address/Netmask:** A dropdown menu set to 'Network' followed by two input fields for IP address and netmask.
- Destination IP Address/Netmask:** A dropdown menu set to 'Network' followed by two input fields for IP address and netmask.

At the bottom of the dialog box are 'Apply' and 'Cancel' buttons. The background configuration page shows 'Peer Parameters' with 'Administrative Status' set to 'Up', 'Description' set to 'Peer-1', and 'Metric' set to '1'.

Fig. 136: VPN->IPsec->IPsec Peers->New->Add

#### Fields in the menu Basic Parameters

Field	Description
<b>Description</b>	Enter a description for the filter.
<b>Protocol</b>	Select a protocol. The <i>Any</i> option (default value) matches all protocols.
<b>Source IP Address/ Netmask</b>	Enter, if required, the source IP address and netmask of the data packets.  Possible values: <ul style="list-style-type: none"> <li>• <i>Any</i></li> <li>• <i>Host</i>: Enter the IP address of the host.</li> <li>• <i>Network</i> (default value): Enter the network address and the related netmask.</li> </ul>
<b>Source Port</b>	Only for <b>Protocol</b> = <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.
<b>Destination IP Address/Netmask</b>	Enter the destination IP address and corresponding netmask of the data packets.
<b>Destination Port</b>	Only for <b>Protocol</b> = <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
<b>Phase-1 Profile</b>	Select a profile for Phase 1. Besides user-defined profiles, pre-defined profiles are available.  Possible values: <ul style="list-style-type: none"> <li>• <i>None (use default profile)</i>: Uses the profile marked as standard in <b>VPN-&gt;IPsec-&gt;Phase-1 Profiles</b></li> <li>• <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 <b>VPN-&gt;IPsec-&gt;Phase-1 Profiles</b>.</li> <li>• <i>&lt;Profilname&gt;</i>: Uses a profile configured in menu <b>VPN-&gt;IPsec-&gt;Phase-1 Profiles</b> for Phase 1.</li> </ul>
<b>Phase-2 Profile</b>	Select a profile for Phase 2. Besides user-defined profiles, pre-defined profiles are available.  Possible values: <ul style="list-style-type: none"> <li>• <i>None (use default profile)</i>: Uses the profile marked as standard in <b>VPN-&gt;IPsec-&gt;Phase-2 Profiles</b></li> <li>• <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 <b>VPN-&gt;IPsec-&gt;Phase-2 Profiles</b>.</li> <li>• <i>&lt;Profilname&gt;</i>: Uses a profile configured in menu <b>VPN-&gt;IPsec-&gt;Phase-2 Profiles</b> for Phase 2.</li> </ul>

Field	Description
<b>XAUTH Profile</b>	<p>Select a profile created in <b>VPN-&gt;IPSec-&gt;XAUTH Profiles</b> 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>
<b>Number of Admitted Connections</b>	<p>Choose how many users can connect using this peer profile.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>One User</i> (default value): Only one peer can be connected with the data defined in this profile.</li> <li>• <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.</li> </ul> <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>
<b>Start Mode</b>	<p>Select how the peer is to be switched to the active state.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>On Demand</i> (default value): The peer is switched to the active state by a trigger.</li> <li>• <i>Always up</i>: The peer is always active.</li> </ul>

#### Fields in the menu **Advanced IP Options**

Field	Description
<b>Public Interface</b>	<p>Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select <i>Chosen 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 <b>Public Interface Mode</b> .
<b>Public Interface Mode</b>	<p>Only when an interface is selected for <b>Public Interface</b>.</p> <p>Specify how strictly the setting is handled.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Force</i>: Only the selected interface is used, independently from the priorities in the current routing table.</li> <li>• <i>Preferred</i>: The priorities in the current routing table will be used. Only if several equivalent routes are available, the route via the selected interface will be applied.</li> </ul>
<b>Public Source IPv4 Address</b>	<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 <b>Public Source IPv4 Address</b> 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>
<b>IPv4 Back Route Verify</b>	<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>
<b>MobiKE</b>	<p>Only for peers with IKEv2.</p> <p><b>MobiKE</b> 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>
<b>IPv4 Proxy ARP</b>	Select whether your device is to respond to ARP requests from

Field	Description
	<p>its own LAN on behalf of the specific connection partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Inactive</i> (default value): Deactivates Proxy ARP for this IPsec peer.</li> <li>• <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.</li> <li>• <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.</li> </ul>

### 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](http://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 IPv4 IPsec Callback* on page 368. 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 IPv4 IPSec Callback**



Field	Description
<b>Mode</b>	<p>Select the Callback Mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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).</li> </ul>
<b>Incoming Phone Number</b>	<p>Only for <b>Mode</b> = <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>
<b>Outgoing Phone Number</b>	<p>Only for <b>Mode</b> = <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>
<b>Transfer own IP address over ISDN/GSM</b>	<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>
<b>Transfer Mode</b>	<p>Only for <b>Transfer own IP address over ISDN/GSM</b> = 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"> <li>• <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.)</li> <li>• <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.</li> <li>• <i>Use specific D Channel Mode</i>: Your device tries to transfer the IP address in the mode set in the <b>Mode</b> field.</li> <li>• <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 <b>Mode</b> field. If this does not succeed, the IP address is transferred in the B channel. (This incurs costs.)</li> <li>• <i>Use only B Channel Mode</i>: Your device transfers the IP address in the B channel. This incurs costs.</li> </ul>
<b>D Channel Mode</b>	<p>Only for <b>Transfer Mode</b> = <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"> <li>• <i>LLC</i> (default value): The IP address is transferred in the "LLC information elements" of the D channel.</li> <li>• <i>SUBADDR</i>: The IP address is transferred in the subaddress "information elements" of the D channel.</li> <li>• <i>LLC and SUBADDR</i>: The IP address is transferred in both the "LLC" and "subaddress information elements".</li> </ul>

### 14.1.2 Phase-1 Profiles

A list of all configured tunnel profiles is displayed in the **VPN->IPSec->Phase-1 Profiles** menu.

**IPSec Peers**   **Phase-1 Profiles**   **Phase-2 Profiles**   **XAUTH Profiles**   **IP Pools**   **Options**

---

Internet Key Exchange Version 1 (IKEv1)

View 20 per page << >> Filter in None equal Go

Default	Description	Proposals	Authentication	Mode	DH Group	Lifetime

Page: 1

Create new IKEv1 Profile   **New**

---

Internet Key Exchange Version 2 (IKEv2)

View 20 per page << >> Filter in None equal Go

Default	Description	Proposals	Lifetime

Page: 1

Create new IKEv2 Profile   **New**

**OK**   **Cancel**

Fig. 137: VPN->IPSec->Phase-1 Profiles

In the **Default** column, you can mark the profile to be used as the default profile.

#### 14.1.2.1 New

Choose the **New** (at **Create new IKEv1 Profile** or **Create new IKEv2 Profile**) button to create additional profiles.

IPSec Peers
Phase-1 Profiles
Phase-2 Profiles
XAUTH Profiles
IP Pools
Options

Phase-1 (IKE) Parameters													
Description	IKE-1												
Proposals	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Encryption</th> <th style="width: 30%;">Authentication</th> <th style="width: 40%;">Enabled</th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Encryption	Authentication	Enabled	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>
Encryption	Authentication	Enabled											
AES	MD5	<input type="checkbox"/>											
AES	MD5	<input type="checkbox"/>											
AES	MD5	<input type="checkbox"/>											
DH Group	<input type="radio"/> 1(768 Bit) <input checked="" type="radio"/> 2(1024 Bit) <input type="radio"/> 5(1536 Bit)												
Lifetime	14400 Seconds 0 kBytes												
Authentication Method	Preshared Keys												
Mode	<input type="radio"/> Main Mode (ID Protect) <input checked="" type="radio"/> Aggressive <input type="checkbox"/> Strict												
Local ID Type	Fully Qualified Domain Name (FQDN)												
Local ID Value	r4402												

Advanced Settings

Alive Check	Autodetect
Block Time	30 Seconds
NAT Traversal	Enabled

Fig. 138: 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
<b>Description</b>	Enter a description that uniquely defines the type of rule.
<b>Proposals</b>	<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 cannot be deactivated.</p> <p>Encryption algorithms (<b>Encryption</b>):</p> <ul style="list-style-type: none"> <li><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.</li> <li><i>Twofish</i>: Twofish was a final candidate for the AES</li> </ul>

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"> <li>• <i>Blowfish</i>: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish.</li> <li>• <i>CAST</i>: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES.</li> <li>• <i>DES</i>: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> </ul> <p>Hash algorithms (<b>Authentication</b>):</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <i>RipeMD 160</i>: RipeMD 160 is a 160 bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD.</li> <li>• <i>Tiger192</i>: Tiger 192 is a relatively new and very fast algorithm.</li> <li>• <i>SHA2-256</i>: SH2 (Secure Hash Algorithmus #2) is a hash algorithm which has been designed to supersede SHA 1. It can</li> </ul>

Field	Description
	<p>be used with hash lengths of 256, 384 or 512 bits.</p> <ul style="list-style-type: none"> <li>• <i>SHA2-384</i>: SHA-2 with 384 bit hash length.</li> <li>• <i>SHA2-512</i>: SHA-2 with 512 bit hash length.</li> </ul> <p>Depending on the hardware of your device some options may not be available.</p> <p>Please note that the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.</p>
<b>DH Group</b>	<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>The following groups with their corresponding bit values are available:</p> <ul style="list-style-type: none"> <li>• <i>1 (768 Bit)</i></li> <li>• <i>2 (1024 Bit)</i></li> <li>• <i>5 (1536 Bit)</i></li> <li>• <i>14 (2048 Bit)</i></li> <li>• <i>15 (3072 Bit)</i></li> <li>• <i>16 (4096 Bit)</i></li> </ul> <p>Depending on the hardware of your device some options may not be available.</p>
<b>Lifetime</b>	<p>Create a lifetime for phase 1 keys.</p> <p>The following options are available for defining the <b>Lifetime</b>:</p> <ul style="list-style-type: none"> <li>• Input in <b>Seconds</b>: 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.</li> <li>• Input in <b>kBytes</b>: 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.</li> </ul>

Field	Description
<b>Authentication Method</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></p> <p>Select the authentication method.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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 <b>VPN-&gt;IPSec-&gt;IPSec Peers</b>. The preshared key is the shared password.</li> <li>• <i>DSA Signature</i>: Phase 1 key calculations are authenticated using the DSA algorithm.</li> <li>• <i>RSA Signature</i>: Phase 1 key calculations are authenticated using the RSA algorithm.</li> <li>• <i>RSA Encryption</i>: In RSA encryption the ID payload is also encrypted for additional security.</li> </ul>
<b>Local Certificate</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></p> <p>Only for <b>Authentication Method = DSA Signature, RSA Signature or RSA Encryption</b></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>
<b>Mode</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></p> <p>Select the phase 1 mode.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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</li> </ul>

Field	Description
	<p>both peers have static IP addresses if preshared keys are used for authentication.</p> <p>Also define whether the selected mode is used exclusively (<b>Strict</b>), or the peer can also propose another mode.</p>
<b>Local ID Type</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></p> <p>Select the local ID type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Fully Qualified Domain Name (FQDN)</i></li> <li>• <i>E-mail Address</i></li> <li>• <i>IPV4 Address</i></li> <li>• <i>ASN.1-DN (Distinguished Name)</i></li> </ul>
<b>Local ID Value</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></p> <p>Enter the ID of your device.</p> <p>For <b>Authentication Method</b> = <i>DSA Signature, RSA Signature</i> or <i>RSA Encryption</i> the <b>Use Subject Name from certificate</b> option is displayed.</p> <p>When you enable the <b>Use Subject Name from certificate</b> 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 <a href="#">Certificates</a> on page 99), 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
<b>Alive Check</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></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"> <li>• <i>Autodetect</i> (default value): Your device detects and uses the mode supported by the remote terminal.</li> <li>• <i>Inactive</i>: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers.</li> <li>• <i>Heartbeats (Expect only)</i>: Your device expects a heartbeat from the peer but does not send one itself.</li> <li>• <i>Heartbeats (Send only)</i>: Your device expects no heartbeat from the peer, but sends one itself.</li> <li>• <i>Heartbeats (Send &amp;Expect)</i>: Your device expects a heartbeat from the peer and sends one itself.</li> <li>• <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.</li> <li>• <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.</li> </ul> <p>Only for <b>Phase-1 (IKEv2) Parameters</b></p>

Field	Description
	<p>Enable or disable alive check.</p> <p>The function is enabled by default.</p>
<b>Block Time</b>	<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>
<b>NAT Traversal</b>	<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"> <li>• <i>Enabled</i> (default value): NAT Traversal is enabled.</li> <li>• <i>Disabled</i>: NAT Traversal is disabled.</li> <li>• <i>Force</i>: The device always behaves as it would if NAT were in use.</li> </ul> <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>
<b>CA Certificates</b>	<p>Only for <b>Phase-1 (IKE) Parameters</b></p> <p>Only for <b>Authentication Method</b> = <i>DSA Signature, RSA Signature</i> or <i>RSA Encryption</i></p>

Field	Description
	<p>If you enable the <b>Trust the following CA certificates</b> option, you can select up to three CA certificates that are accepted for this profile.</p> <p>This option can only be configured if certificates are loaded.</p>

### 14.1.3 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.

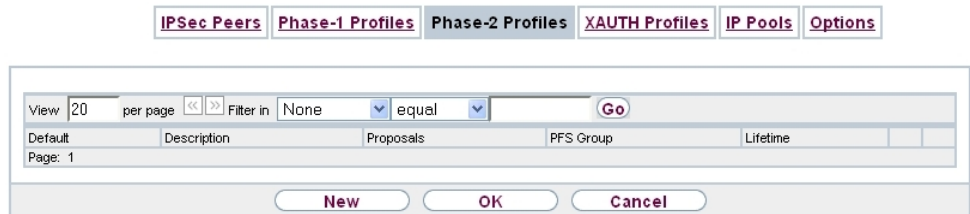


Fig. 139: **VPN->IPSec->Phase-2 Profiles**

In the **Default** column, you can mark the profile to be used as the default profile.

#### 14.1.3.1 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	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Encryption</th> <th style="width: 30%;">Authentication</th> <th style="width: 40%;">Enabled</th> </tr> </thead> <tbody> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> <tr> <td>AES</td> <td>MD5</td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Encryption	Authentication	Enabled	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>	AES	MD5	<input type="checkbox"/>
Encryption	Authentication	Enabled											
AES	MD5	<input type="checkbox"/>											
AES	MD5	<input type="checkbox"/>											
AES	MD5	<input type="checkbox"/>											
Use PFS Group	<input checked="" type="checkbox"/> Enabled <input type="radio"/> 1(768 Bit) <input checked="" type="radio"/> 2(1024 Bit) <input type="radio"/> 5(1536 Bit)												
Lifetime	7200 Seconds 0 kBytes Rekey after 80 % Lifetime												

**Advanced Settings**

IP Compression	<input type="checkbox"/> Enabled
Alive Check	Autodetect
Propagate PMTU	<input checked="" type="checkbox"/> Enabled

Fig. 140: 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
<b>Description</b>	Enter a description that uniquely identifies the profile.  The maximum length of the entry is 255 characters.
<b>Proposals</b>	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.  <b>Encryption algorithms (Encryption):</b> <ul style="list-style-type: none"> <li>• <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.</li> <li>• -- <i>ALL</i> --: All options can be used.</li> <li>• <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</li> </ul>

Field	Description
	<p><i>AES</i> , a key length of 128 bits is used.</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <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.</li> <li>• <i>Blowfish</i>: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish.</li> <li>• <i>CAST</i>: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES.</li> <li>• <i>DES</i>: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits.</li> </ul> <p>Hash algorithms (<b>Authentication</b>):</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>-- ALL --</i>: All options can be used.</li> <li>• <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.</li> <li>• <i>SHA2-256</i>: SH2 (Secure Hash Algorithmus #2) is a hash algorithm which has been designed to supersede SHA 1. It can be used with hash lengths of 256, 384 or 512 bits.</li> <li>• <i>SHA2-384</i>: SHA-2 with 384 bit hash length.</li> <li>• <i>SHA2-512</i>: SHA-2 with 512 bit hash length.</li> </ul> <p>Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2.</p>

Field	Description
	Depending on the hardware of your device some options may not be available.
<b>Use PFS Group</b>	<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 <b>DH Group</b> in the <b>VPN-&gt;IPSec-&gt;Phase-1 Profiles</b> menu. PFS is 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 following groups with their corresponding bit values are available:</p> <ul style="list-style-type: none"> <li>• 1 (768 Bit)</li> <li>• 2 (1024 Bit)</li> <li>• 5 (1536 Bit)</li> <li>• 14 (2048 Bit)</li> <li>• 15 (3072 Bit)</li> <li>• 16 (4096 Bit)</li> </ul> <p>Depending on the hardware of your device some options may not be available.</p>
<b>Lifetime</b>	<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 <b>Lifetime</b>:</p> <ul style="list-style-type: none"> <li>• Input in <b>Seconds</b>: 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.</li> <li>• Input in <b>kBytes</b>: 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.</li> </ul> <p><b>Rekey after</b>: Specify the percentage in the course of the lifetime</p>

Field	Description
	<p>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
<b>IP Compression</b>	<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>
<b>Alive Check</b>	<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"> <li>• <i>Autodetect</i> (default value): Automatic detection of whether the remote terminal is a bintec elmeg device. If it is, <i>Heartbeats (Send &amp; Expect)</i> (for a remote terminal with bintec elmeg) or <i>Inactive</i> (for a remote terminal without bintec elmeg) is set.</li> <li>• <i>Inactive</i>: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers.</li> <li>• <i>Heartbeats (Expect only)</i>: Your device expects a heartbeat from the peer but does not send one itself.</li> <li>• <i>Heartbeats (Send only)</i>: Your device expects no heart-</li> </ul>

Field	Description
	<p>beat from the peer, but sends one itself.</p> <ul style="list-style-type: none"> <li>• <i>Heartbeats (Send &amp;Expect)</i>: Your device expects a heartbeat from the peer and sends one itself.</li> </ul>
<b>Propagate PMTU</b>	<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>

## 14.1.4 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.

### 14.1.4.1 New

Choose the **New** button to create additional profiles.



[IPSec Peers](#) | [Phase-1 Profiles](#) | [Phase-2 Profiles](#) | [XAUTH Profiles](#) | [IP Pools](#) | [Options](#)

Basic Parameters	
Description	<input type="text"/>
Role	Server
Mode	radius
RADIUS Server Group ID	No Radius Server configured for XAUTH

|

Fig. 141: 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
<b>Description</b>	Enter a description for this XAuth profile.
<b>Role</b>	<p>Select the role of the gateway for XAuth authentication.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>Server</i> (default value): The gateway requires a proof of authorisation.</li> <li><i>Client</i>: The gateway provides proof of authorisation.</li> </ul>
<b>Mode</b>	<p>Only for <b>Role</b> = <i>Server</i></p> <p>Select how authentication is carried out.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>RADIUS</i> (default value): Authentication is carried out via a Radius server. It is configured in the <b>System Management-&gt;Remote Authentication-&gt;RADIUS</b> menu and selected in the <b>RADIUS Server Group ID</b> field.</li> <li><i>Local</i>: Authentication is carried out via a local list.</li> </ul>
<b>Name</b>	<p>Only for <b>Role</b> = <i>Client</i></p> <p>Enter the authentication name of the client.</p>
<b>Password</b>	<p>Only for <b>Role</b> = <i>Client</i></p>


Field	Description
	Enter the authentication password.
<b>RADIUS Server Group ID</b>	Only for <b>Role</b> = <i>Server</i> Select the desired list in <b>System Management-&gt;Remote Authentication-&gt;RADIUS</b> configured RADIUS group.
<b>Users</b>	Only for <b>Role</b> = <i>Server</i> and <b>Mode</b> = <i>Local</i> 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 entering the authentication name of the client ( <b>Name</b> ) and the authentication password ( <b>Password</b> ). Add new members with <b>Add</b> .

## 14.1.5 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.

### 14.1.5.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

IPSec Peers
Phase-1 Profiles
Phase-2 Profiles
XAUTH Profiles
IP Pools
Options

Basic Parameters	
IP Pool Name	<input style="width: 95%;" type="text"/>
IP Address Range	<input style="width: 95%;" type="text"/> - <input style="width: 95%;" type="text"/>
DNS Server	Primary <input style="width: 95%;" type="text"/>
	Secondary <input style="width: 95%;" type="text"/>

Fig. 142: VPN->IPSec->IP Pools->New

### Fields in the menu **Basic Parameters**

Field	Description
<b>IP Pool Name</b>	Enter any description to uniquely identify the IP pool.
<b>IP Address Range</b>	Enter the first (first field) and last (second field) IP address of the IP address pool.
<b>DNS Server</b>	<p><b>Primary:</b> Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p><b>Secondary:</b> Optionally, enter the IP address of an alternative DNS server.</p>

## 14.1.6 Options


IPSec Peers | Phase-1 Profiles | Phase-2 Profiles | XAUTH Profiles | IP Pools | **Options**

Global Options	
Enable IPSec	<input type="checkbox"/> Enabled
Delete complete IPSec configuration	<input type="button" value="🗑"/>
IPSec Debug Level	Debug <input type="button" value="v"/>
Advanced Settings	
IPSec over TCP	<input type="checkbox"/> <b>NCP Path Finder Technology</b>
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
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 143: VPN->IPSec->Options

The menu **VPN->IPSec->Options** consists of the following fields:

### Fields in the **Global Options** menu.

Field	Description
<b>Enable IPsec</b>	<p>Select whether you want to activate IPsec.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is active as soon as an IPsec Peer is configured.</p>
<b>Delete complete IPsec configuration</b>	<p>If you click the  icon, delete the complete IPsec configuration of your device.</p> <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 <b>Enable IPsec</b> = not activated.</p>
<b>IPsec Debug Level</b>	<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"> <li>• <i>Emergency</i> (highest priority)</li> <li>• <i>Alert</i></li> <li>• <i>Critical</i></li> <li>• <i>Error</i></li> <li>• <i>Warning</i></li> <li>• <i>Notice</i></li> <li>• <i>Information</i></li> <li>• <i>Debug</i> (default value, lowest priority)</li> </ul> <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
<b>IPSec over TCP</b>	<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> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>Send Initial Contact Message</b>	<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>
<b>Sync SAs with ISP interface state</b>	<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>
<b>Use Zero Cookies</b>	<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>
<b>Zero Cookie Size</b>	<p>Only for <b>Use Zero Cookies</b> = 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>
<b>Dynamic RADIUS Au-</b>	<p>Select whether RADIUS authentication is to be activated via</p>

Field	Description
<b>thentication</b>	IPSec.  The function is enabled with <i>Enabled</i> .  The function is disabled by default.

#### Fields in the PKI Handling Options menu.

Field	Description
<b>Ignore Certificate Request Payloads</b>	Select whether certificate requests received from the remote end during IKE (phase 1) are to be ignored.  The function is enabled with <i>Enabled</i> .  The function is disabled by default.
<b>Send Certificate Request Payloads</b>	Select whether certificate requests are to be sent during IKE (phase 1).  The function is enabled with <i>Enabled</i> .  The function is enabled by default.
<b>Send Certificate Chains</b>	Select whether complete certificate chains are to be sent during IKE (phase 1).  The function is enabled with <i>Enabled</i> .  The function is enabled by default.  Deactivate this function if you do not wish to send the peer the certificates of all levels (from your level to the CA level).
<b>Send CRLs</b>	Select whether CRLs are to be sent during IKE (phase 1).  The function is enabled with <i>Enabled</i> .  The function is disabled by default.
<b>Send Key Hash Payloads</b>	Select whether key hash payloads are to be sent during IKE (phase 1).  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 sup-

Field	Description
	press this behaviour.

## 14.2 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.

### 14.2.1 Tunnel Profiles

A list of all configured tunnel profiles is displayed in the **VPN->L2TP->Tunnel Profiles** menu.

#### 14.2.1.1 New

Choose the **New** button to create additional tunnel profiles.

Tunnel Profiles Users Options

Basic Parameters	
Description	L2TP1
Local Hostname	
Remote Hostname	
Password	••••••••
LAC Mode Parameters	
Remote IP Address	
UDP Source Port	<input type="checkbox"/> 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	<input type="checkbox"/> Enabled

OK Cancel

Fig. 144: 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
<b>Description</b>	<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>
<b>Local Hostname</b>	<p>Enter the host name for LNS or LAC.</p> <ul style="list-style-type: none"> <li><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.</li> <li><i>LNS</i>: Is the same as the value for <b>Remote Hostname</b> of the</li> </ul>



Field	Description
	incoming tunnel setup message from the LAC.
<b>Remote Hostname</b>	<p>Enter the host name of the LNS or LAC.</p> <ul style="list-style-type: none"> <li>• <i>LAC</i>: Defines the value for <b>Local Hostname</b> of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). A <b>Local Hostname</b> configured in the LAC must match <b>Remote Hostname</b> configured for the intended profile in the LNS and vice versa.</li> <li>• <i>LNS</i>: Defines the <b>Local Hostname</b> of the LAC. If the <b>Remote Hostname</b> 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.</li> </ul>
<b>Password</b>	<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 <b>Local Hostname</b> and the <b>Password</b> 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
<b>Remote IP Address</b>	<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>
<b>UDP Source Port</b>	<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 <b>Fixed</b> 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>

Field	Description
	The available values are <i>0</i> to <i>65535</i> .
<b>UDP Destination Port</b>	<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 <i>0</i> to <i>65535</i>.</p> <p>The default value is <i>1701</i> (RFC 2661).</p>

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Local IP Address</b>	<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>
<b>Hello Intervall</b>	<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 <i>0</i> to <i>255</i>, the default value is <i>30</i>. The value <i>0</i> means that no L2TP HELLO messages are sent.</p>
<b>Minimum Time between Retries</b>	<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 <b>Maximum Time between Retries</b>. The available values are <i>1</i> to <i>255</i>, the default value is <i>1</i>.</p>
<b>Maximum Time between Retries</b>	<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>
<b>Maximum Retries</b>	Enter the maximum number of times your device is to try to re-

Field	Description
	send the L2TP control packet for which is received no response. The available values are 8 to 255, the default value is 5.
<b>Data Packets Sequence Numbers</b>	Select whether your device is to use sequence numbers for data packets sent through a tunnel on the basis of this profile. The function is enabled with <i>Enabled</i> . The function is disabled by default.

## 14.2.2 Users

A list of all configured interface L2TP partners is displayed in the **VPN->L2TP->Users** menu.

### 14.2.2.1 New

Choose the **New** button to set up new L2TP partners.

Tunnel Profiles **Users** Options

Basic Parameters													
Description	<input type="text"/>												
Connection Type	<input checked="" type="radio"/> LNS <input type="radio"/> LAC												
User Name	<input type="text"/>												
Password	<input type="password"/>												
Always on	<input type="checkbox"/> Enabled												
Connection Idle Timeout	<input type="text" value="300"/> Seconds												
IP Mode and Routes													
IP Address Mode	<input checked="" type="radio"/> Static <input type="radio"/> Provide IP Address												
Default Route	<input type="checkbox"/> Enabled												
Create NAT Policy	<input type="checkbox"/> Enabled												
Local IP Address	<input type="text"/>												
Route Entries	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Remote IP Address</th> <th style="width: 30%;">Netmask</th> <th style="width: 10%;">Metric</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text" value="1"/></td> <td><input type="text"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Remote IP Address	Netmask	Metric		<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>	<input type="button" value="Add"/>			
Remote IP Address	Netmask	Metric											
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text"/>										
<input type="button" value="Add"/>													
Advanced Settings													
Block after connection failure for	<input type="text" value="300"/> Seconds												
Authentication	<input type="text" value="MS-CHAPv2"/>												
Encryption	<input type="radio"/> None <input checked="" type="radio"/> Enabled <input type="radio"/> Windows compatible												
LCP Alive Check	<input checked="" type="checkbox"/> Enabled												
Prioritize TCP ACK Packets	<input type="checkbox"/> Enabled												
IP Options													
OSPF Mode	<input checked="" type="radio"/> Passive <input type="radio"/> Active <input type="radio"/> Inactive												
Proxy ARP Mode	<input checked="" type="radio"/> Inactive <input type="radio"/> Up or Dormant <input type="radio"/> Up only												
DNS Negotiation	<input checked="" type="checkbox"/> Enabled												
<input type="button" value="OK"/> <input type="button" value="Cancel"/>													

Fig. 145: VPN->L2TP->Users->New

The menu VPN->L2TP->Users->New consists of the following fields:

#### Fields in the Basic Parameters menu.

Field	Description
<b>Description</b>	<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>
<b>Connection Type</b>	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"> <li>• <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.</li> <li>• <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.</li> </ul>
<b>Tunnel Profile</b>	<p>Only for <b>Connection Type</b> = <i>LAC</i></p> <p>Select a profile created in the <b>Tunnel Profile</b> menu for the connection to this L2TP partner.</p>
<b>User Name</b>	Enter the code of your device.
<b>Password</b>	Enter the password.
<b>Always on</b>	<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>
<b>Connection Idle Timeout</b>	<p>Only if <b>Always on</b> 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. The default value is 300.</p>

#### Fields in the IP Mode and Routes menu.

Field	Description
<b>IP Address Mode</b>	<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"> <li>• <i>Static</i> (default value): You enter a static IP address.</li> <li>• <i>Provide IP Address</i>: Only for <b>Connection Type = LNS</b>. Your device dynamically assigns an IP address to the remote terminal.</li> <li>• <i>Get IP Address</i>: Only for <b>Connection Type = LAC</b>. Your device is dynamically assigned an IP address.</li> </ul>
<b>Default Route</b>	<p>Only for <b>IP Address Mode = Get IP Address</b> 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>
<b>Create NAT Policy</b>	<p>Only for <b>IP Address Mode = Get IP Address</b> 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>
<b>IP Assignment Pool (IPCP)</b>	<p>Only for <b>IP Address Mode = Provide IP Address</b></p> <p>Select an IP pool configured in the <b>WAN-&gt;Internet + Dialup-&gt;IP Pools</b> menu.</p>
<b>Local IP Address</b>	<p>Only for <b>IP Address Mode = Static</b></p> <p>Enter the WAN IP address of your device.</p>
<b>Route Entries</b>	<p>Only for <b>IP Address Mode = Static</b></p> <p>Enter <b>Remote IP Address</b> and <b>Netmask</b> of the LANs for L2TP partners and the corresponding <b>Metric</b>. Add new entries with <b>Add</b>.</p>

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

**Fields in the Advanced Settings menu.**

Field	Description
<b>Block after connection failure for</b>	<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>
<b>Authentication</b>	<p>Select the authentication protocol for this L2TP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.)</li> <li>• <i>PAP</i>: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <i>MS-CHAPv2</i>: Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>Encryption</b>	<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 <b>Encryption</b> 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"> <li>• <i>None</i>: MPP encryption is not used.</li> <li>• <i>Enabled</i> (default value): MPP encryption V2 with 128 bit is used to RFC 3078.</li> <li>• <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.</li> </ul>
<b>LCP Alive Check</b>	<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>
<b>Prioritize TCP ACK Packets</b>	<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
<b>OSPF Mode</b>	<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"> <li>• <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.</li> <li>• <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface.</li> <li>• <i>Inactive</i>: OSPF is disabled for this interface.</li> </ul>
<b>Proxy ARP Mode</b>	<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"> <li>• <i>Inactive</i> (default value): Deactivates Proxy ARP for this L2TP partner.</li> <li>• <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</li> </ul>



Field	Description
	<p>up until someone actually wants to use the route.</p> <ul style="list-style-type: none"> <li>• <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.</li> </ul>
<b>DNS Negotiation</b>	<p>Select whether your device receives IP addresses for <b>Primary DNS Server</b> und <b>Secondary DNS Server</b> and <b>WINS Server Primary</b> and <b>Secondary</b> from the L2TP partner or sends these to the L2TP partner.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

### 14.2.3 Options

[Tunnel Profiles](#) | [Users](#) | [Options](#)

Global Options	
UDP Destination Port	1701
UDP Source Port Selection	<input type="checkbox"/> Fixed

Fig. 146: VPN->L2TP->Options

The menu **VPN->L2TP->Options** consists of the following fields:

#### Fields in the **Global Options** menu.

Field	Description
<b>UDP Destination Port</b>	<p>Enter the port to be monitored by the LNS on incoming L2TP tunnel connections.</p> <p>Available values are all whole numbers from 1 to 65535, the default value is 1701, as specified in RFC 2661.</p>
<b>UDP Source Port Selection</b>	<p>Select whether the LNS should only use the monitored port (<b>UDP Destination Port</b>) as the local source port for the L2TP connection.</p> <p>The function is enabled with <i>Fixed</i>.</p>

Field	Description
	The function is disabled by default.

## 14.3 PPTP

The Point-to-Point Tunneling 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).

### 14.3.1 PPTP Tunnels

A list of all PPTP tunnels is displayed in the **PPTP Tunnels** menu.

### 14.3.1.1 New

Click on **New** to set up further PPTP partners.

PPTP Tunnels
Options
IP Pools

PPTP Partner Parameters													
Description	<input style="width: 90%;" type="text"/>												
PPTP Mode	<input checked="" type="radio"/> PNS <input type="radio"/> Windows Client Mode												
User Name	<input style="width: 90%;" type="text"/>												
Password	<input style="width: 90%;" type="password"/>												
Always on	<input type="checkbox"/> Enabled												
Connection Idle Timeout	<input style="width: 50%;" type="text" value="300"/> Seconds												
Remote PPTP IP Address	<input style="width: 90%;" type="text"/>												
IP Mode and Routes													
IP Address Mode	<input type="radio"/> Static <input type="radio"/> Provide IP Address												
Default Route	<input type="checkbox"/> Enabled												
Create NAT Policy	<input type="checkbox"/> Enabled												
Local IP Address	<input style="width: 90%;" type="text"/>												
Route Entries	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Remote IP Address</th> <th style="width: 30%;">Netmask</th> <th style="width: 10%;">Metric</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td><input style="width: 90%;" type="text"/></td> <td><input style="width: 90%;" type="text"/></td> <td>1</td> <td><input type="button" value="v"/></td> </tr> <tr> <td colspan="4" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Remote IP Address	Netmask	Metric		<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	1	<input type="button" value="v"/>	<input type="button" value="Add"/>			
Remote IP Address	Netmask	Metric											
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/>	1	<input type="button" value="v"/>										
<input type="button" value="Add"/>													
Advanced Settings													
Block after connection failure for	<input style="width: 50%;" type="text" value="300"/> Seconds												
Authentication	<input type="text" value="MS-CHAPv2"/> <input type="button" value="v"/>												
Encryption	<input type="radio"/> None <input checked="" type="radio"/> Enabled <input type="radio"/> Windows compatible												
Compression	<input checked="" type="radio"/> None <input type="radio"/> STAC <input type="radio"/> MS-STAC <input type="radio"/> MPPC												
LCP Alive Check	<input checked="" type="checkbox"/> Enabled												
IP Options													
OSPF Mode	<input checked="" type="radio"/> Passive <input type="radio"/> Active <input type="radio"/> Inactive												
Proxy ARP Mode	<input checked="" type="radio"/> Inactive <input type="radio"/> Up or Dormant <input type="radio"/> Up only												
DNS Negotiation	<input checked="" type="checkbox"/> Enabled												
PPTP Callback													
Callback	<input type="checkbox"/> Enabled												
<input type="button" value="OK"/> <input type="button" value="Cancel"/>													

Fig. 147: 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
<b>Description</b>	<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>
<b>PPTP Mode</b>	<p>Enter the role to be assigned to the PPTP interface.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>PNS</i> (default value): this assigns the PPTP interface the role of PPTP server.</li> <li>• <i>Windows Client Mode</i>: This assigns the PPTP interface the role of PPTP client.</li> </ul>
<b>User Name</b>	Enter the user name.
<b>Password</b>	Enter the password.
<b>Always on</b>	<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>
<b>Connection Idle Timeout</b>	<p>Only if <b>Always on</b> 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 0 to 3600 (seconds). 0 deactivates the timeout.</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>
<b>Remote PPTP IP Address</b>	<p>Only for <b>PPTP Mode</b> = <i>PNS</i></p> <p>Enter the IP address of the PPTP partner.</p>
<b>Remote PPTP IP Address/Host Name</b>	<p>Only for <b>PPTP Mode</b> = <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
<b>IP Address Mode</b>	<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"> <li>• <i>Static</i> (default value): You enter a static IP address.</li> <li>• <i>Provide IP Address</i>: Only for <b>PPTP Mode = PNS</b>: Your device dynamically assigns an IP address to the remote terminal.</li> <li>• <i>Get IP Address</i>: Only for <b>PPTP Mode = Windows Client Mode</b>: Your device is dynamically assigned an IP address.</li> </ul>
<b>Default Route</b>	<p>Only if <b>IP Address Mode = Static</b></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>
<b>Create NAT Policy</b>	<p>Only if <b>IP Address Mode = Static</b></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>
<b>Local IP Address</b>	<p>Only for <b>IP Address Mode = Static</b></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>
<b>Route Entries</b>	<p>Only if <b>IP Address Mode = Static</b></p> <p>Define routing entries for this connection partner.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or LAN.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Metric</i>: The lower the value, the higher the priority of the route (possible values 0 . . . 15). The default value is 1.</li> </ul>
<b>IP Assignment Pool (IPCP)</b>	<p>Only if <b>PPTP Mode</b> = <i>PNS</i>, <b>IP Address Mode</b> = <i>Provide IP Address</i></p> <p>Select a IP pool configured in the <b>VPN-&gt;PPTP-&gt;IP Pools</b> menu.</p>

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

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Block after connection failure for</b>	<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 300.</p>
<b>Usage Type</b>	<p>If necessary, select a special interface use.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Standard</i> (default value): No special type is selected.</li> <li>• <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.</li> </ul>
<b>Authentication</b>	<p>Select the authentication protocol for this PPTP partner.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>PAP</i>: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.</li> <li>• <i>CHAP</i>: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted.</li> <li>• <i>PAP/CHAP</i>: Primarily run CHAP, otherwise PAP.</li> <li>• <i>MS-CHAPv1</i>: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol).</li> <li>• <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.)</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>MS-CHAPv2</i> (default value): Run MS-CHAP version 2 only.</li> <li>• <i>None</i>: Some providers use no authentication. In this case, select this option.</li> </ul>
<b>Encryption</b>	<p>If necessary, select the type of encryption that should be used for data traffic to the connection partner. If <b>Encryption</b> 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"> <li>• <i>None</i>: MPP encryption is not used.</li> <li>• <i>Enabled</i> (default value): MPP encryption V2 with 128 bit is used to RFC 3078.</li> <li>• <i>Windows compatible</i>: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.</li> </ul>
<b>Compression</b>	<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"> <li>• <i>None</i> (default value): Encryption is not used.</li> <li>• <i>STAC</i></li> <li>• <i>MS-STAC</i></li> <li>• <i>MPPC</i>: Microsoft Point-to-Point Compression</li> </ul>
<b>LCP Alive Check</b>	<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
<b>OSPF Mode</b>	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Active</i>: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface.</li> <li>• <i>Inactive</i>: OSPF is disabled for this interface.</li> </ul>
<b>Proxy ARP Mode</b>	<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"> <li>• <i>Inactive</i> (default value): Disables Proxy-ARP (Address Resolution Protocol) for this PPTP partner.</li> <li>• <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.</li> <li>• <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.</li> </ul>
<b>DNS Negotiation</b>	<p>Select whether your device receives IP addresses for <b>Primary DNS Server</b> and <b>Secondary DNS Server</b> 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
<b>Callback</b>	<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</p>



Field	Description
	<p>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 special applications.</p>
<b>Incoming ISDN Number</b>	<p>Only if <b>Callback</b> is enabled.</p> <p>Enter the ISDN number from which the remote device calls the local device (calling party number).</p>
<b>Outgoing ISDN Number</b>	<p>Only if <b>Callback</b> is enabled.</p> <p>Enter the ISDN number with which the local device calls the remote device calls (called party number).</p>

#### Fields in the Dial Port Selection (only if callback = activated)

Field	Description
<b>Selected Ports</b>	<p>Enter the ISDN port over which callback is carried out.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>All Ports</i>: The callback is routed over an available ISDN port.</li> <li>• <i>Specify port</i>: In <b>Specific Ports</b> You can select the required ISDN port.</li> </ul>
<b>Specific Ports</b>	<p>Only for <b>Selected Ports</b> = <i>Specify port</i>, you can select additional ports with <b>Add</b>.</p>

## 14.3.2 Options

In this menu, you can make general settings of the global PPTP profile.

Fig. 148: VPN->PPTP->Options

The VPN->PPTP->Options menu consists of the following fields:

### Fields in the Global Options menu.

Field	Description
<b>GRE Window Adaption</b>	<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>
<b>GRE Window Size</b>	<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 <b>GRE Window Size</b> value. Possible values are 0 to 256.</p> <p>The default value is 0.</p>
<b>Max. incoming control connections per remote IP Address</b>	<p>Enter the maximum number of control connections.</p>

### 14.3.3 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.

#### 14.3.3.1 Edit or New

Choose the **New** button to set up new IP address pools. Choose the  icon to edit existing entries.

PPTP Tunnels Options **IP Pools**

Basic Parameters					
IP Pool Name	<input type="text"/>				
IP Address Range	<input type="text"/> - <input type="text"/>				
DNS Server	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%; padding: 2px;">Primary</td> <td style="padding: 2px;"><input type="text"/></td> </tr> <tr> <td style="padding: 2px;">Secondary</td> <td style="padding: 2px;"><input type="text"/></td> </tr> </table>	Primary	<input type="text"/>	Secondary	<input type="text"/>
Primary	<input type="text"/>				
Secondary	<input type="text"/>				
<input type="button" value="OK"/> <input type="button" value="Cancel"/>					

Fig. 149: VPN->PPTP->IP Pools->New

#### Fields in the menu Basic Parameters

Field	Description
<b>IP Pool Name</b>	Enter any description to uniquely identify the IP pool.
<b>IP Address Range</b>	Enter the first (first field) and last (second field) IP address of the IP address pool.

Field	Description
<b>DNS Server</b>	<p><b>Primary:</b> Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p><b>Secondary:</b> Optionally, enter the IP address of an alternative DNS server.</p>

## 14.4 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.

### 14.4.1 GRE Tunnels

A list of all configured GRE tunnels is displayed in the **VPN->GRE->GRE Tunnels** menu.

### 14.4.1.1 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 border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Remote IP Address</th> <th style="width: 30%;">Netmask</th> <th style="width: 10%;">Metric</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <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" style="text-align: center;"><input type="button" value="Add"/></td> </tr> </tbody> </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. 150: 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
<b>Description</b>	Enter a description for the GRE tunnel.
<b>Local GRE IP Address</b>	<p>Enter the source IP address of the GRE packets to the GRE partner.</p> <p>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.</p>
<b>Remote GRE IP Address</b>	Enter the target IP address of the GRE packets to the GRE partner.
<b>Default Route</b>	<p>If you enable the <b>Default Route</b>, all data is automatically routed to one connection.</p> <p>The function is disabled by default.</p>

Field	Description
<b>Local IP Address</b>	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.
<b>Route Entries</b>	<p>Define other routing entries for this connection partner.</p> <p>Add new entries with <b>Add</b>.</p> <ul style="list-style-type: none"> <li>• <i>Remote IP Address</i>: IP address of the destination host or network.</li> <li>• <i>Netmask</i>: Netmask for <b>Remote IP Address</b>. If no entry is made, your device uses a default netmask.</li> <li>• <i>Metric</i>: The lower the value, the higher the priority of the route (range of values 0... 15). The default value is 1.</li> </ul>
<b>MTU</b>	<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 1 to 8192.</p> <p>The default value is 1500.</p>
<b>Use key</b>	<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>
<b>Key Value</b>	<p>Only if <b>Use key</b> is enabled.</p> <p>Enter the GRE connection key.</p> <p>Possible values are 0 to 2147483647.</p> <p>The default value is 0.</p>

## Chapter 15 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).

## 15.1 Policies

### 15.1.1 IPv4 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.

The security concept is based on the assumption that an infrastructure consists of trusted and untrusted zones. The security policies *Trusted* and *Untrusted* describe this assumption. They define the filter rules **Trusted Interfaces** and **Untrusted Interfaces** which are created by default and cannot be deleted.

If you use the **Security Policy** *Trusted*, all data packets are accepted. You can create additional filter rules that discard specific packets. In the same way, you can allow specific packets when using the *Untrusted* policy.

A list of all configured filter rules is displayed in the **Firewall->Policies+IPv4 Filter Rules** menu.

IPv4 Filter Rules IPv6 Filter Rules Options

View  per page << >> Filter in None equal Go

Order	Source	Destination	Service	Action	Priority	Policy active			
Page: 1									
Default Filter Rules									
n+1	Trusted Interfaces	ANY	any	Access	None	<input checked="" type="checkbox"/>	Enabled		
n+2	Untrusted Interfaces	ANY	any	Deny	None	<input checked="" type="checkbox"/>	Enabled		

New OK Cancel

Fig. 151: **Firewall->Policies+IPv4 Filter Rules**

Using the button in the line **Trusted Interfaces**, you can determine which interfaces are **Trusted**. A new window opens with an interface list. You can mark individual interfaces as trusted.

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.

### 15.1.1.1 New

Choose the **New** button to create additional parameters.

Fig. 152: Firewall->Policies+IPv4 Filter Rules->New

The menu **Firewall->Policies+IPv4 Filter Rules->New** consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>Source</b>	<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 <b>Firewall-&gt;Interfaces-&gt;Groups</b>), addresses (see <b>Firewall-&gt;Addresses-&gt;Address List</b>) and address groups (see <b>Firewall-&gt;Addresses-&gt;Groups</b>) are available.</p> <p>The value <i>any</i> means that neither the source interface nor the source address is checked.</p>
<b>Destination</b>	<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 <b>Firewall-&gt;Interfaces-&gt;Groups</b>), addresses (see <b>Firewall-&gt;Addresses-&gt;Address List</b>) and address groups (see <b>Firewall-&gt;Addresses-&gt;Groups</b>).</p> <p>The value <i>any</i> means that neither the destination interface nor the destination address is checked.</p>
<b>Service</b>	<p>Select one of the preconfigured services to which the packet to be filtered must be assigned.</p>

Field	Description
	<p>The extensive range of services configured ex works includes the following:</p> <ul style="list-style-type: none"> <li>• <i>ftp</i></li> <li>• <i>telnet</i></li> <li>• <i>smtp</i></li> <li>• <i>dns</i></li> <li>• <i>http</i></li> <li>• <i>nntp</i></li> <li>• <i>Internet</i></li> <li>• <i>Netmeeting</i></li> </ul> <p>Additional services are created in <b>Firewall-&gt;Services-&gt;Service List</b>.</p> <p>In addition, the service groups configured in <b>Firewall-&gt;Services-&gt;Groups</b> can be selected.</p>
<b>Action</b>	<p>Select the action to be applied to a filtered packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Access</i> (default value): The packets are forwarded on the basis of the entries.</li> <li>• <i>Deny</i>: The packets are rejected.</li> <li>• <i>Reject</i>: The packets are rejected. An error message is issued to the sender of the packet.</li> </ul>

## 15.1.2 IPv6 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.

The security concept is based on the assumption that an infrastructure consists of trusted and untrusted zones. The security policies *Trusted* and *Untrusted* describe this assumption. They define the filter rules **Trusted Interfaces** and **Untrusted Interfaces** which are created by default and cannot be deleted.

If you use the **Security Policy** *Trusted*, all data packets are accepted. You can create additional filter rules that discard specific packets. In the same way, you can allow specific packets when using the *Untrusted* policy.

A list of all configured filter rules is displayed in the **Firewall->Policies->IPv6 Filter Rules** menu.

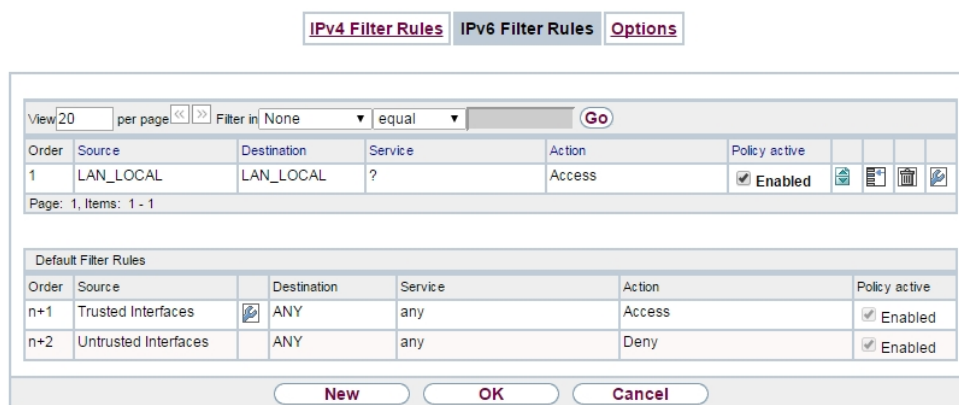





Fig. 153: Firewall->Policies->IPv6 Filter Rules

Using the  button in the line **Trusted Interfaces**, you can determine which interfaces are **Trusted**. A new window opens with an interface list. You can mark individual interfaces as trusted.

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.

### 15.1.2.1 New

Choose the **New** button to create additional parameters.

[IPv4 Filter Rules](#) | [IPv6 Filter Rules](#) | [Options](#)

Basic Parameters	
Source	--- GROUPS --- ▾
Destination	--- GROUPS --- ▾
Service	--- SERVICES --- ▾
Action	Access ▾

Fig. 154: Firewall->Policies->IPv6 Filter Rules->New

The menu **Firewall->Policies->IPv6 Filter Rules->New** consists of the following fields:

#### Fields in the **Basic Parameters** menu

Field	Description
<b>Source</b>	<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 <b>Firewall-&gt;Interfaces-&gt;IPv6 Groups</b>), addresses (see <b>Firewall-&gt;Addresses-&gt;Address List</b>) and address groups (see <b>Firewall-&gt;Addresses-&gt;Groups</b>) are available for selection for IPv6.</p>
<b>Destination</b>	<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 <b>Firewall-&gt;Interfaces-&gt;IPv6 Groups</b>), addresses (see <b>Firewall-&gt;Addresses-&gt;Address List</b>) and address groups (see <b>Firewall-&gt;Addresses-&gt;Groups</b>) are available for selection for IPv6.</p>
<b>Service</b>	<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"> <li>• <i>ftp</i></li> <li>• <i>telnet</i></li> <li>• <i>smtp</i></li> <li>• <i>dns</i></li> <li>• <i>http</i></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li><i>nntp</i></li> </ul> <p>Additional services are created in <b>Firewall-&gt;Services-&gt;Service List</b>.</p> <p>In addition, the service groups configured in <b>Firewall-&gt;Services-&gt;Groups</b> can be selected.</p>
<b>Action</b>	<p>Select the action to be applied to a filtered packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li><i>Access</i> (default value): The packets are forwarded on the basis of the entries..</li> <li><i>Deny</i>: The packets are rejected.</li> <li><i>Reject</i>: The packets are rejected. An error message is issued to the sender of the packet.</li> </ul>

### 15.1.3 Options

In this menu, you can disable or enable the IPv4 firewall and can log its activities. In addition, you can define after how many seconds of inactivity a session shall be ended.



#### Note

The IPv6 firewall is always active and cannot be disabled.

IPv4 Filter Rules
IPv6 Filter Rules
Options

Global Firewall Options	
IPv4 Firewall Status	<input type="checkbox"/> Enabled
Logged Actions	All ▾
IPv4 Full Filtering	<input checked="" type="checkbox"/> Enable
Session Timer	
UDP Inactivity	<input type="text" value="180"/> Seconds
TCP Inactivity	<input type="text" value="3600"/> Seconds
PPTP Inactivity	<input type="text" value="86400"/> Seconds
Other Inactivity	<input type="text" value="30"/> Seconds
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 155: Firewall->Policies->Options

The menu **Firewall->Policies->Options** consists of the following fields:

#### Fields in the **Global Firewall Options** menu.

Field	Description
<b>IPv4 Firewall Status</b>	<p>Enable or disable the IPv4 firewall function.</p> <p>The function is enabled with <i>Enabled</i></p> <p>The function is enabled by default.</p>
<b>Logged Actions</b>	<p>Select the firewall syslog level.</p> <p>The messages are output together with messages from other subsystems.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>All</i> (default value): All firewall activities are displayed.</li> <li>• <i>Deny</i>: Only reject and deny events are shown, see "Action".</li> <li>• <i>Accept</i>: Only accept events are shown.</li> <li>• <i>None</i>: Syslog messages are not generated.</li> </ul>
<b>IPv4 Full Filtering</b>	<p>With TCP sessions, the SIF first verifies if a session has been established completely and correctly. The filtering itself is carried out in a second step. The default setting <b>IPv4 Full Filtering</b> has been designed to meet this "standard" case.</p> <p>If - in a two-way communication - one traffic direction is sent through the router, but the counter direction takes a different route, the data traffic of this connection will be blocked because the session is interpreted as "incomplete" by the SIF. This will happen even if there is a rule that allows the same kind data traffic in a complete session.</p> <p>In order to allow the data traffic of "incomplete" sessions you have to disable <b>IPv4 Full Filtering</b>.</p>

#### Fields in the **Session Timer** menu.

Field	Description
<b>UDP Inactivity</b>	<p>Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds).</p> <p>Possible values are <i>30</i> to <i>86400</i>.</p>

Field	Description
	The default value is <i>180</i> .
<b>TCP Inactivity</b>	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> .
<b>PPTP Inactivity</b>	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds).  Possible values are <i>30</i> to <i>86400</i> .  The default value is <i>86400</i> .
<b>Other Inactivity</b>	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds).  Possible values are <i>30</i> to <i>86400</i> .  The default value is <i>30</i> .

#### Fields in the Factory Reset Firewall

Field	Description
<b>Factory Reset Firewall</b>	Click <b>Reset</b> to reset the firewall to factory defaults.

## 15.2 Interfaces

### 15.2.1 IPv4 Groups

A list of all configured IPv4 interface routes is displayed in the **Firewall->Interfaces->IPv4 Groups** menu.

You can group together the interfaces of your device. This makes it easier to configure firewall rules.

#### 15.2.1.1 New

Choose the **New** button to set up new IPv4 interface groups.



IPv4 Groups IPv6 Groups

Basic Parameters											
Description	<input style="width: 90%;" type="text"/>										
Members	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #f2f2f2;"> <th style="width: 70%;">Interface</th> <th style="width: 30%;">Selection</th> </tr> </thead> <tbody> <tr> <td>LAN_LOCAL</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-0</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>LAN_EN1-4</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>WAN_ETH0A50-0</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>	Interface	Selection	LAN_LOCAL	<input type="checkbox"/>	LAN_EN1-0	<input type="checkbox"/>	LAN_EN1-4	<input type="checkbox"/>	WAN_ETH0A50-0	<input type="checkbox"/>
Interface	Selection										
LAN_LOCAL	<input type="checkbox"/>										
LAN_EN1-0	<input type="checkbox"/>										
LAN_EN1-4	<input type="checkbox"/>										
WAN_ETH0A50-0	<input type="checkbox"/>										

OK Cancel

Fig. 156: Firewall->Interfaces->IPv4 Groups->New

The menu **Firewall->Interfaces->IPv4 Groups->New** consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>Description</b>	Enter the desired description of the IPv4 interface group.
<b>Members</b>	Select the members of the group from the available interfaces. To do this, activate the field in the <b>Selection</b> column.

## 15.2.2 IPv6 Groups

A list of all configured IPv6 interface routes is displayed in the **Firewall->Interfaces+IPv6 Groups** menu.

You can group together the IPv6 interfaces of your device. This makes it easier to configure firewall rules.

### 15.2.2.1 New

Choose the **New** button to set up new IPv6 interface groups.

The screenshot shows a configuration window for IPv6 Groups. It features two tabs at the top: 'IPv4 Groups' (highlighted in red) and 'IPv6 Groups'. Below the tabs is a 'Basic Parameters' section with a 'Description' text input field and a 'Members' section containing an 'Interface Selection' button. At the bottom of the window are 'OK' and 'Cancel' buttons.

Fig. 157: Firewall->Interfaces->IPv6 Groups->New

The menu **Firewall->Interfaces->IPv6 Groups->New** consists of the following fields

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>Description</b>	Enter the desired description of the IPv6 interface group.
<b>Members</b>	Select the members of the group from the available interfaces. To do this, activate the field in the <b>Selection</b> column.

## 15.3 Addresses

### 15.3.1 Address List

A list of all configured addresses is displayed in the **Firewall->Addresses->Address List** menu.

#### 15.3.1.1 New

Choose the **New** button to create additional addresses.

Address List Groups

Basic Parameters	
Description	<input type="text"/>
IPv4	<input checked="" type="checkbox"/> Enabled
Address Type	<input checked="" type="radio"/> Address / Subnet <input type="radio"/> Address Range
Address / Subnet	<input type="text"/> / <input type="text" value="255.255.255.0"/>
IPv6	<input type="checkbox"/> Enabled

OK Cancel

Fig. 158: 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
<b>Description</b>	Enter the desired description of the address.
<b>IPv4</b>	Allows configuration of IPv4 address lists.  The function is enabled with <i>Enabled</i> .  The function is enabled by default.
<b>Address Type</b>	Only for <b>IPv4</b> = <i>Enabled</i>  Select the type of address you want to specify.  Possible values: <ul style="list-style-type: none"> <li>• <i>Address / Subnet</i> (default value): Enter an IP address with subnet mask.</li> <li>• <i>Address Range</i>: Enter an IP address range with a start and end address.</li> </ul>
<b>Address / Subnet</b>	Only for <b>IPv4</b> = <i>Enabled</i>  and <b>Address Type</b> = <i>Address / Subnet</i>  Enter the IP address of the host or a network address and the related netmask.  The default value is <i>0.0.0.0</i> .
<b>IPv6</b>	Allows configuration of IPv6 address lists.

Field	Description
	The function is enabled with <i>Enabled</i> . The function is disabled by default.
<b>Address / Prefix</b>	Only for IPv6 = <i>Enabled</i> Enter IPv6 address and the related prefix.

## 15.3.2 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.

### 15.3.2.1 New

Choose the **New** button to set up additional address groups.

Fig. 159: Firewall->Addresses->Groups->New

The menu **Firewall->Addresses->Groups->New** consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>Description</b>	Enter the desired description of the address group.
<b>IP Version</b>	Select the IP version used.  Possible values: <ul style="list-style-type: none"> <li>• <i>IPv4</i></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li><i>IPv6</i></li> </ul> <p><i>IPv4</i> is selected by default.</p>
<b>Selection</b>	Select the members of the group from the available <b>Addresses</b> . To do this, activate the Fields in the <b>Selection</b> column.

## 15.4 Services

### 15.4.1 Service List

In the **Firewall->Services->Service List** menu, a list of all available services is displayed.

#### 15.4.1.1 New

Choose the **New** button to set up additional services.

Fig. 160: 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
<b>Description</b>	Enter an alias for the service you want to configure.
<b>Protocol</b>	Select the protocol on which the service is to be based. The most important protocols are available for selection.
<b>Destination Port Range</b>	<p>Only for <b>Protocol</b> = <i>TCP</i>, <i>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>

Field	Description
	<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>
<b>Source Port Range</b>	<p>Only for <b>Protocol</b> = <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>
<b>Type</b>	<p>Only for <b>Protocol</b> = <i>ICMP</i></p> <p>The <b>Type</b> field shows the class of ICMP messages, the <b>Code</b> field specifies the type of message in greater detail.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value)</li> <li>• <i>Echo Reply</i></li> <li>• <i>Destination unreachable</i></li> <li>• <i>Source Quench</i></li> <li>• <i>Redirect</i></li> <li>• <i>Echo</i></li> <li>• <i>Time Exceeded</i></li> <li>• <i>Parameter Problem</i></li> <li>• <i>Timestamp</i></li> <li>• <i>Timestamp Reply</i></li> <li>• <i>Information Request</i></li> <li>• <i>Information Reply</i></li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Address Mask Request</i></li> <li>• <i>Address Mask Reply</i></li> </ul>
<b>Code</b>	<p>Selection options for the ICMP codes are only available for <b>Type</b> = <i>Destination unreachable</i></p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any (default value)</i></li> <li>• <i>Net Unreachable</i></li> <li>• <i>Host Unreachable</i></li> <li>• <i>Protocol Unreachable</i></li> <li>• <i>Port Unreachable</i></li> <li>• <i>Fragmentation Needed</i></li> <li>• <i>Communication with Destination Network is Administratively Prohibited</i></li> <li>• <i>Communication with Destination Host is Administratively Prohibited</i></li> </ul>

## 15.4.2 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.

### 15.4.2.1 New

Choose the **New** button to set up additional service groups.

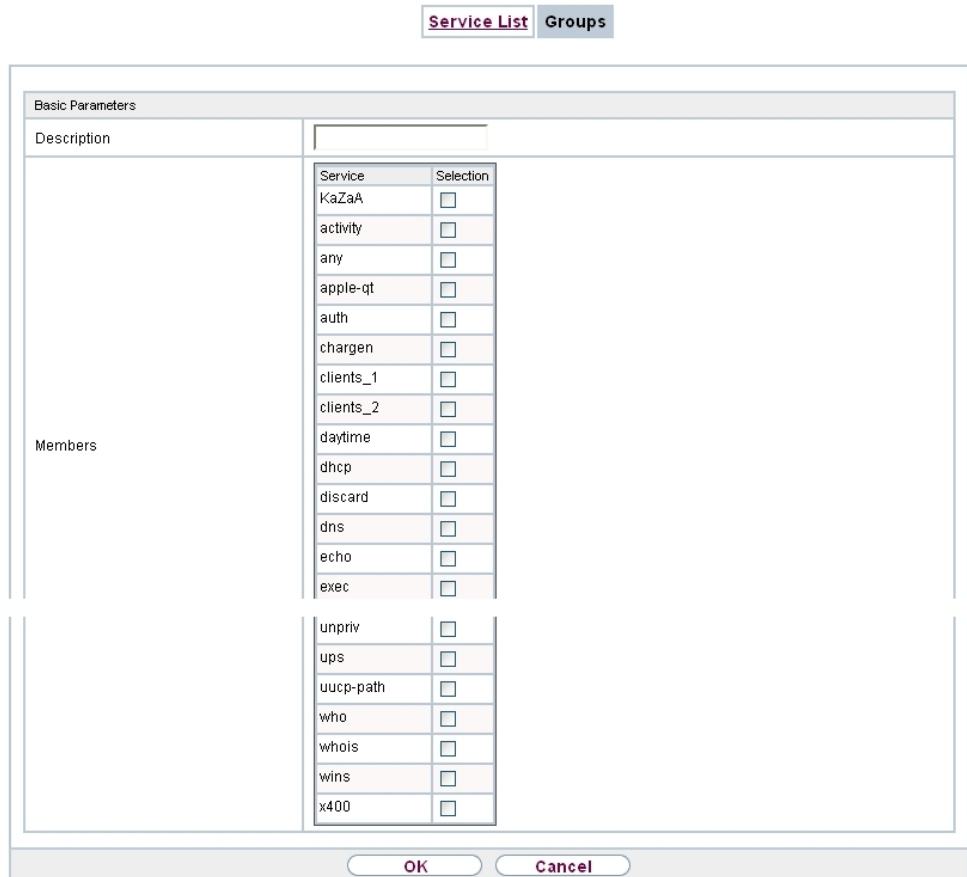


Fig. 161: Firewall->Services->Groups->New

The menu **Firewall->Services->Groups->New** consists of the following fields:

**Fields in the Basic Parameters menu.**

Field	Description
<b>Description</b>	Enter the desired description of the service group.
<b>Members</b>	Select the members of the group from the available service aliases. To do this, activate the Fields in the <b>Selection</b> column.

## 15.5 Configuration

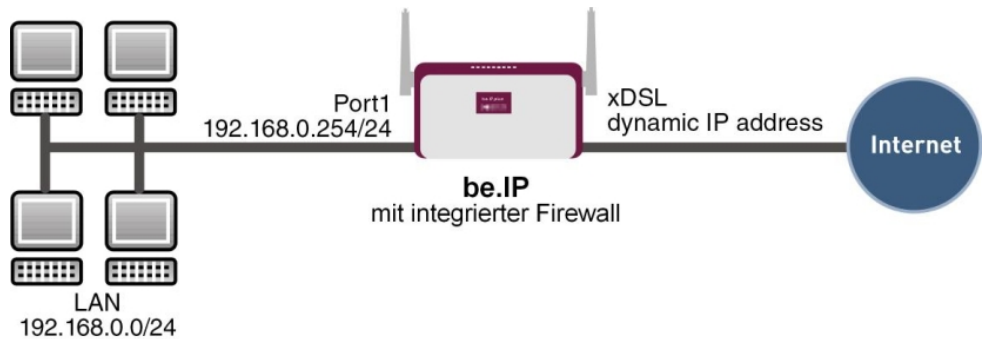


## 15.5.1 SIF - Configuration example

### Requirements

- Internet connection
- Your LAN must be connected to one of ports 1, 2, 3 or 4 on the gateway.

### Example scenario



### Configuration target

- Only certain Internet services are to be available for the staff of a company (HTTP, HTTPS, FTP, DNS).
- The gateway should operate as a DNS proxy, which means that the clients use the gateway as a DNS server.
- Only the system administrator and the director should be able to establish an HTTP and a Telnet connection to the gateway.
- The director must be able to use all services in the Internet..
- All other data traffic will be blocked.



#### Important

An incorrect configuration of the firewall can significantly disrupt the functionality of the gateway or drop the connections.

The usual principle for firewalls also applies: Everything that is not explicitly allowed is prohibited.

This means accurate planning of the filter rules and filter rule chain is necessary to ensure correct operation.

## Overview of Configuration Steps

### Aliases for IP addresses and network address

Field	Menu	Value
Description	Firewall->Addresses->Address List->New	e.g. <i>Administrator</i>
Address Type	Firewall->Addresses->Address List->New	<i>Address / Subnet</i>
Address / Subnet	Firewall->Addresses->Address List->New	e.g. <i>192.168.0.2</i> with <i>255.255.255.255</i>
Description	Firewall->Addresses->Address List->New	e.g. <i>Director</i>
Address Type	Firewall->Addresses->Address List->New	<i>Address / Subnet</i>
Address / Subnet	Firewall->Addresses->Address List->New	e.g. <i>192.168.0.3</i> with <i>255.255.255.255</i>
Description	Firewall->Addresses->Address List->New	e.g. <i>be.IP</i>
Address Type	Firewall->Addresses->Address List->New	<i>Address / Subnet</i>
Address / Subnet	Firewall->Addresses->Address List->New	e.g. <i>192.168.0.254</i> with <i>255.255.255.255</i>
Description	Firewall->Addresses->Address List->New	e.g. <i>Network Internal</i>
Address Type	Firewall->Addresses->Address List->New	<i>Address / Subnet</i>
Address / Subnet	Firewall->Addresses->Address List->New	e.g. <i>192.168.0.0</i> with <i>255.255.255.0</i>

### Address groups

Field	Menu	Value
Description	Firewall -> Addresses -> Groups -> New	e.g. <i>be.IP</i>
IP Version	Firewall -> Addresses -> Groups -> New	<i>IPv4</i>

Field	Menu	Value
Selection	Firewall -> Addresses -> Groups -> New	e.g. <i>Administrator</i> and <i>Director</i>

#### Service Sets

Field	Menu	Value
Description	Firewall -> Services -> Groups -> New	e.g. <i>Internet Ports</i>
Members	Firewall -> Services -> Groups -> New	e.g. <i>http</i> , <i>http (SSL)</i> and <i>ftp</i>
Description	Firewall -> Services -> Groups -> New	e.g. <i>Administration Ports</i>
Members	Firewall -> Services -> Groups -> New	e.g. <i>http</i> and <i>telnet</i>

#### Filter rules 1: Manage Gateway (System administrator)

Field	Menu	Value
Source Location	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>be.IP</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>be.IP</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Administration Ports</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>

#### Filter rules 2: Use gateway as DNS proxy

Field	Menu	Value
Source Location	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>LOCAL</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>ANY</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>dns</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>
Source Location	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Netzwerk_Intern</i>
Destination	Firewall -> Policies -> IPv4	<i>be.IP</i>

Field	Menu	Value
	Filter Rules -> New	
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>dns</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>

### Filter rules 3: Deny access from outside to the Gateway

Field	Menu	Value
Source Location	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>ANY</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>be.IP</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>any</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Deny</i>

### Filter rules 4: Allow access to all services on the Internet (Director)

Field	Menu	Value
Source Location	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Director</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>ANY</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>any</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>

### Filter rules 5: Allow access to the Internet (Staff)

Field	Menu	Value
Source Location	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Network_Internal</i>
Destination	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>ANY</i>
Service	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Internet Ports</i>
Action	Firewall -> Policies -> IPv4 Filter Rules -> New	<i>Access</i>

## Chapter 16 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.

### 16.1 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).

#### 16.1.1 Options

In the **VoIP->SIP->Options** menu, you can make global settings for the SIP.

The screenshot shows a dialog box titled "Options" with a "Basic Parameters" section. It contains three rows of settings:

Basic Parameters	
SIP Proxy	<input type="checkbox"/> Enabled
SIP Port	5060
Prioritize SIP Calls	<input type="checkbox"/> Enabled

At the bottom of the dialog are "OK" and "Cancel" buttons.

Fig. 162: **VoIP->SIP->Options**

The **VoIP->SIP->Options** menu consists of the following fields:

#### Fields in the Basic Parameters menu.

Field	Description
<b>SIP Proxy</b>	<p>Select whether you want to activate the SIP proxy.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>SIP Port</b>	<p>Enter the port to be supervised by the proxy.</p>

Field	Description
	<p>You must configure a proxy for each destination port to which VoIP clients from the LAN can connect. An error message appears when you enter multiple ports (e.g. 5060; 5061).</p> <p>The ports can be provider-specific.</p> <p>Possible values are 0 to 65535.</p> <p>The default value is 5060.</p>
<b>Prioritize SIP Calls</b>	<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>

## 16.2 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.

### 16.2.1 RTSP Proxy

In the **VoIP->RTSP->RTSP Proxy** menu, you configure the use of the RealTime Streaming protocol.

**RTSP Proxy**

Basic Parameters	
RTSP Proxy	<input type="checkbox"/> <b>Enabled</b>
RTSP Port	<input style="width: 80%;" type="text" value="554"/>

Fig. 163: **VoIP->RTSP->RTSP Proxy**

The **VoIP->RTSP->RTSP Proxy** menu consists of the following fields:

**Fields in the Basic Parameters menu.**

Field	Description
<b>RTSP Proxy</b>	Select whether you want to permit RTSP sessions.  The function is activated by selecting <i>Enabled</i> .  The function is disabled by default.
<b>RTSP Port</b>	Select the port over which the RTSP messages are to come in and go out.  Possible values are 0 to 65535.  The default value is 554.

## Chapter 17 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)
- Assignment of incoming and outgoing data and voice calls to authorised users (CAPI server)
- Automation of tasks according to schedule (scheduling)
- Alive checks for hosts or interfaces, ping tests
- User LAN protection (theft protection)
- Realtime video/audio conferences (Messenger services, universal plug & play)
- Provision of public Internet accesses (hotspot).
- Wake on LAN, um Netzwerkgeräte zu aktivieren, die aktuell ausgeschaltet sind.
- Use of a redundant gateway (BRRP).

### 17.1 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.

## 17.1.1 Global Settings

Global Settings
DNS Servers
Static Hosts
Domain Forwarding
Cache
Statistics

**Basic Parameters**

Domain Name	<input type="text"/>
WINS Server	Primary <input type="text" value="0.0.0.0"/>
	Secondary <input type="text" value="0.0.0.0"/>

**Advanced Settings**

Positive Cache	<input checked="" type="checkbox"/> Enabled
Negative Cache	<input checked="" type="checkbox"/> Enabled
Cache Size	<input type="text" value="100"/> Entries
Maximum TTL for Positive Cache Entries	<input type="text" value="86400"/> Seconds
Maximum TTL for Negative Cache Entries	<input type="text" value="300"/> Seconds
Fallback interface to get DNS server	<input type="text" value="Automatic"/> <small>▼</small>
<small>IP address to use for DNS/WINS server assignment</small>	
As DHCP Server	<input type="radio"/> None <input checked="" type="radio"/> Own IP Address <input type="radio"/> DNS Setting
As IPCP Server	<input type="radio"/> None <input type="radio"/> Own IP Address <input checked="" type="radio"/> DNS Setting

Fig. 164: 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
<b>Domain Name</b>	Enter the standard domain name of your device.
<b>WINS Server</b>	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).
<b>Primary</b>	
<b>Secondary</b>	

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

### Fields in the Advanced Settings menu

Field	Description
<b>Positive Cache</b>	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>
<b>Negative Cache</b>	<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>
<b>Cache Size</b>	<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. <b>Cache Size</b> is reduced by the user, dynamic entries are deleted if necessary. Statistical entries are not deleted. <b>Cache Size</b> 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>
<b>Maximum TTL for Positive Cache Entries</b>	<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 <b>Maximum TTL for Positive Cache Entries</b>.</p> <p>The default value is <i>86400</i>.</p>
<b>Maximum TTL for Negative Cache Entries</b>	<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>
<b>Fallback interface to get DNS server</b>	<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
<b>As DHCP Server</b>	<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"> <li>• <i>None</i>: No name server address is sent.</li> <li>• <i>Own IP Address</i> (default value): The address of your device is transferred as the name server address.</li> <li>• <i>DNS Setting</i>: The addresses of the global name servers entered on your device are sent.</li> </ul>
<b>As IPCP Server</b>	<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"> <li>• <i>None</i>: No name server address is sent.</li> <li>• <i>Own IP Address</i>: The address of your device is transferred as the name server address.</li> <li>• <i>DNS Setting</i> (default value): The addresses of the global name servers entered on your device are sent.</li> </ul>

## 17.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services->DNS->DNS Servers** menu.

### 17.1.2.1 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	<input checked="" type="checkbox"/> Enabled
Description	<input type="text"/>
Priority	6 ▾
Interface Mode	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic
Interface	None ▾
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 165: 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
<b>Admin Status</b>	<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>
<b>Description</b>	<p>Enter a description for DNS server.</p>
<b>Priority</b>	<p>Assign a priority to the DNS server.</p> <p>You can assign more than one pair of DNS servers (<b>Primary DNS Server</b> and <b>Secondary DNS Server</b>) 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 0 (highest priority) to 9 (lowest priority).</p> <p>The default value is 5.</p>
<b>Interface Mode</b>	<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>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Static</i></li> <li>• <i>Dynamic</i> (default value)</li> </ul>
<b>Interface</b>	<p>Select the interface to which the DNS server pair is to be assigned.</p> <p>For <b>Interface Mode</b> = <i>Dynamic</i></p> <p>A global DNS server is created with the setting <i>None</i>.</p> <p>For <b>Interface Mode</b> = <i>Static</i></p> <p>A DNS server is configured for all interfaces with the <i>Any</i> setting.</p>
<b>IP Version</b>	<p>Select the IP version used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>IPv4</i></li> <li>• <i>IPv6</i></li> </ul> <p><i>IPv4</i> is selected by default.</p>
<b>Primary IPv4 DNS Server</b>	<p>Only if <b>Interface Mode</b> = <i>Static</i></p> <p>Enter the IPv4 address of the first name server for Internet address name resolution.</p>
<b>Secondary IPv4 DNS Server</b>	<p>Only if <b>Interface Mode</b> = <i>Static</i></p> <p>Optionally, enter the IPv4 address of an alternative name server.</p>
<b>Primary IPv6 DNS Server</b>	<p>Only if <b>Interface Mode</b> = <i>Static</i></p> <p>Enter the IPv6 address of the first name server for Internet address name resolution.</p>
<b>Secondary IPv6 DNS Server</b>	<p>Only if <b>Interface Mode</b> = <i>Static</i></p> <p>Optionally, enter the IPv6 address of an alternative name server.</p>

## 17.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services->DNS->Static Hosts** menu.

### 17.1.3.1 New

Choose the **New** button to set up new static hosts.

Fig. 166: **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
<b>DNS Hostname</b>	<p>Enter the host name to which the <b>IP Address</b> 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 <b>OK</b> "&lt;Name.&gt;" after confirmation.</p> <p>Entries with spaces are not allowed.</p>
<b>Response</b>	In this entry, select the type of response to DNS requests.

Field	Description
	Possible values: <ul style="list-style-type: none"> <li>• <i>Negative</i>: A DNS request for <b>DNS Hostname</b> gets a negative response.</li> <li>• <i>Positive</i> (default value): A DNS request for <b>DNS Hostname</b> is answered with the related <b>IP Address</b>.</li> <li>• <i>None</i>: A DNS request is ignored; no answer is given.</li> </ul>
<b>IPv4 Address</b>	Only if <b>Response</b> = <i>Positive</i> Enter the IPv4 address assigned to <b>DNS Hostname</b> .
<b>IPv6 Address</b>	Only if <b>Response</b> = <i>Positive</i> Enter the IPv6 address assigned to <b>DNS Hostname</b> .

## 17.1.4 Domain Forwarding

In the **Local Services->DNS->Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

### 17.1.4.1 New

Choose the **New** button to set up additional forwardings.

The screenshot shows a navigation bar with tabs: Global Settings, DNS Servers, Static Hosts, Domain Forwarding (selected), Cache, and Statistics. Below the navigation bar is a 'Forwarding Parameters' dialog box with the following fields:

Forwarding Parameters	
Forward	<input checked="" type="radio"/> Host <input type="radio"/> Domain
Host	<input type="text"/>
Forward to	<input checked="" type="radio"/> Interface <input type="radio"/> DNS Server
Interface	Automatic ▾
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 167: **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
<b>Forward</b>	<p>Select whether requests for a host or domain are to be forwarded.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Host</i> (default value)</li> <li>• <i>Domain</i></li> </ul>
<b>Host</b>	<p>Only for <b>Forward</b> = <i>Host</i></p> <p>Enter the name of the host for which requests are to be forwarded.</p> <p>If you enter a name without a ".", the entry is supplemented with the name supplied by the value specified in <b>Local Services-&gt;DNS-&gt;Global Settings</b> for <b>Domain Name</b> as soon as you confirm with <b>OK</b>.</p>
<b>Domain</b>	<p>Only for <b>Forward</b> = <i>Domain</i></p> <p>Enter the name of the domain for which requests are to be forwarded.</p> <p>The entry can start with the wildcard "*", e.g. "*.bintec-elmeg.com".</p> <p>If you enter a name without a leading wildcard "*" a leading wildcard "*" is supplemented as soon as you confirm with <b>OK</b>.</p>
<b>Forward to</b>	<p>Select if matching DNS requests are to be forwarded to the DNS server of an <b>Interface</b> or to a manually specified <b>DNS Server</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Interface</i> (default value): Requests are forwarded to the DNS server assigned to either an automatically selected or to a user-selected interface.</li> <li>• <i>DNS Server</i>: Requests are forwarded to the specified <b>DNS Server</b>.</li> </ul>
<b>Interface</b>	<p>Only for <b>Forward to</b> = <i>Interface</i></p> <p>Select the interface that has the DNS server assigned which is to receive the DNS requests.</p>

Field	Description
<b>Primärer DNS-Server (IPv4/IPv6)</b>	Only for <b>Forward to = DNS Server</b> Enter the IPv4/IPv6 address of the primary DNS server.
<b>Sekundärer DNS-Server (IPv4/IPv6)</b>	Only for <b>Forward to = DNS Server</b> Enter the IPv4/IPv6 address of the secondary DNS server.

## 17.1.5 Dynamic Hosts

In the menu **Local Services->DNS->Dynamic Hosts**, you can find relevant information on dynamic DNS entries.

The screenshot shows the 'Dynamic Hosts' configuration page. At the top, there are navigation tabs: Global Settings, DNS Servers, Static Hosts, Domain Forwarding, Dynamic Hosts (selected), Cache, and Statistics. Below the tabs is a search and filter area with 'View 20 per page', 'Filter in None', and 'equal' dropdowns, followed by a 'Go' button. The main content area is a table with columns: Description, IPv4 Address, IPv6 Address, and Created by. The page number 'Page: 1' is shown at the bottom left. At the bottom of the page are 'OK' and 'Cancel' buttons.

Fig. 168: Local Services->DNS->Dynamic Hosts

## 17.1.6 Cache

In the **Local Services->DNS->Cache** menu, a list of all available cache entries is displayed.

The screenshot shows the 'Cache' configuration page. At the top, there are navigation tabs: Global Settings, DNS Servers, Static Hosts, Domain Forwarding, Cache (selected), and Statistics. Below the tabs is an 'Automatic Refresh Interval' set to 60 seconds with an 'Apply' button. Below that is a search and filter area with 'View 20 per page', 'Filter in None', and 'equal' dropdowns, followed by a 'Go' button. The main content area is a table with columns: Description, IPv4 Address, TTL, Response, IPv6 Address, TTL, Response, Select all/Deselect all (with a trash icon), and Make static. The page number 'Page: 1' is shown at the bottom left. At the bottom of the page are 'OK' and 'Cancel' buttons.

Fig. 169: 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.

## 17.1.7 Statistics

Global Settings
DNS Servers
Static Hosts
Domain Forwarding
Cache
Statistics

Automatic Refresh Interval  Seconds Apply

DNS Statistics	
Received DNS Packets	0
Invalid DNS Packets	0
DNS Requests	0
Cache Hits	0
Forwarded Requests	0
Cache Hitrate (%)	0
Successfully Answered Queries	0
Server Failures	0

Fig. 170: 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
<b>Received DNS Packets</b>	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
<b>Invalid DNS Packets</b>	Shows the number of invalid DNS packets received and addressed direct to your device.
<b>DNS Requests</b>	Shows the number of valid DNS requests received and addressed direct to your device.
<b>Cache Hits</b>	Shows the number of requests that were answered with static or dynamic entries from the cache.
<b>Forwarded Requests</b>	Shows the number of requests forwarded to other name servers.
<b>Cache Hitrate (%)</b>	Indicates the number of <b>Cache Hits</b> pro DNS request in percentage.
<b>Successfully Answered Queries</b>	Shows the number of successfully answered requests (positive and negative).

Field	Description
<b>Server Failures</b>	Shows the number of requests that were not answered by any name server (either positively or negatively).

## 17.2 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.

### 17.2.1 HTTPS Server

In the **Local Services->HTTPS->HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

The screenshot shows a configuration window titled "HTTPS Server". Inside, there is a section labeled "HTTPS Parameters" which contains two rows of input fields. The first row is "HTTPS TCP Port" with a text box containing the number "443". The second row is "Local Certificate" with a dropdown menu currently set to "Internal". Below these fields are two buttons: "Apply" and "Cancel".

Fig. 171: **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
<b>HTTPS TCP Port</b>	Enter the port via which the HTTPS connection is to be established.  Possible values are 0 to 65535.  The default value is 443.
<b>Local Certificate</b>	Select a certificate that you want to use for the HTTPS connection.

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Internal</i> (default value): Select this option if you want to use the certificate built into the device.</li> <li>• <i>&lt;Certificate name&gt;</i>: Under <b>System Management-&gt;Certificates-&gt;Certificate List</b> select entered certificate.</li> </ul>

## 17.3 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.

### 17.3.1 DynDNS Update

In the **Local Services->DynDNS Client->DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed

#### 17.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

DynDNS Update DynDNS Provider

Basic Parameters	
Host Name	<input type="text"/>
Interface	Select one ▾
User Name	<input type="text"/>
Password	••••••••
Provider	dyndns ▾
Enable update	<input type="checkbox"/> Enabled
Advanced Settings	
Mail Exchanger (MX)	<input type="text"/>
Wildcard	<input type="checkbox"/> Enabled
<span>OK</span> <span>Cancel</span>	

Fig. 172: 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
<b>Host Name</b>	Enter the complete host name as registered with the DynDNS provider.
<b>Interface</b>	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
<b>User Name</b>	Enter the user name as registered with the DynDNS provider.
<b>Password</b>	Enter the password as registered with the DynDNS provider.
<b>Provider</b>	<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 <b>Local Services-&gt;DynDNS Client-&gt;DynDNS Provider</b> menu.</p>

Field	Description
	The default value is <i>DynDNS</i> .
<b>Enable update</b>	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
<b>Mail Exchanger (MX)</b>	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.
<b>Wildcard</b>	Select whether forwarding of all subdomains of the <b>Host Name</b> is to be enabled for the current IP address of the <b>Interface</b> (advanced name resolution).  The function is activated by selecting <i>Enabled</i> .  The function is disabled by default.

## 17.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services->DynDNS Client->DynDNS Provider** menu.

### 17.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

DynDNS Update
DynDNS Provider

Basic Parameters	
Provider Name	<input style="width: 90%;" type="text"/>
Server	<input style="width: 90%;" type="text"/>
Update Path	<input style="width: 90%;" type="text"/>
Port	<input style="width: 90%;" type="text" value="80"/>
Protocol	<input style="width: 90%;" type="text" value="DynDNS"/> <span style="float: right;">▼</span>
Update Interval	<input style="width: 80%;" type="text" value="300"/> <span style="float: right;">Seconds</span>

OK
Cancel

Fig. 173: 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
<b>Provider Name</b>	Enter a name for this entry.
<b>Server</b>	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
<b>Update Path</b>	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.
<b>Port</b>	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 <i>80</i> .
<b>Protocol</b>	Select one of the protocols implemented.  Possible values: <ul style="list-style-type: none"> <li>• <i>DynDNS</i> (default value)</li> <li>• <i>Static DynDNS</i></li> <li>• <i>ODS</i></li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• <i>HN</i></li> <li>• <i>DYNS</i></li> <li>• <i>GnuDIP-HTML</i></li> <li>• <i>GnuDIP-TCP</i></li> <li>• <i>Custom DynDNS</i></li> <li>• <i>DnsExit</i></li> </ul>
<b>Update Interval</b>	<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>

## 17.4 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.

### 17.4.1 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.

### 17.4.1.1 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	<input style="width: 90%;" type="text"/>
IP Address Range	<input style="width: 45%;" type="text"/> - <input style="width: 45%;" type="text"/>
DNS Server	Primary <input style="width: 60%;" type="text"/>
	Secondary <input style="width: 60%;" type="text"/>
<input type="button" value="OK"/> <input style="margin-left: 50px;" type="button" value="Cancel"/>	

Fig. 174: Local Services->DHCP Server->IP Pool Configuration->New

#### Fields in the menu Basic Parameters

Field	Description
<b>IP Pool Name</b>	Enter any description to uniquely identify the IP pool.
<b>IP Address Range</b>	Enter the first (first field) and last (second field) IP address of the IP address pool.
<b>DNS Server</b>	<p><b>Primary:</b> Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.</p> <p><b>Secondary:</b> Optionally, enter the IP address of an alternative DNS server.</p>

### 17.4.2 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 DHCP 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.

**17.4.2.1 Edit or New**

Choose the **New** button to set up new DHCP 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	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%; padding: 2px;">Option</th> <th style="width: 40%; padding: 2px;">Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center; padding: 5px;"><span style="border: 1px solid black; border-radius: 5px; padding: 2px 10px;">Add</span></td> </tr> </tbody> </table>	Option	Value	<span style="border: 1px solid black; border-radius: 5px; padding: 2px 10px;">Add</span>	
Option	Value				
<span style="border: 1px solid black; border-radius: 5px; padding: 2px 10px;">Add</span>					
<span style="border: 1px solid black; border-radius: 15px; padding: 5px 15px; margin: 0 10px;">OK</span> <span style="border: 1px solid black; border-radius: 15px; padding: 5px 15px; margin: 0 10px;">Cancel</span>					

Fig. 175: 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
<b>Interface</b>	<p>Select the interface over which the addresses defined in <b>IP Pool Name</b> are to be assigned to DHCP clients.</p> <p>When a DHCP request is received over this <b>Interface</b>, one of the addresses from the address pool is assigned.</p>
<b>IP Pool Name</b>	<p>Select an IP pool name configured in the <b>Local Services-&gt;DHCP Server-&gt;IP Pool Configuration</b> menu.</p>

Field	Description
<b>Pool Usage</b>	<p>Select if the DHCP pool is to be used for requests from clients in a network directly connected to an Ethernet interface, or if it is to be used for DHCP requests from a remote network that are sent to your device via a DHCP relay station.</p> <p>In the second case, it is possible to use an IP address pool for the remote network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Local</i> (default value): The DHCP pool is only used for DHCP requests from a network directly connected to an Ethernet interface.</li> <li>• <i>Relay</i>: The DHCP pool is only used for DHCP requests forwarded from remote networks.</li> <li>• <i>Local/Relay</i>: The DHCP pool can be used for both kinds of requests.</li> </ul>

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


#### Fields in the menu **Advanced Settings**

Field	Description
<b>Gateway</b>	<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"> <li>• <i>Use router as gateway</i> (default value): Here, the IP address defined for the <b>Interface</b> is transferred.</li> <li>• <i>No gateway</i>: No IP address is sent.</li> <li>• <i>Specify</i>: Enter the corresponding IP address.</li> </ul>
<b>Lease Time</b>	<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 <b>Lease Time</b> expires, the address can be reassigned by the server.</p> <p>The default value is <i>120</i>.</p>
<b>DHCP Options</b>	Specify which additional data is forwarded to the DHCP client.

Field	Description
	<p>Possible values for <b>Option</b>:</p> <ul style="list-style-type: none"> <li>• <i>Time Server</i> (default value): Enter the IP address of the time server to be sent to the client.</li> <li>• <i>DNS Server</i>: Enter the IP address of the DNS server to be sent to the client.</li> <li>• <i>DNS Domain Name</i>: Enter the DNS domain to be sent to the client.</li> <li>• <i>WINS/NBNS Server</i>: Enter the IP address of the WINS/NBNS server to be sent to the client.</li> <li>• <i>WINS/NBT Node Type</i>: Select the type of the WINS/NBT node to be sent to the client.</li> <li>• <i>TFTP Server</i>: Enter the IP address of the TFTP server to be sent to the client.</li> <li>• <i>CAPWAP Controller</i>: Enter the IP address of the CAPWAP controller to be sent to the client.</li> <li>• <i>URL (provisioning server)</i>: This option enables you to send a client any URL.</li> </ul> <p>Use this option to send querying <b>IP1x0</b> 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://&lt;IP address of the provisioning server&gt;/eg_prov</i>.</p> <ul style="list-style-type: none"> <li>• <i>Vendor Group</i> (Vendor Specific Information): This enables you to send the client any manufacturer-specific information in any text string.</li> <li>• <i>Vendor String</i>: With this option, the configuration parameters (e. g. PIN and the SIM card's access point name (APN)) can be transferable.</li> </ul> <p>Several entries are possible. Add additional entries with the <b>Add</b> button.</p>

### Vendor Group

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
<b>Select vendor</b>	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server.  Possible values: <ul style="list-style-type: none"> <li>• <i>Siemens</i> (default value)</li> <li>• <i>Other</i></li> </ul>
<b>Provisioning Server</b>	Only für <b>Select vendor</b> = <i>Siemens</i>  Enter which manufacturer value shall be transmitted.  For the setting <b>Select vendor</b> = <i>Siemens</i> , the default value <i>sdlp</i> is displayed.  You can complete the IP address of the desired server.
<b>Vendor Description</b>	Only für <b>Select vendor</b> = <i>Other</i>  Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
<b>Custom DHCP Options</b>	Only für <b>Select vendor</b> = <i>Other</i>  Use <b>Add</b> to add more entries.  You can add custom DHCP options.

#### Vendor String

Go to the menu **Local Services->DHCP Server->DHCP Configuration->Advanced Settings**, proceed as follows in order to specify the respective parameter:

Click the **Add** button in the **DHCP Options** field and choose **Option** = *Vendor String*.  
Click the  button to edit the entry.

#### Fields in the Basic Parameters menu

Field	Description
<b>Select vendor</b>	Here, you can select for which manufacturer specific values

Field	Description
	shall be transmitted for the DHCP server.  Possible values: <ul style="list-style-type: none"> <li>• <i>Other</i> (default value)</li> <li>• <i>-bintec-</i></li> </ul>
<b>APN</b>	Only für <b>Select vendor</b> = <i>-bintec-</i>  Enter the Access Point Namen (APN) of the SIM card.
<b>PIN</b>	Only für <b>Select vendor</b> = <i>-bintec-</i>  Enter the PIN of the SIM card.
<b>Vendor Description</b>	Only für <b>Select vendor</b> = <i>Other</i>  Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
<b>Vendor Option String</b>	Only für <b>Select vendor</b> = <i>Other</i>  Enter the manufacturer specific configuration parameters.

### 17.4.3 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**, and in the **Local Services->DHCP Server->IP Pool Configuration** menu is assigned a valid IP Pool.

### 17.4.3.1 New

Choose the **New** button to set up new IP/MAC bindings.

The screenshot shows a configuration window with four tabs: "IP Pool Configuration", "DHCP Configuration", "IP/MAC Binding" (which is selected), and "DHCP Relay Settings". Below the tabs is a "Basic Parameters" section containing three input fields: "Description", "IP Address", and "MAC Address". At the bottom of the window are two buttons: "OK" and "Cancel".

Fig. 176: 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
<b>Description</b>	Enter the name of the host to which the <b>MAC Address</b> the <b>IP Address</b> is to be bound.  A character string of up to 256 characters is possible.
<b>IP Address</b>	Enter the IP address to be assigned to the MAC address specified in <b>MAC Address</b> is to be assigned.
<b>MAC Address</b>	Enter the MAC address to which the IP address specified in <b>IP Address</b> is to be assigned.

### 17.4.4 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.



Basic Parameters	
Primary DHCP Server	0.0.0.0
Secondary DHCP Server	0.0.0.0

OK Cancel

Fig. 177: 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.

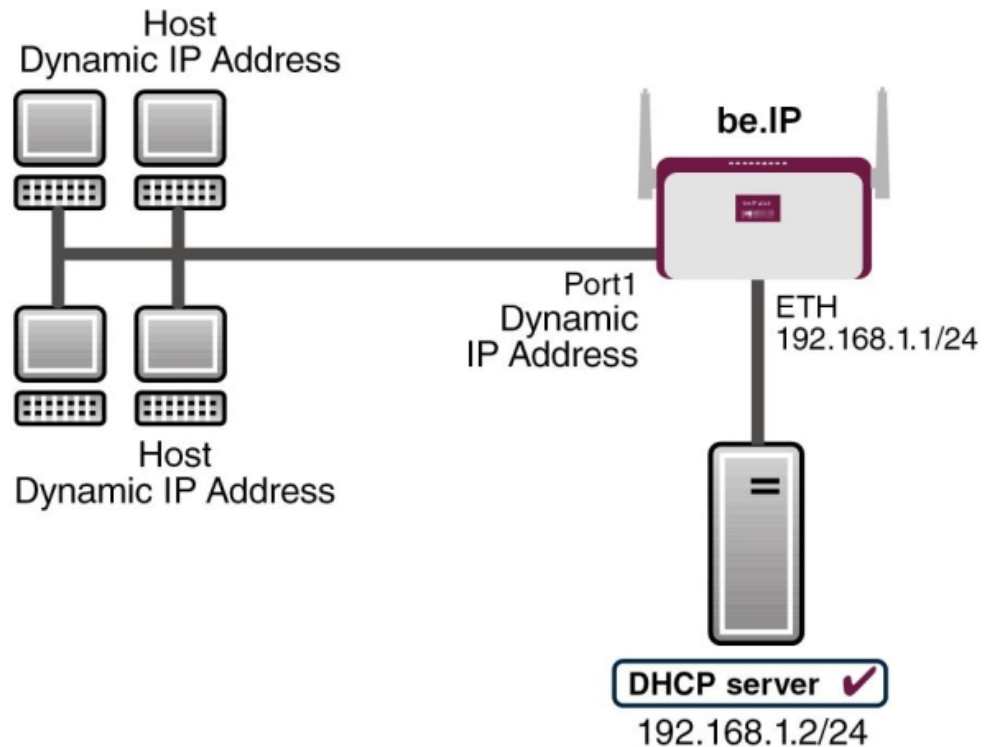
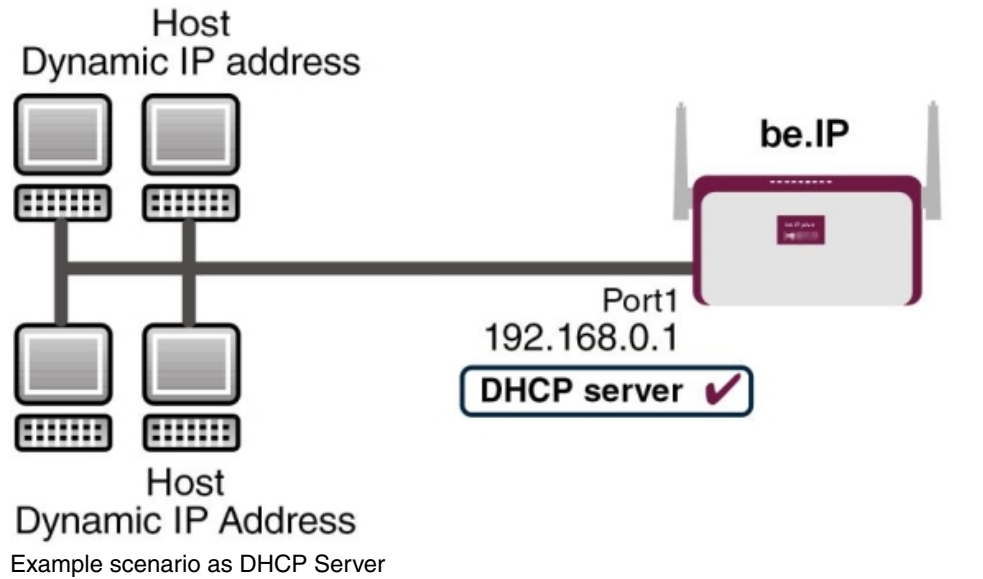
Field	Description
<b>Primary DHCP Server</b>	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded.  The default value is 0 . 0 . 0 . 0.
<b>Secondary DHCP Server</b>	Enter the IP address of an alternative BootP or DHCP server.  The default value is 0 . 0 . 0 . 0.

## 17.4.5 DHCP - Configuration example

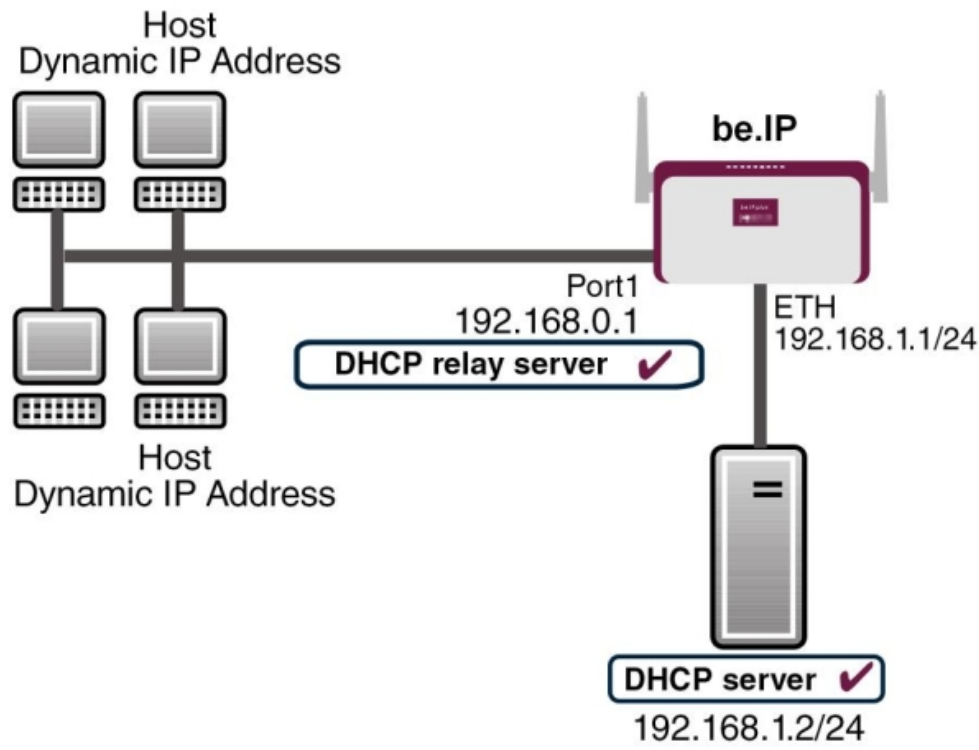
### Requirements

- An optional DHCP server

### Example scenaria



Example scenario as DHCP Client



Example scenario as DHCP Relay Server

### Configuration target

You can use your device as a DHCP server, DHCP client or DHCP relay agent.



### Overview of Configuration Steps

#### DHCP Server

Field	Menu	Value
IP Pool Name	Local Services->DHCP Server->IP Pool Configuration->New	e.g. <i>IP-Pool-1</i>
IP Address Range	Local Services->DHCP Server->IP Pool Configuration->New	e.g. <i>192.168.0.2</i> and <i>192.168.0.10</i>
Interface	Local Services->DHCP Server->DHCP Configuration->New	e.g. <i>en1-0</i>
IP Pool Name	Local Services->DHCP Server->DHCP Configuration->New	<i>IP-Pool-1</i>
Pool Usage	Local Services->DHCP Server->DH-	<i>Local</i>

Field	Menu	Value
	<b>CP Configuration-&gt;New</b>	
<b>Gateway</b>	<b>Local Services-&gt;DHCP Server-&gt;DH-CP Configuration-&gt;New-&gt;Ad- vanced Settings</b>	<i>Use Router as Gateway</i>
<b>Lease Time</b>	<b>Local Services-&gt;DHCP Server-&gt;DH-CP Configuration-&gt;New-&gt;Ad- vanced Settings</b>	e.g. <i>120</i>
<b>IP address to use for DNS/WINS server as- signment</b>	<b>Local Services-&gt;DNS-&gt;Global Set- tings-&gt;Advanced Settings</b>	e.g. <i>Own IP address</i>

#### DHCP Client

Field	Menu	Value
<b>Address Mode</b>	<b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt; &lt;en1-4&gt;-&gt; </b>	<i>DHCP</i>
<b>DHCP MAC Address (optional)</b>	<b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt; &lt;en1-4&gt; -&gt; -&gt;Advanced Set- tings</b>	MAC address for a spec- ific DHCP server

#### DHCP Relay Server

Field	Menu	Value
<b>Primary DHCP Server</b>	<b>Local Services-&gt;DHCP Server-&gt;DH-CP Relay Settings</b>	e.g. <i>192.168.1.2</i>
<b>Secondary DHCP Serv- er (optional)</b>	<b>Local Services-&gt;DHCP Server-&gt;DH-CP Relay Settings</b>	if one exists

## 17.5 DHCPv6 Server

You can operate your device as a DHCPv6 server. The DHCPv6 server can either assign IP addresses as well as DHCPv6 options or DHCPv6 options only without any addresses. These parameters are collected in a so called "Option Set". An option set can be linked to an interface (see **Local Services->DHCPv6 Server->DHCPv6 Server->New**), or it can be configured globally (see **Local Services->DHCPv6 Server->DHCPv6 Global Options->New**). DHCP options can, e.g., contain information about DNS or time servers.



### Note

An IPv6 address pool is created by assigning an IPv6 Link Prefix (a subnet with a length of /64) to a DHCPv6 option set. The definition of a separate set of IP addresses like, e.g. fc00:1:2:3::1..fc00:1:2:3::100, is - in contrast with IPv4 - not specified for IPv6.

The following requirements must be met for the configuration of an IPV6 address pool:


- (a) IPv6 has to be activated for the respective interface.
- (b) An IPv6 Link Prefix (subnet) with a length of /64 has to be configured for the respective interface. An IPv6 link prefix can be defined in either of two ways:
  - The IPv6 Link Prefix is derived from a General IPv6 Prefix (a prefix with a length of, e.g., /56 or /48). In this case, the General IPv6 Prefix has to be configured in the menu **Networking->IPv6 General Prefixes->General Prefix Configuration** .
  - The IPv6 Link Prefix with a length of /64 is manually configured for the respective interface and is not derived from a General IPv6 Prefix.
- (c) The **DHCP Server** option has to be enabled for the interface.

Moreover, the following settings are recommended:

- The options **Preferred Lifetime** and **Valid Lifetime** should be set to values higher than the value configured for the option **Router Lifetime**.

With a **Router Lifetime** of 600 seconds a **Preferred Lifetime** of, e.g., 900 seconds and a **Valid Lifetime** of 1800 seconds are reasonable settings.

- The option **DHCP Mode** should be enabled.

In order to make the settings mentioned above, go to the menu **LAN->IP Configuration->Interfaces**. Choose the intended interface with the  icon. Activate IPv6 and set the **IPv6 Mode** to *Router (Transmit Router Advertisement)*. In the field **IPv6-Adressen**, click **Hinzufügen** and configure the Link Prefix. Confirm your configuration with **Accept**. The configuration of the recommended settings is then carried out in the following menus:

- **Router Lifetime:** **LAN->IP Configuration->Interfaces->New->Advanced Settings->Advanced IPv6 Settings**
- **Preferred Lifetime** and **Valid Lifetime:** **LAN->IP Configuration->Interfaces->New->Basic IPv6 Parameters->Add->Advanced**

## 17.5.1 DHCPv6 Server

Here you can create interface-related address pools and define DHCP options inside of an DHCP Option Set.

### 17.5.1.1 Edit or New



Use the **New** button in order to create an Option Set. Use the  icon in order to edit an existing entry.

Fig. 178: Local Services->DHCPv6 Server->DHCPv6 Server

The menu consists of the following fields:

#### Fields in the menu Basic Parameters

Field	Description
<b>Name</b>	Enter a name for the Option Set.
<b>Interface</b>	<p>Select the IPv6 interface the Option Set is assigned to.</p> <p>You can choose from interfaces with the following configuration:</p> <ul style="list-style-type: none"> <li>• IPv6 is enabled.</li> <li>• The option <b>DHCP Server</b> is enabled.</li> </ul> <p>In the ex works state, IPv6 is disabled for all interfaces. If the in-</p>


Field	Description
	tended interface is not offered for selection, configure it according to the requirements detailed in the introduction of this section. Configuration is done on the menu <b>LAN-&gt;IP Configuration-&gt;Interfaces</b> .
<b>Address assignment</b>	<p>The definition of an IPv6 address pools is carried out by assigning an IPv6 Link Prefix (subnet with a length of /64) to a DHCPv6 Option Set. The IPv6 address pool always comprises the complete 64 Bit address space of the selected IPv6 Link Prefix. Address assignment is random.</p> <p>Use <b>Add</b> to assign one or more IPv6 Link Prefixes to the IPv6 Option Set.</p>
	<p> <b>Note</b></p> <p>Note that only such IPv6 Link Prefixes are available for selection that are assigned to the selected interface.</p>

#### Fields in the menu **Server Options**

Field	Description
<b>DNS domains search list</b>	Use <b>Add</b> to create a list of domain names which is queried by the client during name resolution (DHCPv6 Option 24 "Domain Search List"). Domain names will be transmitted to the clients in the order defined by the list.

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

#### Fields in the menu **Advanced Server Options**

Field	Description
<b>DNS Server</b>	<p>Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server").</p> <p>Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field <b>DNS Propagation</b> in the menu <b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt;</b>  <b>-&gt;Advanced Settings</b> if <b>IPv6 = Enabled</b>.)</p> <p>You can also manually specify DNS servers and have them</p>

Field	Description
	propagated to the clients. To do this disable the option <b>Use RA or Global Fallback DNS Server</b> and create the desired DNS server entries using <b>Add</b> .
<b>SNTP Server</b>	Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Use <b>Add</b> to create the desired time server entries.

## 17.5.2 DHCPv6 Global Options

In this menu, you can configure those DHCPv6 options which are globally valid for the DHCPv6 server. An option that has been configured here will be propagated if there is no more specific definition is available (e.g., no interface- or vendor-ID-specific definition).

Fig. 179: Local Services->DHCPv6 Server->DHCPv6 Global Options

The menu consist of the following fields:

### Fields in the menu Basic Parameters

Field	Description
<b>DNS domains search list</b>	Use <b>Add</b> to create a list of domain names which is queried by the client during name resolution (DHCPv6 Option 24 "Domain Search List"). Domain names will be transmitted to the clients in the order defined by the list. The domain name (e.g. dev.bintec.de.) mast end with a dot (.).


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



### Fields in the menu **Server preference**

Field	Description
<b>Server preference</b>	<p>The DHCPv6 advertisements sent by the DHCPv6 server to the clients may contain the DHCPv6 option 7 "Preference".</p> <p>Possible values are <code>0 . . . 255</code>.</p> <p>In a network with multiple DHCPv6 servers this option controls which server takes the highest priority. If a client receives DHCPv6 advertisements with different priorities from different servers, it will usually accept the parameters from the highest priority server. The client can, however, also accept DHCPv6 advertisements with a lower priority if the set of parameters in the advertisement provides more of the options requested by the client.</p> <p>A value of <code>0</code> means "not specified" (lowest priority), <code>255</code> denotes the highest priority.</p>

### Fields in the menu **Advanced Server Fallback Options**

Field	Description
<b>DNS Server</b>	<p>Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server").</p> <p>Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field <b>DNS Propagation</b> in the menu <b>LAN-&gt;IP Configuration-&gt;Interfaces-&gt;</b>  <b>-&gt;Advanced Settings</b> if <b>IPv6 = Enabled</b>.)</p> <p>You can also manually specify DNS servers and have them propagated to the clients. To do this disable the option <b>Use RA or Global Fallback DNS Server</b> and create the desired DNS server entries using <b>Add</b>.</p>
<b>SNTP Server</b>	<p>Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Use <b>Add</b> to create the desired time server entries.</p>

## 17.5.3 Stateful Clients

Here you see an entry for each Stateful Client that has contacted the server and has been assigned an IPv6 address.

Fig. 180: Local Services->DHCPv6 Server->Stateful Clients

## 17.5.4 Stateful Clients Configuration

During a stateful configuration of IPv6 clients not only the DHCP options, but also the IPv6 prefix is transmitted to the client.

### 17.5.4.1 Edit or New


Use **New** to create entries for Stateful Clients. Normally, you do not have to create any entries. Use  in order to edit existing entries. You should check each automatically created entry once to verify the settings and adjust them if required.

Fig. 181: Local Services->DHCPv6 Server->Stateful Clients Configuration+New

The menu consists of the following fields.

#### Fields in the menu Basic Parameters

Field	Description
<b>DUID</b>	<p>Clients use the <b>DUID field</b> (DHCP Unique Identifier) in order to identify themselves and request an IP address from the DHCPv6 server.</p> <p>If you create an entry using <b>New</b> you can specify the <b>DUID</b> as a</p>

Field	Description
	16 - 20 digit HEX number. You can enter them using a "-" (minus) as separator (Windows style), or you can enter them in a single block (Linux style).
<b>Accept Client FQDN</b>	If <b>Accept Client FQDN</b> is enabled, the client is entered into the cache of the Domain Name Server with the parameter FQDN (Fully Qualified Domain Name).
<b>Administrative FQDNs</b>	With <b>Add</b> , you can specify an FQDN (Fully Qualified Domain Name) - even for automatically created entries.
<b>Static Interface Identifier</b>	The field <b>Static Interface Identifier</b> is the host portion of the IPv6 address, i.e., the last 64 Bit of the IP address. This prefix must start with ::.

## 17.6 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](http://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.

## 17.6.1 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	<input checked="" type="checkbox"/> Enabled
Filtered Input Interface(s):	<input type="button" value="Add"/>
Maximum Number of History Entries	<input type="text" value="64"/>
URL Path Depth	<input type="text" value="1"/> <input type="button" value="v"/>
Action if server not reachable	<input checked="" type="radio"/> Allow all <input type="radio"/> Block all <input type="radio"/> Log all
Action if license not registered	<input checked="" type="radio"/> Allow all <input type="radio"/> Block all <input type="radio"/> Log all

**License Information**

Licence Key	<input type="text" value="B1BT"/> <span style="float: right; font-size: small;">[Activate 30 days demo licence]</span>
Licence Status	
<div style="border: 1px solid #ccc; width: 100%; height: 100%; background-color: #f2f2f2;"></div>	
Licence valid until	Not activated

Fig. 182: 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
<b>Web Filter Status</b>	<p>Activate or deactivate the filter.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>Filtered Input Interface(s)</b>	Select for which of the existing Ethernet and WLAN interfaces web filtering is to be activated.

Field	Description
	Press the <b>Add</b> button to add more interfaces. The requests from http Internet pages that reach your device via these interfaces are then monitored by web filtering.
<b>Maximum Number of History Entries</b>	<p>Define the number of entries to be saved in the web filtering history (<b>History</b> menu).</p> <p>Possible values are <i>1</i> to <i>512</i>.</p> <p>The default value is <i>64</i>.</p>
<b>URL Path Depth</b>	Select the path length to which a URL is to be checked by the Cobion Orange Filter.
<b>Action if server not reachable</b>	<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"> <li>• <i>Allow all</i> (default value): Callup is permitted.</li> <li>• <i>Block all</i>: Callup of the requested page is blocked.</li> <li>• <i>Log all</i>: Callup is permitted, but logged.</li> </ul>
<b>Action if license not registered</b>	<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"> <li>• <i>Allow all</i> (default value): Callup is permitted.</li> <li>• <i>Block all</i>: Callup of the requested page is blocked.</li> <li>• <i>Log all</i>: Callup is permitted, but logged.</li> </ul>

The menu **License Information** consists of the following fields:

#### Fields in the License Information menu.

Field	Description
<b>Licence Key</b>	<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 <b>Activate 30 days demo licence</b></p>

Field	Description
<b>Licence Status</b>	Shows the result of the last validity check of the licence. The validity of the licence is checked every 23 hours.
<b>License valid until</b>	This shows the expiry date of the licence (relative to the time set on your device) and cannot be edited.

## 17.6.2 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).

### 17.6.2.1 New

Choose the **New** button to create additional filters.

The screenshot shows a configuration window with a tabbed interface. The 'Filter List' tab is active. Below the tabs is a 'Filter Parameters' section with the following fields:

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

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Fig. 183: **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
<b>Category</b>	<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"> <li>• <i>Default behaviour</i>: This category applies to all Internet addresses.</li> <li>• <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.</li> <li>• <i>Unknown URL</i>: If an address is not known to the Proventia Web Filter, the action associated with this category is used.</li> </ul>
<b>Day</b>	<p>Select the days on which the filter is to be active.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> <li>• <i>Everyday</i> (default value): The filter is used every day of the week.</li> <li>• <i>&lt;Weekday&gt;</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.</li> <li>• <i>Monday-Friday</i>: The filter is used from Monday to Friday.</li> </ul> <p>The default value is <i>Everyday</i>.</p>
<b>Schedule (Start / Stop Time)</b>	<p>In <b>From</b>, 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 <b>to</b> in the field. The time is entered in the form hh:mm. The default value is 00:00 to 23:59.</p>
<b>Action</b>	<p>Select the action to be executed if the filter matches a call.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Block and Log</i> (default value): The call of the requested page is prevented and logged.</li> <li>• <i>Allow and Log</i>: Callup is permitted, but logged. You can view the logged events in the <b>Local Services-&gt;Web Filter-&gt;Filter List</b> menu.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li><i>Allow</i>: Callup is allowed and not logged.</li> </ul>

### 17.6.3 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.

Fig. 184: **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
<b>URL / IP Address</b>	You enter a URL or IP address. The length of the entry is limited to 60 characters.
<b>Blacklisted</b> <b>Whitelisted</b>	<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>



## 17.6.4 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.

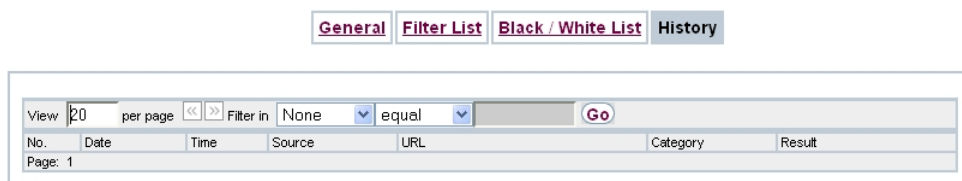


Fig. 185: **Local Services->Web Filter->History**

## 17.7 CAPI Server

You can use the CAPI Server function to assign user names and passwords to users of the CAPI applications on your device. This makes sure that only authorised users can receive incoming calls and make outgoing calls via CAPI.

The CAPI service allows connection of incoming and outgoing data and voice calls to communications applications on hosts in the LAN that access the Remote CAPI interface of your device. This enables, for example, hosts connected to your device to receive and send faxes.



### Note

All incoming calls to the CAPI are offered to all registered and "eavesdropping" CAPI applications in the LAN.

In the ex works state, a user with the user name *default* and no password is entered for the CAPI subsystem.

Once you've created your intended users with password, you should delete the *default* user without password.

### 17.7.1 User

A list of all configured CAPI users is displayed in the **Local Services->CAPI Server->User** menu.

### 17.7.1.1 New

Choose the **New** button to set up new CAPI users.

The screenshot shows a dialog box titled 'User' with two tabs: 'User' and 'Options'. The 'User' tab is active and contains a 'Basic Parameters' section. This section has three rows: 'User Name' with an empty text input field, 'Password' with a masked input field (represented by dots), and 'Access' with a checked checkbox labeled 'Enabled'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Fig. 186: **Local Services->CAPI Server->User->New**

The menu **Local Services->CAPI Server->User->New** consists of the following fields:

#### Fields in the **Basic Parameters** menu.

Field	Description
<b>User Name</b>	Enter the user name for which access to the CAPI service is to be allowed or denied.
<b>Password</b>	Enter the password which the user <b>User Name</b> shall use for identification to gain access to the CAPI service.
<b>Access</b>	<p>Select whether access to the CAPI service is to be permitted or denied for the user.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>

## 17.7.2 Options

Basic Parameters	
Enable server	<input checked="" type="checkbox"/> Enabled
Faxheader	<input type="checkbox"/> Enabled
CAPI Server TCP Port	2662

Fig. 187: Local Services->CAPI Server->Options

The menu **Local Services->CAPI Server->Options** consists of the following fields:

### Fields in the Basic Parameters menu.

Field	Description
<b>Enable server</b>	<p>Select whether your device is to be enabled as a CAPI server.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is enabled by default.</p>
<b>Faxheader</b>	<p>Only for devices the <b>RTxxx2</b> series.</p> <p>Select whether the fax header should be printed at the top of outgoing faxes.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
<b>CAPI Server TCP Port</b>	<p>The field can only be edited if <b>Enable server</b> is enabled.</p> <p>Enter the TCP port number for remote CAPI connections.</p> <p>The default value is <i>2662</i>.</p>

## 17.8 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 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.

### 17.8.1 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.

### 17.8.1.1 New

Choose the **New** button to create more event lists.

Trigger Actions Options

Basic Parameters									
Event List	New ▾								
Description	<input type="text"/>								
Event Type	Time ▾								
Select time interval									
Time Condition	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">Condition Type</th> <th style="width: 50%;">Condition Settings</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/> Weekday</td> <td>Monday ▾</td> </tr> <tr> <td><input checked="" type="radio"/> Periods</td> <td>Daily ▾</td> </tr> <tr> <td><input type="radio"/> Day of Month</td> <td>1 ▾</td> </tr> </tbody> </table>	Condition Type	Condition Settings	<input type="radio"/> Weekday	Monday ▾	<input checked="" type="radio"/> Periods	Daily ▾	<input type="radio"/> Day of Month	1 ▾
Condition Type	Condition Settings								
<input type="radio"/> Weekday	Monday ▾								
<input checked="" type="radio"/> Periods	Daily ▾								
<input type="radio"/> Day of Month	1 ▾								
Start Time	Hour <input type="text"/> Minute <input type="text"/>								
Stop Time	Hour <input type="text"/> Minute <input type="text"/>								
<span>OK</span> <span>Cancel</span>									

Fig. 188: 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
<b>Event List</b>	<p>You can create a new event list with <i>New</i> (default value). You give this list a name with <b>Description</b>. You use the remaining parameters to create the first event in the list.</p> <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>
<b>Description</b>	<p>Only for <b>Event List</b> = <i>New</i></p> <p>Enter your chosen designation for the event list.</p>
<b>Event Type</b>	<p>Select the type of event.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Time</i> (default value): The operations configured and assigned in <b>Actions</b> are initiated at specific points in time.</li> <li>• <i>MIB/SNMP</i>: The actions configured and assigned in <b>Actions</b> are initiated when the defined MIB variables assumes the assigned values.</li> <li>• <i>Interface Status</i>: Operations configured and assigned in <b>Actions</b> are initiated, when the defined interfaces take on a specified status.</li> <li>• <i>Interface Traffic</i>: The operations configured and assigned in <b>Actions</b> are triggered if the data traffic on the specified interfaces falls below or exceed the defined value.</li> <li>• <i>Ping Test</i>: the operations configured and assigned in <b>Actions</b> are triggered if the defined IP address is accessible or not accessible.</li> <li>• <i>Certificate Lifetime</i>: Operations configured and assigned in <b>Actions</b> are initiated when the defined period of validity is reached.</li> <li>• <i>Function Button</i> (not available on all devices): The option <i>Function Button</i> determines that pushing the function button on the device can serve as a trigger for any configured action. Pushing the button for approx. one second (but less than three seconds) sets the button status to <i>Active</i>, pushing it for more than three seconds sets it to <i>Inactive</i>. Actions depending on the state of the button are then carried out after the next cyclical query determined by the <b>Schedule Interval</b>. In this way, e.g., a WLAN interface can be activated when the button is pushed for a second. Pushing the button for more than three seconds deactivates the interface again.</li> <li>• <i>GEO Zone Status</i>: Operations configured and assigned in <b>Actions</b> are initiated, when the defined <b>GEO Zones</b> take on a specified status.</li> </ul>
<b>Monitored GEO Zone</b>	<p>Only for <b>Event Type</b> <i>GEO Zone Status</i></p> <p>Select a GEO zone configured in the <b>Physical Interfaces</b> menu.</p>
<b>GEO Zone Status</b>	<p>Only for <b>Event Type</b> <i>GEO Zone Status</i></p>

Field	Description
	<p>Select the <b>GEO Zone Status</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>True</i>: The current position lies within the defined zone.</li> <li>• <i>False</i>: The current position lies outside the defined zone.</li> </ul>
<b>Monitored Variable</b>	<p>Only for <b>Event Type</b> <i>MIB/SNMP</i></p> <p>Select the MIB variable whose defined value is to be configured as initiator. First, select the <b>System</b> in which the MIB variable is saved, then the <b>MIB Table</b> and finally the <b>MIB Variable</b> itself. Only the MIB tables and MIB variables present in the respective area are displayed.</p>
<b>Compare Condition</b>	<p>Only for <b>Event Type</b> <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>
<b>Compare Value</b>	<p>Only for <b>Event Type</b> <i>MIB/SNMP</i></p> <p>Enter the value of the MIB variable.</p>
<b>Index Variables</b>	<p>Only for <b>Event Type</b> <i>MIB/SNMP</i></p> <p>Where required, select MIB variables to uniquely identify a specific data set in the <b>MIB Table</b>, e.g. <i>ConnIfIndex</i>. The unique identification of a particular table entry is derived from the combination of <b>Index Variable</b> (usually an index variable which is flagged with *) and <b>Index Value</b>.</p> <p>Use <b>Index Variables</b> to create more entries with <b>Add</b>.</p>
<b>Monitored Interface</b>	<p>Only for <b>Event Type</b> <i>Interface Status</i> and <i>Interface Traffic</i></p> <p>Select the interface whose defined status shall trigger an operation.</p>
<b>Interface Status</b>	<p>Only for <b>Event Type</b> <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"> <li>• <i>Up</i> (default value): The function is enabled.</li> <li>• <i>Down</i>: The interface is disabled.</li> </ul>
<b>Traffic Direction</b>	<p>Only for <b>Event Type</b> <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"> <li>• <i>RX</i> (default value): Incoming data traffic is monitored.</li> <li>• <i>TX</i>: Outgoing data traffic is monitored.</li> </ul>
<b>Interface Traffic Condition</b>	<p>Only for <b>Event Type</b> <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>
<b>Transferred Traffic</b>	<p>Only for <b>Event Type</b> <i>Interface Traffic</i></p> <p>Enter the desired value in <b>kBytes</b> for the data traffic to serve as comparison.</p> <p>The default value is <i>0</i>.</p>
<b>Destination IP Address</b>	<p>Only for <b>Event Type</b> <i>Ping Test</i></p> <p>Enter the IP address whose accessibility is to be checked.</p>
<b>Source IP Address</b>	<p>Only for <b>Event Type</b> <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"> <li>• <i>Automatic</i> (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address.</li> <li>• <i>Specific</i>: Enter the desired IP address in the input field.</li> </ul>



Field	Description
<b>Status</b>	<p>Only for <b>Event Type</b> <i>Ping Test</i></p> <p>Select whether <b>Destination IP Address</b> <i>Reachable</i> must be (default value) or <i>Unreachable</i> in order to initiate the operation.</p>
<b>Interval</b>	<p>Only for <b>Event Type</b> <i>Ping Test</i></p> <p>Enter the time in <b>Seconds</b> after which a ping must be resent.</p> <p>The default value is <i>60</i> seconds.</p>
<b>Successful Trials</b>	<p>Only for <b>Event Type</b> <i>Ping Test</i></p> <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 <i>1</i> to <i>65536</i>.</p> <p>The default value is <i>3</i>.</p>
<b>Unsuccessful Trials</b>	<p>Only for <b>Event Type</b> <i>Ping Test</i></p> <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 used.</p> <p>Possible values are <i>1</i> to <i>65536</i>.</p> <p>The default value is <i>3</i>.</p>
<b>Monitored Certificate</b>	<p>Only for <b>Event Type</b> <i>Certificate Lifetime</i></p> <p>Select the certificate whose validity should be checked.</p>
<b>Remaining Validity</b>	<p>Only for <b>Event Type</b> <i>Certificate Lifetime</i></p> <p>Enter the desired value for the remaining validity of the certificate in percentage.</p>

Field	Description
<b>Function Button Status</b>	<p>Only for <b>Event Type</b> <i>Function Button</i>.</p> <p>When creating the trigger the dropdown selection <b>Function Button Status</b> allows you to choose which status of the function button activates or deactivates the trigger. If you set the status to <i>On</i>, the trigger becomes active if the status of the function button is <i>Active</i>, and inactive, if the state of the function button is <i>Inactive</i>. If you set it to <i>Off</i>, the trigger becomes active if the state of the function button is <i>Inactive</i>, and inactive if the state of the function button is <i>Active</i>. The current state is checked cyclically at the configured schedule interval.</p>

#### Fields in the menu **Select time interval**

Field	Description
<b>Time Condition</b>	<p>For <b>Event Type</b> <i>Time</i> only</p> <p>First select the type of time entry in <b>Condition Type</b>.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Weekday</i>: Select a weekday in <b>Condition Settings</b>.</li> <li>• <i>Periods</i> (default value): In <b>Condition Settings</b>, select a particular period.</li> <li>• <i>Day of Month</i>: Select a specific day of the month in <b>Condition Settings</b>.</li> </ul> <p>Possible values for <b>Condition Settings</b> in <b>Condition Type</b> = <i>Weekday</i>:</p> <p><i>Monday</i> (default value) ... <i>Sunday</i>.</p> <p>Possible values for <b>Condition Settings</b> in <b>Condition Type</b> = <i>Periods</i>:</p> <ul style="list-style-type: none"> <li>• <i>Daily</i>: The initiator becomes active daily (default value).</li> <li>• <i>Monday-Friday</i>: The initiator becomes active daily from Monday to Friday.</li> <li>• <i>Monday - Saturday</i>: The initiator becomes active daily from Monday to Saturday.</li> <li>• <i>Saturday - Sunday</i>: The initiator becomes active on Saturdays and Sundays.</li> </ul>

Field	Description
	Possible values for <b>Condition Settings</b> in <b>Condition Type = Day of Month</b> :  1... 31.
<b>Start Time</b>	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.
<b>Stop Time</b>	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 <b>Stop Time</b> or set a <b>Stop Time = Start Time</b> , the initiator is activated, and deactivated after 10 seconds.

## 17.8.2 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**.

### 17.8.2.1 New

Choose the **New** button to configure additional operations.

Trigger Actions Options

Basic Parameters	
Description	<input type="text"/>
Command Type	Reboot <span style="float: right;">▼</span>
Event List	Select one <span style="float: right;">▼</span>
Event List Condition	All <span style="float: right;">▼</span>
Reboot device after	<input type="text" value="60"/> Seconds

OK Cancel

Fig. 189: **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
<b>Description</b>	Enter your chosen designation for the action.
<b>Command Type</b>	<p>Select the desired action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Reboot</i> (default value): Your device is rebooted.</li> <li>• <i>MIB/SNMP</i>: The desired value is entered for a MIB variable.</li> <li>• <i>Interface Status</i>: The status of an interface is modified.</li> <li>• <i>Wlan Status</i>: Only for devices with a wireless LAN. The status of a WLAN-SSID is modified.</li> <li>• <i>Software Update</i>: A software update is initiated.</li> <li>• <i>Configuration Management</i>: A configuration file is loaded onto your device or backed up by your device.</li> <li>• <i>Ping Test</i>: Accessibility of an IP address is checked.</li> <li>• <i>Certificate Management</i>: A certificate is to be renewed, deleted or entered.</li> <li>• <i>5 GHz WLAN Bandscan</i>: Only for devices with a wireless LAN. A scan of the 5 GHz frequency band is performed.</li> <li>• <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.</li> <li>• <i>WLC: New Neighbor Scan</i>: Only for devices with a WLAN controller. A Neighbor Scan is initiated by the WLAN network controlled by the WLAN controller.</li> <li>• <i>WLC: VSS State</i>: Only for devices with a WLAN controller. The status of a wireless network is modified.</li> <li>• <i>WLAN: Operation Mode</i>: The operating mode of a WLAN radio module is modified.</li> </ul>
<b>Event List</b>	Select the event list you want which has been created in <b>Local Services-&gt;Scheduling-&gt;Trigger</b> .
<b>Event List Condition</b>	<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"> <li>• <i>All</i> (default value): The operation is initiated if all events occur.</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>One</i>: The operation is initiated if a single event occurs.</li> <li>• <i>None</i>: The operation is triggered if no event occurs.</li> <li>• <i>One not</i>: The operation is triggered if one of the events does not occur.</li> </ul>
<b>Reboot device after</b>	<p>Only if <b>Command Type</b> = <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>
<b>MIB/SNMP Variable to add/edit</b>	<p>Only if <b>Command Type</b> = <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 <b>System</b>, then the <b>MIB Table</b>. Only the MIB tables present in the respective area are displayed.</p>
<b>Command Mode</b>	<p>Only if <b>Command Type</b> = <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"> <li>• <i>Change existing entry</i> (default value): An existing entry shall be modified.</li> <li>• <i>Create new MIB entry</i>: A new entry shall be created.</li> </ul>
<b>Index Variables</b>	<p>Only if <b>Command Type</b> = <i>MIB/SNMP</i></p> <p>Where required, select MIB variables to uniquely identify a specific data set in <b>MIB Table</b>, e.g. <i>ConnIfIndex</i>. The unique identification of a particular table entry is derived from the combination of <b>Index Variable</b> (usually an index variable which is flagged with *) and <b>Index Value</b>.</p> <p>Use <b>Index Variables</b> to create more entries with <b>Add</b>.</p>
<b>Trigger Status</b>	<p>Only if <b>Command Type</b> = <i>MIB/SNMP</i></p> <p>Select what status the event must have in order to modify the MIB variable as defined.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Active</i> (default value): The value of the MIB variable is modified if the initiator is active.</li> <li>• <i>Inactive</i>: The value of the MIB variable is modified if the initiator is inactive.</li> <li>• <i>Both</i>: The value of the MIB variable is differentially modified if the initiator status changes.</li> </ul>
<b>MIB Variables</b>	<p>Only if <b>Command Type</b> = <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 (<b>Trigger Status</b> <i>Active</i>), the MIB variable is described with the value entered in <b>Active Value</b>.</p> <p>If the initiator is inactive (<b>Trigger Status</b> <i>Inactive</i>), the MIB variable is described with the value entered in <b>Inactive Value</b>.</p> <p>If the MIB variable is to be modified, depending on whether the initiator is active or inactive (<b>Trigger Status</b> <i>Both</i>), it is described with an active initiator with the value entered in <b>Active Value</b> and with an inactive initiator with the value in <b>Inactive Value</b>.</p> <p>Use <b>Add</b> to create more entries.</p>
<b>Interface</b>	<p>Only if <b>Command Type</b> = <i>Interface Status</i></p> <p>Select the interface whose status should be changed.</p>
<b>Set interface status</b>	<p>Only if <b>Command Type</b> = <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"> <li>• <i>Up</i> (default value)</li> <li>• <i>Down</i></li> <li>• <i>Reset</i></li> </ul>
<b>Local WLAN SSID</b>	<p>Only if <b>Command Type</b> = <i>Wlan Status</i></p>

Field	Description
	Select the desired wireless network whose status shall be changed.
<b>Set status</b>	<p>Only if <b>Command Type</b> = <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"> <li>• <i>Activate</i> (default value)</li> <li>• <i>Deactivate</i></li> </ul>
<b>Source Location</b>	<p>Only if <b>Command Type</b> = <i>Software Update</i></p> <p>Select the source for the software update.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Current Software from Update Server</i> (default value): The latest software will be downloaded from the update server.</li> <li>• <i>HTTP Server</i>: The latest software will be downloaded from an HTTP server that you define in <i>Server URL</i>.</li> <li>• <i>HTTPS Server</i>: The latest software will be downloaded from an HTTPS server that you define in <i>Server URL</i>.</li> <li>• <i>TFTP Server</i>: The latest software will be downloaded from an TFTP server that you define in <i>Server URL</i>.</li> </ul>
<b>Server URL</b>	<p>Where <b>Command Type</b> = <i>Software Update</i> if <b>Source Location</b> 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 <b>Command Type</b> = <i>Configuration Management</i> with <b>Action</b> = <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>
<b>File Name</b>	For <b>Command Type</b> = <i>Software Update</i>

Field	Description
	<p>Enter the file name of the software version.</p> <p>Where <b>Command Type</b> = <i>Certificate Management</i> with <b>Action</b> = <i>Import certificate</i></p> <p>Enter the file name of the certificate file.</p>
<b>Action</b>	<p>For <b>Command Type</b> = <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"> <li>• <i>Import configuration</i> (default value)</li> <li>• <i>Export configuration</i></li> <li>• <i>Rename configuration</i></li> <li>• <i>Delete configuration</i></li> <li>• <i>Copy configuration</i></li> </ul> <p>For <b>Command Type</b> = <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"> <li>• <i>Import certificate</i> (default value)</li> <li>• <i>Delete certificate</i></li> <li>• <i>SCEP</i></li> </ul>
<b>Protocol</b>	<p>Only for <b>Command Type</b> = <i>Certificate Management</i> and <i>Configuration Management</i> if <b>Action</b> = <i>Import configuration</i></p> <p>Select the protocol for the data transfer.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>HTTP</i> (default value)</li> <li>• <i>HTTPS</i></li> <li>• <i>TFTP</i></li> </ul>
<b>CSV File Format</b>	<p>Only where <b>Command Type</b> = <i>Configuration Management</i></p>



Field	Description
	<p>and <b>Action</b> = <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>
<b>Remote File Name</b>	<p>Only if <b>Command Type</b> = <i>Configuration Management</i></p> <p>For <b>Action</b> = <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 <b>Action</b> = <i>Export configuration</i></p> <p>Enter the file name under which it should be saved on the server.</p>
<b>Local File Name</b>	<p>Only where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <i>Import configuration, 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>
<b>File Name in Flash</b>	<p>Where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <i>Export configuration</i></p> <p>Select the file to be exported.</p> <p>Where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <i>Rename configuration</i></p> <p>Select the file to be renamed.</p> <p>Where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <i>Delete configuration</i></p> <p>Select the file to be deleted.</p> <p>Where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <i>Copy configuration</i></p>

Field	Description
	Select the file to be copied.
<b>Configuration contains certificates/keys</b>	<p>Only where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <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>
<b>Encrypt configuration</b>	<p>Only where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <i>Import configuration</i> or <i>Export configuration</i></p> <p>Define whether the data of the selected <b>Action</b> are to be encrypted..</p> <p>The function is disabled by default.</p>
<b>Reboot after execution</b>	<p>Only if <b>Command Type</b> = <i>Configuration Management</i></p> <p>Select whether your device should restart after the intended <b>Action</b>.</p> <p>The function is disabled by default.</p>
<b>Version Check</b>	<p>Only where <b>Command Type</b> = <i>Configuration Management</i> and <b>Action</b> = <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>
<b>Destination IP Address</b>	<p>Only if <b>Command Type</b> = <i>Ping Test</i></p> <p>Enter the IP address whose accessibility is to be checked.</p>
<b>Source IP Address</b>	<p>Only if <b>Command Type</b> = <i>Ping Test</i></p> <p>Enter an IP address to be used as sender address for the ping test.</p>

Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Automatic</i> (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address.</li> <li>• <i>Specific</i>: Enter the desired IP address in the input field.</li> </ul>
<b>Interval</b>	<p>Only if <b>Command Type</b> = <i>Ping Test</i></p> <p>Enter the time in <b>Seconds</b> after which a ping must be resent.</p> <p>The default value is <i>1</i> second.</p>
<b>Count</b>	<p>Only if <b>Command Type</b> = <i>Ping Test</i></p> <p>Enter the number of ping tests to be performed until <b>Destination IP Address</b> is considered unreachable.</p> <p>The default value is <i>3</i>.</p>
<b>Server Address</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <i>Import certificate</i></p> <p>Enter the URL of the server from which a certificate file is to be retrieved.</p>
<b>Local Certificate Description</b>	<p>Where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <i>Import certificate</i></p> <p>Enter a description for the certificate under which to save it on the device.</p> <p>Where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <i>Delete certificate</i></p> <p>Select the certificate to be deleted.</p>
<b>Password for protected Certificate</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>

Field	Description
<b>Overwrite similar certificate</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>
<b>Write certificate in configuration</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>
<b>Certificate Request Description</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <i>SCEP</i></p> <p>Enter a description under which the SCEP certificate on your device is to be saved.</p>
<b>URL SCEP Server URL</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>
<b>Subject Name</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <i>SCEP</i></p> <p>Enter a subject name with attributes.</p> <p>Example: <i>"CN=VPNServer, DC=mydomain, DC=com, c=DE"</i></p>
<b>CA Name</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>

Field	Description
<b>Password</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>
<b>Key Size</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>
<b>Autosave Mode</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <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>
<b>Use CRL</b>	<p>Only where <b>Command Type</b> = <i>Certificate Management</i> and <b>Action</b> = <i>SCEP</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 values:</p> <ul style="list-style-type: none"> <li>• <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.</li> <li>• <i>Yes</i>: CRLs are always checked.</li> <li>• <i>No</i>: No checking of CRLs.</li> </ul>
<b>Select radio</b>	<p>Only where <b>Command Type</b> = <i>5 GHz WLAN Bandscan</i>, <i>5.8 GHz WLAN Bandscan</i> or</p>

Field	Description
	<p><i>WLAN: Operation Mode</i></p> <p>Select the WLAN module on which to perform the frequency band scan.</p>
<b>WLC SSID</b>	<p>Only where <b>Command Type</b> = <i>WLC: VSS State</i></p> <p>Select the wireless network administered over the WLAN controller whose status should be changed.</p>
<b>Operation Mode (Active)</b>	<p>Only where <b>Command Type</b> = <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>
<b>Operation Mode (Inactive)</b>	<p>Only where <b>Command Type</b> = <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>

### 17.8.3 Options

You configure the schedule interval in the **Local Services->Scheduling->Options**.

The screenshot shows a dialog box with three tabs: 'Trigger', 'Actions', and 'Options'. The 'Options' tab is selected. Inside the dialog, there is a section titled 'Scheduling Options'. Below this title, there is a 'Schedule Interval' field containing the value '0', followed by the unit 'sec' and a checked checkbox labeled 'Enabled'. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

Fig. 190: **Local Services->Scheduling->Options**

The **Local Services->Scheduling->Options** menu consists of the following fields:

#### Fields in the Scheduling Options menu.

Field	Description
<b>Schedule Interval</b>	Select whether the schedule interval is to be enabled for the in-

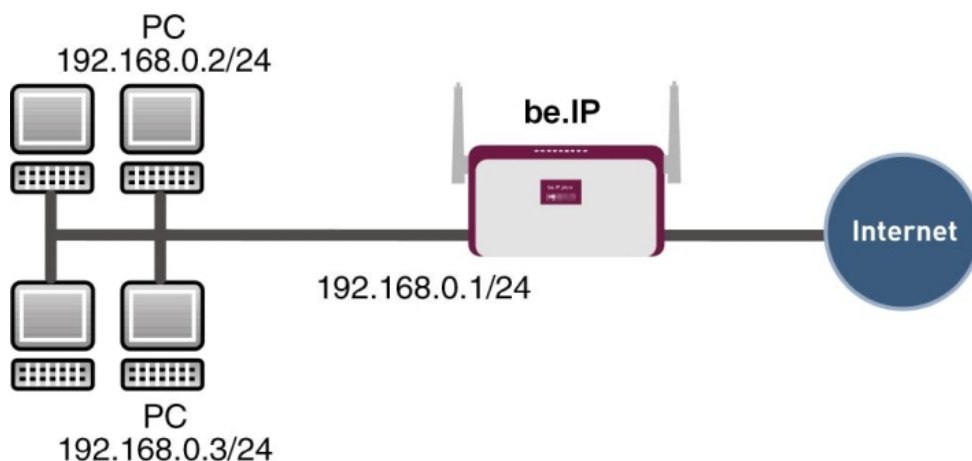
Field	Description
	<p>terface.</p> <p>The schedule interval is disabled by default.</p> <p>Enter the period of time in seconds after which the system checks whether configured events have occurred.</p> <p>Possible values are <code>0</code> to <code>65535</code>.</p> <p>The value <code>300</code> is recommended (5 minute accuracy).</p>

## 17.8.4 Configuration example - Time-controlled Tasks (Scheduling)

### Requirements

- Basic configuration of the gateway.

### Example scenario



Example scenario Time-controlled Tasks

### Configuration target

- You want to reboot your gateway automatically overnight.
- The WLAN interface is to be suspended at the weekend.

- In addition, the configuration is to be backed up automatically once a month on a TFTP server.

## Overview of Configuration Steps

### Daily reboot

Field	Menu	Value
Event List	Local Services->Scheduling->Trigger->New	<i>New</i>
Description	Local Services->Scheduling->Trigger->New	<i>e.g. Trigger Reboot</i>
Event Type	Local Services->Scheduling->Trigger->New	<i>Time</i>
Time Condition	Local Services->Scheduling->Trigger->New	Condition Type = <i>Periods</i> , Condition Settings = <i>Daily</i>
Start Time	Local Services->Scheduling->Trigger->New	Hour <i>02</i> Minute <i>00</i>
Description	Local Services->Scheduling->Actions->New	<i>e.g. Reboot the devicet</i>
Command Type	Local Services->Scheduling->Actions->New	<i>Reboot</i>
Event List	Local Services->Scheduling->Actions->New	<i>Trigger Reboot</i>
Event List Condition	Local Services->Scheduling->Actions->New	<i>All</i>
Reboot device after	Local Services->Scheduling->Actions->New	<i>e.g. 60 Seconds</i>
Schedule Interval	Local Services->Scheduling->Options	<i>Enabled, 55 sec</i>

### Suspending the WLAN interface

Field	Menu	Value
Event List	Local Services->Scheduling->Trigger->New	<i>New</i>
Description	Local Services->Scheduling->Trigger->New	<i>e.g. Trigger switch off WLAN interface</i>
Event Type	Local Services->Scheduling->Trigger->New	<i>Time</i>



Field	Menu	Value
Time Condition	Local Services->Scheduling->Trigger->New	Condition Type = <i>Periods</i> , Condition Settings = <i>Saturday - Sunday</i>
Start Time	Local Services->Scheduling->Trigger->New	Hour <i>00</i> Minute <i>00</i>
Stop Time	Local Services->Scheduling->Trigger->New	Hour <i>23</i> Minute <i>59</i>
Description	Local Services->Scheduling->Actions->New	e.g. <i>Switch off WLAN interface</i>
Command Type	Local Services->Scheduling->Actions->New	<i>Interface Status</i>
Event List	Local Services->Scheduling->Actions->New	<i>Trigger switch off WLAN interface</i>
Event List Condition	Local Services->Scheduling->Actions->New	<i>All</i>
Interface	Local Services->Scheduling->Actions->New	e.g. <i>vss1-0</i>
Set interface status	Local Services->Scheduling->Actions->New	<i>Down</i>
Schedule Interval	Local Services->Scheduling->Options	<i>Enabled, 55 sec</i>

#### Monthly configuration backup

Field	Menu	Value
Event List	Local Services->Scheduling->Trigger->New	<i>New</i>
Description	Local Services->Scheduling->Trigger->New	e.g. <i>Trigger configuration backup</i>
Event Type	Local Services->Scheduling->Trigger->New	<i>Time</i>
Time Condition	Local Services->Scheduling->Trigger->New	Condition Type = <i>Day of Month</i> , Condition Settings = <i>1</i>
Start Time	Local Services->Scheduling->Trigger->New	Hour <i>03</i> Minute <i>00</i>
Description	Local Services->Scheduling->Actions->New	<i>Configuration backup</i>

Field	Menu	Value
Command Type	Local Services->Scheduling->Actions->New	Configuration Management
Event List	Local Services->Scheduling->Actions->New	Trigger configuration backup
Event List Condition	Local Services->Scheduling->Actions->New	All
Action	Local Services->Scheduling->Actions->New	Export configuration
Server URL	Local Services->Scheduling->Actions->New	e.g. <i>tftp://192.168.2.5</i>
CSV File Format	Local Services->Scheduling->Actions->New	<i>Enabled</i>
Remote File Name	Local Services->Scheduling->Actions->New	e.g. <i>monthly-backup.cf</i>
File Name in Flash	Local Services->Scheduling->Actions->New	<i>boot</i>
Configuration contains certificates/keys	Local Services->Scheduling->Actions->New	<i>Aktiviert</i>
Schedule Interval	Local Services->Scheduling->Options	<i>Enabled, 55 sec</i>

## 17.9 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.

### 17.9.1 Hosts

A list of all monitored hosts is displayed in the **Local Services->Surveillance->Hosts** menu.

### 17.9.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional monitoring tasks.

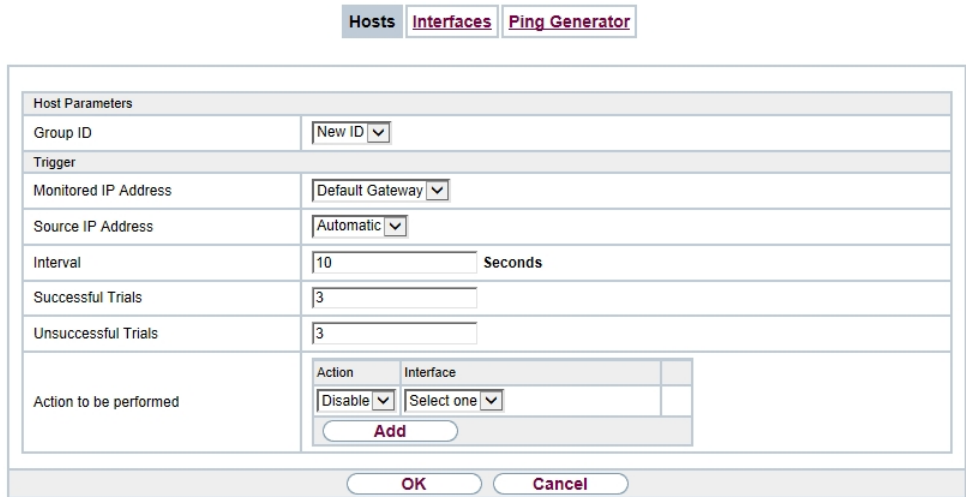


Fig. 191: Local Services->Surveillance->Hosts->New

The menu **Local Services->Surveillance->Hosts->New** consists of the following fields:

#### Fields in the Host Parameters menu

Field	Description
<b>Group ID</b>	<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 <b>Interface</b> is only executed if no group member can be reached.</p>

#### Fields in the Trigger menu.


Field	Description
<b>Monitored IP Address</b>	<p>Enter the IP address of the host to be monitored.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Default Gateway</i> (default value): The default gateway is monitored.</li> <li>• <i>Specific</i>: Enter the IP address of the host to be monitored manually in the adjacent input field.</li> </ul>
<b>Source IP Address</b>	<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"> <li>• <i>Automatic</i> (default value): The IP address is determined automatically.</li> <li>• <i>Specific</i>; Enter the IP address in the adjacent input field.</li> </ul>
<b>Interval</b>	<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 <b>Interval</b> of the group members is used.</p>
<b>Successful Trials</b>	<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>
<b>Unsuccessful Trials</b>	<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>
<b>Action to be performed</b>	<p>Select which <b>Action</b> should be run. For most actions, you select an <b>Interface</b> to which the <b>Action</b> 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 <b>Action</b> = <i>Monitor</i> you can monitor the IP address that is specified under <b>Monitored IP Address</b>. This information can be used for other functions, such as the <b>Tracking IP Address</b>.</p>

## 17.9.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services->Surveillance->Interfaces** menu.

### 17.9.2.1 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. 192: **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
<b>Monitored Interface</b>	Select the interface on your device that is to be monitored.
<b>Trigger</b>	Select the state or state transition of <b>Monitored Interface</b> that is to trigger a particular <b>Interface Action</b> .  Possible values: <ul style="list-style-type: none"> <li>• <i>Interface goes up</i> (default value)</li> <li>• <i>Interface goes down</i></li> </ul>
<b>Interface Action</b>	Select the action that is to follow the state or state transition defined in <b>Trigger</b> .  The action is applied to the Interface(s) selected in <b>Interface</b> .  Possible values: <ul style="list-style-type: none"> <li>• <i>Enable</i> (default value): Activation of interface(s)</li> <li>• <i>Disable</i>: Deactivation of interface(s)</li> </ul>
<b>Interface</b>	Select the interface(s) for which the action defined in <b>Interface</b> is to be performed.  You can choose all physical and virtual interfaces as well as options <i>All PPP Interfaces</i> and <i>All IPSec Interfaces</i> .

## 17.9.3 Ping Generator

In the **Local Services->Surveillance->Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

### 17.9.3.1 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	<input type="text"/>
Source IP Address	Specific <span style="border: 1px solid black; padding: 2px;">▼</span> <input type="text"/>
Interval	<input type="text" value="10"/> Seconds
Trials	<input type="text" value="3"/>

OK
Cancel


Fig. 193: 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
<b>Destination IP Address</b>	Enter the IP address to which the ping is automatically sent.
<b>Source IP Address</b>	Enter the source IP address of the outgoing ICMP echo request packets.  Possible values: <ul style="list-style-type: none"> <li>• <i>Automatic</i>: The IP address is determined automatically.</li> <li>• <i>Specific</i> (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.</li> </ul>
<b>Interval</b>	Enter the interval in seconds during which the ping is sent to the address specified in <b>Remote IP Address</b> .  Possible values are 1 to 65536.  The default value is 10.
<b>Trials</b>	Enter the number of ping tests to be performed until <b>Destination IP Address</b> as <i>Unreachable</i> applies.  The default value is 3.

## 17.10 ISDN Theft Protection

With the ISDN theft protection function, you can prevent a thief who has stolen a gateway from gaining access to the gateway owner's LAN. (Without theft protection, he could dial in to the LAN by ISDN if under **WAN->Internet + Dialup->ISDN->**  the field **Always on** is activated.)

### 17.10.1 Options

All interfaces for which the theft protection is enabled are administratively set to "down" when the gateway boots.

The gateway then calls itself by ISDN and checks its location. If the configured ISDN call numbers differ from the numbers dialled, the interfaces remain disabled.

If the numbers agree, the device assumes that it is at the original location and the interfaces are administratively set to "up".

To reduce cost, the function uses the ISDN D channel.



#### Note

Note that the ISDN theft protection function is not available for Ethernet interfaces.



**Options**

Basic Parameters	
ISDN Theft Protection Service	<input checked="" type="checkbox"/> <b>Enabled</b>
Dialling Number	<input type="text"/>
Incoming Number	<input type="text"/>
Outgoing Number	<input type="text"/>
Monitored Interfaces	<div style="border: 1px solid #ccc; padding: 2px;"> <input type="text" value="Interface"/> </div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Add"/> </div>
Advanced Settings	
Number of Dialling Retries	<input type="text" value="3"/>
Timeout	<input type="text" value="5"/> <b>Seconds</b>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Fig. 194: **Local Services->ISDN Theft Protection->Options**

The menu **Local Services->ISDN Theft Protection->Options** consists of the following fields:

**Fields in the Basic Parameters menu.**

Field	Description
<b>ISDN Theft Protection Service</b>	Enable or disable the ISDN theft protection function.  The function is enabled with <i>Enabled</i> .  The function is disabled by default.
<b>Dialling Number</b>	Only if <b>ISDN Theft Protection Service</b> is enabled.  Enter the subscriber number that the gateway dials to call itself.
<b>Incoming Number</b>	Only if <b>ISDN Theft Protection Service</b> is enabled.  Enter the subscriber number to be compared with the current calling party number.
<b>Outgoing Number</b>	Only if <b>ISDN Theft Protection Service</b> is enabled.  Enter the subscriber number to be set as calling party number.
<b>Monitored Interfaces</b>	Only if <b>ISDN Theft Protection Service</b> is enabled.

Field	Description
	Use <b>Add</b> to add a new interface.  Select from the available interfaces those to which the ISDN theft protection function is to be applied.

#### Fields in the **Advanced Settings** menu.

Field	Description
<b>Number of Dialling Retries</b>	Enter the number of dial attempts that the gateway is to make to call itself by ISDN after a reboot.  Possible values are <i>1</i> to <i>255</i> .  The default value is <i>3</i> .
<b>Timeout</b>	Enter the time in seconds that the gateway is to wait before trying again after an unsuccessful attempt to call itself.  Possible values are <i>2</i> to <i>20</i> .  The default value is <i>5</i> .

## 17.11 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](http://www.upnp.org).

## 17.11.1 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.

The screenshot shows the 'Interfaces' configuration window. At the top, there are tabs for 'Interfaces' and 'General'. Below the tabs is a search bar with 'View 20 per page' and a 'Go' button. The main area contains a table with the following data:

Interface	Answer to client request	Interface is UPnP controlled
en1-0	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
en1-4	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

At the bottom of the window, there are 'OK' and 'Cancel' buttons. The status bar at the bottom left indicates 'Page: 1, Items: 1 - 2'.

Fig. 195: Local Services->UPnP->Interfaces

The menu **Local Services->UPnP->Interfaces** consists of the following fields:

### Fields in the Interfaces menu.

Field	Description
<b>Interface</b>	Shows the name of the interface for which the UPnP settings are to be made. The entry cannot be changed.
<b>Answer to client request</b>	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.

Field	Description
<b>Interface is UPnP controlled</b>	<p>Determine whether the NAT configuration of this interface is controlled by UPnP.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

## 17.11.2 General

In this menu, you make the basic UPnP settings.

Fig. 196: Local Services->UPnP->General

The **Local Services->UPnP->General** menu consists of the following fields:

### Fields in the General menu.

Field	Description
<b>UPnP Status</b>	<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>
<b>UPnP TCP Port</b>	<p>Enter the number of the port on which the gateway listens for UPnP requests.</p> <p>The possible values are 1 to 65535, the default value is 5678.</p>

## 17.12 HotSpot Gateway



### Important

The Hotspot Gateway must not be operated with IPv6 enabled, since IPv6 data traffic is not registered by the Hotspot Gateway and, therefore, cannot be controlled.

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 elmegbintec elmeg gateway installed onsite (with its own WLAN access point or additional connected WLAN device or wired LAN) and of the Hotspot 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 elmegbintec 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 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](http://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 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	<a href="https://hotspot.bintec-elmeg.com/">https://hotspot.bintec-elmeg.com/</a>
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](http://www.bintec-elmeg.com)

## 17.12.1 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.

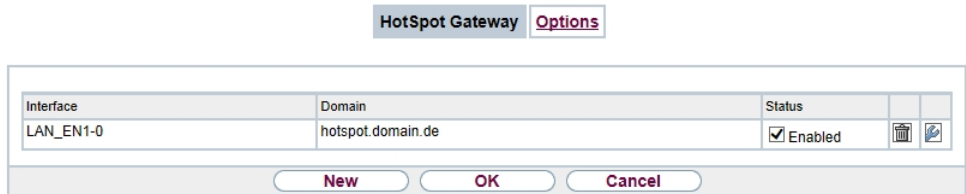


Fig. 197: **Local Services->HotSpot Gateway->HotSpot Gateway**

You can use the **Enabled** option to enable or disable the corresponding entry.

### 17.12.1.1 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 <span style="float: right;">▼</span>
Domain at the HotSpot Server	<input type="text"/>
Walled Garden	<input type="checkbox"/> Enabled
Post Login URL	<input type="text"/>
Language for login window	English <span style="float: right;">▼</span>

Advanced Settings

Ticket Type	Username/Password <span style="float: right;">▼</span>
Allowed HotSpot Client	All <span style="float: right;">▼</span>
Login Frameset	<input checked="" type="checkbox"/> Active
Pop-Up window for status indication	<input checked="" type="checkbox"/> Active
Default Idle Timeout	<input checked="" type="checkbox"/> Enabled
	600 <input type="text"/> Seconds

OK
Cancel

Fig. 198: **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
<b>Interface</b>	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.
	<p><b>Caution</b></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>



Field	Description
<b>Domain at the HotSpot Server</b>	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).
<b>Walled Garden</b>	<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>
<b>Walled Network / Net-mask</b>	<p>Only if <b>Walled Garden</b> is enabled.</p> <p>Enter the network address of the <b>Walled Network</b> and the corresponding <b>Netmask</b> of the intranet server.</p> <p>For the address range resulting from <b>Walled Network / Net-mask</b>, 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>
<b>Walled Garden URL</b>	<p>Only if <b>Walled Garden</b> is enabled.</p> <p>Enter the <b>Walled Garden URL</b> of the intranet server. Freely accessible websites must be reachable over this address.</p>
<b>Terms &amp;Conditions</b>	<p>Only if <b>Walled Garden</b> is enabled.</p> <p>In the <b>Terms &amp;Conditions</b> input field, enter the address of the general terms and conditions on the intranet server, or public server, e.g., <a href="http://www.webserver.de/agb.htm">http://www.webserver.de/agb.htm</a>. The page must lie within the address range of the walled garden network.</p>
<b>Additional freely accessible Domain Names</b>	<p>Only if <b>Walled Garden</b> is enabled.</p> <p>Add further URLs or IP addresses with <b>Add</b>. The web pages can be accessed via these additional freely accessible addresses.</p>
<b>Post Login URL</b>	Here you can specify the URL a user is redirected to after logging in to the Hotspot Solution.
<b>Language for login window</b>	Here you can choose the language for the start/login page.

Field	Description
	<p>The following languages are supported: <i>English, Deutsch, Italiano, Français, Español, Português</i> and <i>Nederlands</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
<b>Ticket Type</b>	<p>Select the ticket type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Voucher</i>: Only the user name must be entered. Define a default password in the input field.</li> <li>• <i>Username/Password</i> (default value): User name and password must be entered.</li> </ul>
<b>Allowed HotSpot Client</b>	<p>Here you can define which type of users can log in to the Hot-spot.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>All</i>: All clients are approved.</li> <li>• <i>DHCP Client</i>: Prevents users who have not received an IP address from DHCP from logging in.</li> </ul>
<b>Login Frameset</b>	<p>Enable or disable the login window.</p> <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>

Field	Description
<b>Pop-Up window for status indication</b>	Specify whether the device uses pop-up windows to display the status.  The function is enabled by default.
<b>Default Idle Timeout</b>	Enable or disable the <b>Default Idle Timeout</b> . If a hotspot user does not trigger any data traffic for a configurable length of time, they are logged out of the hotspot.  The function is enabled by default.  The default value is 600 seconds.

## 17.12.2 Options

In the **Local Services->HotSpot Gateway->Options** menu, general settings are performed for the hotspot.

The screenshot shows a software interface with two tabs: 'HotSpot Gateway' and 'Options'. The 'Options' tab is selected. Below the tabs, there is a 'Basic Parameters' section with a text input field labeled 'Host for multiple locations'. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

Fig. 199: **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
<b>Host for multiple locations</b>	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.


## 17.13 Wake-On-LAN

With the function **Wake-On-LAN** 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**.

### 17.13.1 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.

#### 17.13.1.1 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 IPv4 Address/Netmask	Any ▾
Destination IPv6 Address/Length	Any ▾
Source IPv4 Address/Netmask	Any ▾
Source IPv6 Address/Length	Any ▾
DSCP/Traffic Class Filter (Layer 3)	Ignore ▾
COS Filter (802.1p/Layer 2)	Ignore ▾

OK Cancel

Fig. 200: **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
<b>Description</b>	Enter the name of the filter.

Field	Description
<b>Service</b>	<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"> <li>• <i>activity</i></li> <li>• <i>apple-qt</i></li> <li>• <i>auth</i></li> <li>• <i>charge</i></li> <li>• <i>clients_1</i></li> <li>• <i>daytime</i></li> <li>• <i>dhcp</i></li> <li>• <i>discard</i></li> </ul> <p>The default value is <i>Any</i>.</p>
<b>Protocol</b>	<p>Select a protocol.</p> <p>The option <i>Any</i> (default value) matches any protocol.</p>
<b>Type</b>	<p>Only for <b>Protocol</b> = <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>
<b>Connection State</b>	<p>With <b>Protocol</b> = <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"> <li>• <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.</li> <li>• <i>Any</i> (default value): All TCP packets match the filter.</li> </ul>
<b>Destination IPv4 Address/Netmask</b>	<p>Enter the destination IPv4 address of the data packets and the corresponding netmask.</p> <p>Possible values:</p>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The destination IP address/netmask are not specified.</li> <li>• <i>Host</i>: Enter the destination IP address of the host.</li> <li>• <i>Network</i>: Enter the destination network address and the corresponding netmask.</li> </ul>
<b>Destination IPv6 Address/Length</b>	<p>Enter the destination IPv6 address of the data packets and the prefix length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The destination IP address/length are not specified.</li> <li>• <i>Host</i>: Enter the destination IP address of the host.</li> <li>• <i>Network</i>: Enter the destination network address and the prefix length.</li> </ul>
<b>Destination Port/Range</b>	<p>Only for <b>Protocol</b> = <i>TCP</i>, <i>UDP</i> or <i>TCP/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"> <li>• <i>-All-</i> (default value): The destination port is not specified.</li> <li>• <i>Specify port</i>: Enter a destination port.</li> <li>• <i>Specify port range</i>: Enter a destination port range.</li> </ul>
<b>Source IPv4 Address/Netmask</b>	<p>Enter the source IPv4 address of the data packets and the corresponding netmask.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The source IP address/netmask are not specified.</li> <li>• <i>Host</i>: Enter the source IP address of the host.</li> <li>• <i>Network</i>: Enter the source network address and the corresponding netmask.</li> </ul>
<b>Source IPv6 Address/Length</b>	<p>Enter the source IPv6 address of the data packets and the prefix length.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Any</i> (default value): The source IP address/length are not</li> </ul>


Field	Description
	<p>specified.</p> <ul style="list-style-type: none"> <li>• <i>Host</i>: Enter the source IP address of the host.</li> <li>• <i>Network</i>: Enter the source network address and the prefix length.</li> </ul>
<b>Source Port/Range</b>	<p>Only for <b>Protocol</b> = <i>TCP</i>, <i>UDP</i> or <i>TCP/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"> <li>• <i>-All-</i> (default value): The source port is not specified.</li> <li>• <i>Specify port</i>: Enter a source port.</li> <li>• <i>Specify port range</i>: Enter a source port range.</li> </ul>
<b>DSCP/TOS Filter (Layer 3)</b>	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Ignore</i> (default value): The type of service is ignored.</li> <li>• <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).</li> <li>• <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).</li> <li>• <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).</li> <li>• <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111.</li> <li>• <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63.</li> <li>• <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.</li> </ul>
<b>COS Filter (802.1p/Layer 2)</b>	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Value range 0 to 7.</p>

Field	Description
	The default value is <i>0</i> .
	The default value is <i>Ignore</i> .

## 17.13.2 WOL Rules

The menu **Local Services->Wake-On-LAN->WOL Rules** displays a list of all the WOL rules that have been configured.

### 17.13.2.1 Edit or New

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

Wake-On-LAN Filter WOL Rules Interface Assignment

Basic Parameters	
Wake-On-LAN Rule Chain	New ▾
Description	<input type="text"/>
Wake-On-LAN Filter	Select one ▾
Action	Invoke WOL if filter matches ▾
Type	Ethernet ▾
Send WOL packet over Interface	Select one ▾
Target MAC-Address	<input type="text"/>
Password	<input type="text"/>

Fig. 201: **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
<b>Wake-On-LAN Rule Chain</b>	<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"> <li><i>New</i> (default value): You can create a new rule chain with this</li> </ul>



Field	Description
	<p>setting.</p> <ul style="list-style-type: none"> <li>• <i>&lt;Name of the rule chain&gt;</i>: Shows a rule chain that has already been created, which you can select and edit.</li> </ul>
<b>Description</b>	<p>Only where <b>Wake-On-LAN Rule Chain</b> = <i>New</i></p> <p>Enter the name of the rule chain.</p>
<b>Wake-On-LAN Filter</b>	<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 <b>Local Services-&gt;Wake-On-LAN-&gt;WOL Rules</b> menu.</p>
<b>Action</b>	<p>Define the action to be taken for a filtered data packet.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Invoke WOL if filter matches</i>: Run WOL if the filter matches.</li> <li>• <i>Invoke if filter does not match</i>: Run WOL if the filter does not match.</li> <li>• <i>Deny WOL if filter matches</i>: Do not run WOL if the filter matches.</li> <li>• <i>Deny WOL if filter does not match</i>: Do not run WOL if the filter does not match.</li> <li>• <i>Ignore rule and skip to next rule</i>: This rule is ignored and the next one in the chain is examined.</li> </ul>
<b>Type</b>	<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 specified in <b>Send WOL packet over Interface</b>.</p>
<b>Send WOL packet over Interface</b>	<p>Select the interface which is to be used to send the Wake on LAN magic packet.</p>
<b>Target MAC-Address</b>	<p>Only where <b>Action</b> = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p>

Field	Description
	Enter the MAC address of the network device that is to be enabled using WOL.
<b>Password</b>	<p>Only where <b>Action</b> = <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>

### 17.13.3 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.

#### 17.13.3.1 Edit or New


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



Fig. 202: **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
<b>Interface</b>	Select the interface for which a configured rule chain is to be assigned.

Field	Description
Rule Chain	Select a rule chain.

## 17.14 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 ( <b>Virtual Router ID</b> ) 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 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.”

Field	Description
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."

### 17.14.1 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](http://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, change-over tolerance) 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.)

### 17.14.1.1 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	<table border="1"> <thead> <tr> <th>IP Address</th> <th>Netmask</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>255.255.255.0</td> <td></td> </tr> </tbody> </table> <input type="button" value="Add"/>			IP Address	Netmask			255.255.255.0	
IP Address	Netmask								
	255.255.255.0								
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)	<input checked="" type="checkbox"/> Enabled								
Enable authentication	<input type="checkbox"/>								
<input type="button" value="OK"/>		<input type="button" value="Cancel"/>							


Fig. 203: **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
<b>Ethernet Interface</b>	<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 <b>Virtual Router Interface</b>.</p>
<b>IP Address</b>	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
<b>Virtual Router Interface</b>	<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>
<b>Virtual Router IP Address</b>	<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>
	<p> <b>Note</b></p> <p>To avoid problems in the LAN, the <b>IP Address</b> for advertisements and the <b>Virtual Router IP Address</b> cannot originate from the same subnet.</p>
<b>Virtual Router ID</b>	<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 <i>1</i> and <i>255</i>.</p>

Field	Description
<b>Virtual Interface Priority</b>	<p>Define the transmitted BRRP priority of the interface for the virtual router. Higher priorities determine the master interfaces during the initialization phase as well as with active Pre-Empt-Mode. Possible values are between <i>1</i> and <i>255</i>. The higher the value, the higher the priority. The value <i>255</i> defines that this virtual router always functions as master as soon as it is active.</p> <p>The default value is <i>100</i>.</p> <p>A priority of <i>255</i> is used for routers the IP address of which is identical 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
<b>Advertisement send interval</b>	<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 <i>1</i> and <i>255</i>. The value is indicated in seconds and the default value is <i>1</i>. <i>1</i>.</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>
<b>Master down trials</b>	<p>Define the number of BRRP advertisements that must be missing in one sequence before the backup router with the highest priority value assumes that the master is inactive and takes over the role of master.</p> <p>A master down timer based on the <b>Master down trials</b> 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</p>



Field	Description
	<p>the number of expected but omitted BRRP advertisements, the advertisement interval and the skew time, which adds a minimal 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 <i>1</i> to <i>255</i> and the default value is <i>10</i>.</p>
<p><b>Pre-empt mode (go back into master state)</b></p>	<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 <b>Virtual Interface Priority 255</b> is selected, the gateway with this priority certainly takes over the master role, i.e. the setting in <b>Pre-empt mode (go back into master state)</b> is ignored. You should therefore select a <b>Virtual Interface Priority</b> lower than <i>255</i> if you wish to use Pre-empt Mode.</p>
<p><b>Enable authentication</b></p>	<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>

## 17.14.2 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.

### 17.14.2.1 New

Select the **New** button to create new synchronisations.

Fig. 204: **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
<b>Monitoring Mode</b>	Shows which mechanism is used for monitoring a virtual router.  Possible values: <ul style="list-style-type: none"> <li>• <i>BRRP</i>: The BRRP-specific state advertisements are used for determining the state of the master. (The master sends ad-</li> </ul>

Field	Description
	vertisements as per its configuration in the <b>Local Services-&gt;BRRP-&gt;Virtual Routers-&gt;New-&gt;Advanced Settings</b> menu.)
<b>Virtual Router ID</b>	Select a virtual router using the <b>Virtual Router ID</b> and define which interface is to be checked. You can choose previously defined IDs (see <b>Virtual Router ID</b> in the <b>Local Services-&gt;BRRP-&gt;Virtual Router-&gt;New</b> menu under <b>BRRP Monitored Interface</b> ). The watchdog daemon requests detailed information entered in the <b>Virtual Routers</b> .

#### Fields in the Synchronisation VR / Interface menu.

Field	Description
<b>Synchronisation Mode</b>	Indicates the mechanism with which virtual routers or interfaces are synchronised:  Possible values:  <ul style="list-style-type: none"> <li>• <i>BRRP</i>: BRRP is used to synchronise the virtual router.</li> </ul>
<b>Virtual Router ID</b>	Select the ID of the virtual router to be synchronised. Synchronising the virtual router implicitly synchronises the virtual interface associated with the virtual router.

### 17.14.3 Options

In the **Local Services->BRRP->Options** menu, you can enable or disable the BRRP function.

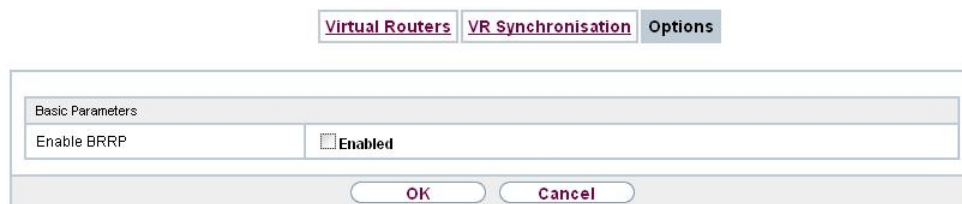


Fig. 205: **Local Services->BRRP->Options**

The **Local Services->BRRP->Options** menu consists of the following fields:

#### Fields in the Basic Parameters menu.

Field	Description
<b>Enable BRRP</b>	Enable or disable the BRRP function. The function is enabled with <i>Enabled</i> . The function is disabled by default.

## Chapter 18 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.

### 18.1 Log out Users

It can happen that an incompletely terminated configuration session affects functions of the configuration interface. In this case, all active configurations can be checked and - if applicable - terminated.

#### 18.1.1 Log out Users

In this menu, you are presented with a list of all active configuration sessions.

**Log out Users**

Automatic Refresh Interval		60	Seconds	<b>Apply</b>
Class	User	Remote IP Address	Expires	Log out immediately Select all/ Deselect all
Admin	admin	10.0.0.254	01:50:50	<input checked="" type="checkbox"/>

**Logout**      **Cancel**

Fig. 206: Maintenance->Log out Users->Log out Users

#### Fields in the manu Log out Users

Field	Description
<b>Class</b>	Displays the class the signed-on user belongs to.
<b>User</b>	Displays the user name.
<b>Remote IP Address</b>	Displays the IP address from which the connection has been established. This may be the address of a PC, but it may also be the address of an intermediate router.
<b>Expires</b>	Displays when the connection will be automatically terminated by the device.
<b>Log out immediately</b>	If you activate the check box, this user will be disconnected

Field	Description
	from the system when you click <b>Logout</b> .

### 18.1.1.1 Logout Options

After you have confirmed your selection of connections to be terminated with **Logout** you can choose if any configuration related to the connections is to be saved before the user is actually disconnected, and in which way.

Fig. 207: Maintenance->Log out Users->Logout Options

## 18.2 Diagnostics

In the **Maintenance->Diagnostics** menu, you can test the availability of individual hosts, the resolution of domain names and certain routes.

### 18.2.1 Ping Test

Fig. 208: 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.

#### Fields in the Ping Test menu

Field	Description
<b>Test Ping Mode</b>	Select the IP version to be used for the ping test.  Possible values: <ul style="list-style-type: none"> <li>• <i>IPv4</i></li> <li>• <i>IPv6</i></li> </ul>
<b>Test Ping Address</b>	Enter the IP address to be tested.
<b>Use Interface</b>	Only for <b>Test Ping Mode</b> = <i>IPv6</i>  For link local addresses select the interface to be used for the ping test. <i>Default</i> can be used for global addresses.

Pressing the **Go** button starts the ping test. The **Output** field displays the ping test messages.

## 18.2.2 DNS Test

The screenshot shows a web-based configuration interface for network diagnostics. At the top, there are three tabs: 'Ping Test', 'DNS Test', and 'Traceroute Test'. The 'DNS Test' tab is currently selected. Below the tabs, the interface is divided into sections. The 'DNS Test' section has a 'DNS Address' input field. Below that is a large 'Output' area, which is currently empty. At the bottom of the interface, there is a 'Go' button.

Fig. 209: Maintenance->Diagnostics->DNS Test

The DNS test is used to check whether the domain name of a particular host is correctly resolved. 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.

## 18.2.3 Traceroute Test

Fig. 210: 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.

### Fields in the Traceroute Test menu

Field	Description
<b>Traceroute Mode</b>	Select the IP version to be used for the Traceroute test.  Possible values: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
<b>Traceroute Address</b>	Enter the IP address to be tested.

Pressing the **Go** button starts the Traceroute test. The **Output** field displays the traceroute test messages.

## 18.3 Software & Configuration

You can use this menu to manage the software version of your device, your configuration files and the language of the **GUI**.



### 18.3.1 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](http://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 <input type="button" value="v"/>

Fig. 211: Maintenance->Software & Configuration->Options

The **Maintenance->Software & Configuration->Options** menu consists of the following fields:

### Fields in the **Currently Installed Software** menu.

Field	Description
<b>BOSS</b>	Shows the current software version loaded on your device.
<b>System Logic</b>	Shows the current system logic loaded on your device.
<b>ADSL Logic</b>	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"> <li>• <i>No Action</i> (default value):</li> <li>• <i>Export configuration</i>: The configuration file <b>Current File Name in Flash</b> is transferred to your local host. If you click the <b>Go</b> button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name.</li> <li>• <i>Import configuration</i>: Under <b>Filename</b> select a configuration file you want to import. Please note: Click <b>Go</b> 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.</li> </ul> <p>Please note: The files to be imported must be in CSV format!</p> <ul style="list-style-type: none"> <li>• <i>Copy configuration</i>: The configuration file in the <b>Source File Name</b> field is saved as <b>Destination File Name</b>.</li> <li>• <i>Delete configuration</i>: The configuration in the <b>Select file</b> field is deleted.</li> <li>• <i>Rename configuration</i>: The configuration file in the <b>Select file</b> field is renamed to <b>New File Name</b>.</li> <li>• <i>Restore backup configuration</i>: Only if, under <b>Save configuration</b> with the setting <i>Save configuration and back up previous boot configuration</i> the current configuration was saved as boot configuration and the previous boot configuration was also archived.</li> </ul> <p>You can load back the archived boot configuration.</p> <ul style="list-style-type: none"> <li>• <i>Delete software/firmware</i>: The file in the <b>Select file</b> field is deleted.</li> <li>• <i>Import language</i>: You can import additional language versions of the <b>GUI</b> into your device. You can download the files to your PC from the download area at <a href="http://www.bintec-elmeg.com">www.bintec-elmeg.com</a> and from there import them to your device</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>• <i>Update system software</i>: You can launch an update of the system software, the ADSL logic and the BOOTmonitor.</li> <li>• <i>Import Voice Mail Wave Files</i>: (Only displayed if an SD card is inserted, if supported by you device) In <b>file name</b>, select the <i>vms_wavfiles.zip</i> file that you wish to import.</li> <li>• <i>Export configuration with state information</i>: The active configuration from the RAM is transferred to your local host. If you click the <b>Go</b> button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name.</li> </ul>
<b>Current File Name in Flash</b>	<p>For <b>Action</b> = <i>Export configuration</i></p> <p>Select the configuration file to be exported.</p>
<b>Include certificates and keys</b>	<p>For <b>Action</b> = <i>Export configuration, Export configuration with state information</i></p> <p>Define whether the selected <b>Action</b> 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>
<b>Configuration Encryption</b>	<p>Only for <b>Action</b> = <i>Import configuration, Export configuration, Export configuration with state information</i>. Define whether the data of the selected <b>Action</b> 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 <b>Password</b> in the text field.</p>
<b>Filename</b>	<p>Only for <b>Action</b> = <i>Import configuration, Import language Update system software</i>.</p> <p>Enter the path and name of the file or select the file with <b>Browse...</b> via the explorer/finder.</p>
<b>Source File Name</b>	<p>Only for <b>Action</b> = <i>Copy configuration</i></p>

Field	Description
	Select the source file to be copied.
<b>Destination File Name</b>	<p>Only for <b>Action</b> = <i>Copy configuration</i></p> <p>Enter the name of the copy.</p>
<b>Select file</b>	<p>Only for <b>Action</b> = <i>Rename configuration, Delete configuration</i> or <i>Delete software/firmware</i></p> <p>Select the file or configuration to be renamed or deleted.</p>
<b>New File Name</b>	<p>Only for <b>Action</b> = <i>Rename configuration</i></p> <p>Enter the new name of the configuration file.</p>
<b>Source Location</b>	<p>Only for <b>Action</b> = <i>Update system software</i></p> <p>Select the source of the update.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Local File</i> (default value): The system software file is stored locally on your PC.</li> <li>• <i>HTTP Server</i>: The file is stored on a remote server specified in the <b>URL</b>.</li> <li>• <i>Current Software from Update Server</i>: The file is on the official update server.</li> </ul>
<b>URL</b>	<p>Only for <b>Source Location</b> = <i>HTTP Server</i></p> <p>Enter the URL of the update server from which the system software file is loaded.</p>

## 18.4 Reboot

### 18.4.1 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.

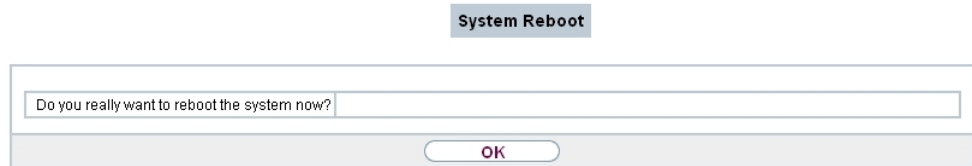


Fig. 212: **Maintenance->Reboot->System Reboot**

If you wish to restart your device, click the **OK** button. The device will reboot.

## 18.5 Factory Reset

In the menu **Maintenance->Factory Reset**, you can reset your device to the ex works state without having to have physical access to it.

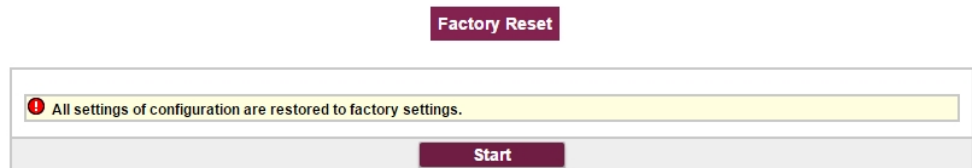


Fig. 213: **Maintenance->Factory Reset**

## Chapter 19 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.

### 19.1 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 Daemon 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](http://www.bintec-elmeg.com)).

#### 19.1.1 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.

### 19.1.1.1 New

Select the **New** button to set up additional syslog servers.

Fig. 214: **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
<b>IP Address</b>	Enter the IP address of the host to which syslog messages are passed.
<b>Level</b>	<p>Select the priority of the syslog messages that are to be sent to the host.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>Emergency</i> (highest priority)</li> <li>• <i>Alert</i></li> <li>• <i>Critical</i></li> <li>• <i>Error</i></li> <li>• <i>Warning</i></li> <li>• <i>Notice</i></li> <li>• <i>Information</i> (default value)</li> </ul>



Field	Description
	<ul style="list-style-type: none"> <li>• <i>Debug</i> (lowest priority)</li> </ul> <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>
<b>Facility</b>	<p>Enter the syslog facility on the host.</p> <p>This is only required if the <b>Log Host</b> is a Unix computer.</p> <p>Possible values: <i>local0</i> - 7 .</p> <p>The default value is <i>local0</i>.</p>
<b>Timestamp</b>	<p>Select the format of the time stamp in the syslog.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>None</i> (default value): No system time indicated.</li> <li>• <i>Time</i>: System time without date.</li> <li>• <i>Date &amp;Time</i>: System time with date.</li> </ul>
<b>Protocol</b>	<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"> <li>• <i>UDP</i> (default value)</li> <li>• <i>TCP</i></li> </ul>
<b>Type of Messages</b>	<p>Select the message type.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>System &amp;Accounting</i> (default value)</li> <li>• <i>System</i></li> <li>• <i>Accounting</i></li> </ul>

## 19.2 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).

### 19.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

The screenshot shows a web-based configuration interface for IP Accounting. At the top, there are two tabs: 'Interfaces' (selected) and 'Options'. Below the tabs is a table with the following structure:

#	Interface	IP Accounting Select all   Deselect all
1	en1-0	<input type="checkbox"/>
2	en1-4	<input type="checkbox"/>

Below the table, there is a status bar that reads 'Page: 1, Items: 1 - 2'. At the bottom of the interface, there are two buttons: 'OK' and 'Cancel'.

Fig. 215: **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.

### 19.2.2 Options

In this menu, you configure general settings for IP Accounting.

Fig. 216: 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]`

`%d%t%a%c%i:%r/%f -> %l:%R/%F%p%o%P%O[%s]`

## 19.3 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.

### 19.3.1 Alert Recipient

A list of Syslog messages is displayed in the **Alert Recipient** menu.

#### 19.3.1.1 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 style="border: 1px solid gray; padding: 2px;">           Subsystem  <input type="button" value="Add"/> </div>
Message Timeout	<input type="text" value="60"/>
Number of Messages	<input type="text" value="1"/>

Fig. 217: 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
<b>Alert Service</b>	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"> <li>• E-mail</li> <li>• SMS</li> </ul>
<b>Recipient</b>	Enter the recipient's e-mail address. The entry is limited to 40 characters.
<b>Message Compression</b>	<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>
<b>Subject</b>	You can enter a subject.
<b>Event</b>	<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"> <li>• <i>Syslog contains string</i> (default value): A Syslog message includes a specific string.</li> <li>• <i>New Neighbor AP found</i>: A new adjacent AP has been found.</li> <li>• <i>New Rogue AP found</i>: A new Rogue AP has been found, i.e. an AP using an SSID of its own network, yet is not a component of this network.</li> <li>• <i>New Slave AP (WTP) found</i>: A new unconfigured AP has reported to the WLAN.</li> <li>• <i>Managed AP offline</i>: A managed AP is no longer accessible.</li> </ul>
<b>Matching String</b>	<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 "*".
<b>Severity</b>	<p>Select the severity level which the string configured in the <b>Matching String</b> 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>
<b>Monitored Subsystems</b>	<p>Select the subsystems to be monitored.</p> <p>Add new subsystems with <b>Add</b>.</p>
<b>Message Timeout</b>	<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>
<b>Number of Messages</b>	<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>

## 19.3.2 Alert Settings

Alert Recipient
Alert Settings

Basic Parameters	
Alert Service	<input checked="" type="checkbox"/> Enabled
Maximum E-mails per Minute	6 ▼
E-mail Parameters	
Sender E-mail Address	<input type="text"/>
SMTP Server	<input type="text"/>
SMTP Port	25 <input checked="" type="checkbox"/> SSL
SMTP Authentication	<input checked="" type="radio"/> None <input type="radio"/> ESMTP <input type="radio"/> SMTP after POP
SMS Parameters	
SMS Device	Select one ▼
Maximum SMS per Day	<input type="checkbox"/> Unlimited <input type="text" value="10"/>

OK
Cancel

Fig. 218: 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
<b>Alert Service</b>	<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>
<b>Maximum E-mails per Minute</b>	Limit the number of outgoing mails per minute. Possible values are 1 to 15, the default value is 6.

### Fields in the E-mail Parameters menu.

Field	Description
<b>Sender E-mail Address</b>	Enter the mail address to be entered in the sender field of the E-mail.

Field	Description
<b>SMTP Server</b>	<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>
<b>SMTP Port</b>	<p>Encryption of e-mails (SSL / TLS).</p> <p>The field <b>SMTP Port</b> is per default preset to <i>25</i> and <b>SSL Encryption</b> is enabled.</p>
<b>SMTP Authentication</b>	<p>Authentication expected by the SMTP server.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <li>• <i>None</i> (default value): The server accepts and send emails without further authentication.</li> <li>• <i>ESMTP</i>: The server only accepts e-mails if the router logs in with the correct user name and password.</li> <li>• <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.</li> </ul>
<b>User Name</b>	<p>Only if <b>SMTP Authentication</b> = <i>ESMTP</i> or <i>SMTP after POP</i></p> <p>Enter the user name for the POP3 or SMTP server.</p>
<b>Password</b>	<p>Only if <b>SMTP Authentication</b> = <i>ESMTP</i> or <i>SMTP after POP</i></p> <p>Enter the password of this user.</p>
<b>POP3 Server</b>	<p>Only if <b>SMTP Authentication</b> = <i>SMTP after POP</i></p> <p>Enter the address of the server from which the e-mails are to be retrieved.</p>
<b>POP3 Timeout</b>	<p>Only if <b>SMTP Authentication</b> = <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
<b>SMS Device</b>	You can receive notification of system alerts in text messages. Select the device to be used to send the text message.
<b>Maximum SMS per Day</b>	<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>

## 19.4 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

### 19.4.1 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. 219: 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
<b>SNMP Trap Broadcasting</b>	<p>Select whether the transfer of SNMP traps is to be activated.</p> <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>
<b>SNMP Trap UDP Port</b>	<p>Only if <b>SNMP Trap Broadcasting</b> 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>
<b>SNMP Trap Community</b>	<p>Only if <b>SNMP Trap Broadcasting</b> 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>

## 19.4.2 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.

### 19.4.2.1 New

Select the **New** button to create additional SNMP trap hosts.

Fig. 220: **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.

## 19.5 SIA

### 19.5.1 SIA

In the menu **External Reporting->SIA->SIA**, you can create and download a file that provides extensive support information about the status of your device like, e.g., the current configuration, available memory, uptime etc.

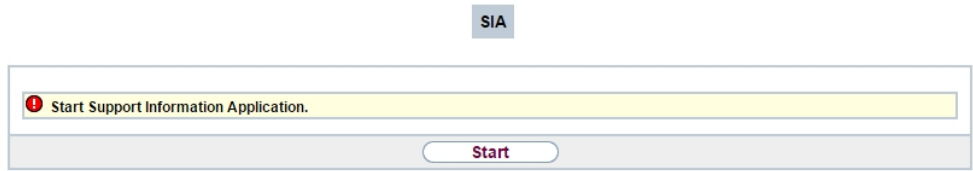


Fig. 221: **External Reporting->SIA->SIA**



Field	Description
<b>Subsystem</b>	Displays which subsystem of the device generated the message.
<b>Message</b>	Displays the message text.

## 20.2 IPSec



### 20.2.1 IPSec Tunnels

A list of all configured IPSec tunnel providers is displayed in the **Monitoring->IPSec->IPSec Tunnels** menu.

Fig. 223: **Monitoring->IPSec->IPSec Tunnels**

#### Values in the IPSec Tunnels list

Field	Description
<b>Description</b>	Displays the name of the IPSec tunnel.
<b>Remote IP</b>	Displays the IP address of the remote IPSec Peers.
<b>Remote Networks</b>	Displays the currently negotiated subnets of the remote terminal.
<b>Security Algorithm</b>	Displays the encryption algorithm of the IPSec tunnel.
<b>Status</b>	Displays the operating status of the IPSec tunnel.
<b>Action</b>	Enables you to change the status of the IPSec tunnel as displayed.
<b>Details</b>	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.

IPSec Tunnels
IPSec Statistics

Automatic Refresh Interval <input type="text" value="60"/> Seconds <span style="float: right; border: 1px solid black; border-radius: 10px; padding: 2px 10px;">Apply</span>		
<b>General</b>		
Description	Peer-1	
Local IP Address	0.0.0.0	
Remote IP Address	0.0.0.0	
Local ID		
Remote ID		
Negotiation Type		
Authentication Method		
MTU	1418	
Alive Check		
<b>Statistics</b>	<b>In</b>	<b>Out</b>
Packets	0	0
Bytes	0	0
Errors	0	0
Messages ( 0)		

Fig. 224: Monitoring->IPSec->IPSec Tunnels->

#### Values in the IPSec Tunnels list

Field	Description
<b>Description</b>	Shows the description of the peer.
<b>Local IP Address</b>	Shows the WAN IP address of your device.
<b>Remote IP Address</b>	Shows the WAN IP address of the connection partner.
<b>Local ID</b>	Shows the ID of your device for this IPSec tunnel.
<b>Remote ID</b>	Shows the ID of the peer.
<b>Negotiation Type</b>	Shows the exchange type.
<b>Authentication Method</b>	Shows the authentication method.
<b>MTU</b>	Shows the current MTU (Maximum Transfer Unit).
<b>Alive Check</b>	Shows the method for checking that the peer is reachable.
<b>NAT Detection</b>	Displays the NAT detection method.
<b>Local Port</b>	Shows the local port.
<b>Remote Port</b>	Shows the remote port.
<b>Packets</b>	Shows the total number of incoming and outgoing packets.
<b>Bytes</b>	Shows the total number of incoming and outgoing bytes.
<b>Errors</b>	Shows the total number of errors.
<b>IKE (Phase-1) SAs (x)</b>	The parameters of the IKE (Phase 1) SAs are displayed here.

Field	Description
<b>Role / Algorithm / Lifetime remaining / Status</b>	
<b>IPSec (Phase-2) SAs (x)</b>	Shows the parameters of the IPSec (Phase 2) SAs.
<b>Role / Algorithm / Lifetime remaining / Status</b>	
<b>Messages</b>	The system messages for this IPSec tunnel are displayed here.

## 20.2.2 IPSec Statistics

In the **Monitoring->IPSec->IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

IPSec Tunnels
IPSec Statistics

Automatic Refresh Interval		60	Seconds	<span style="border: 1px solid black; padding: 2px;">Apply</span>	
Licences			In Use	Maximum	
IPSec Tunnels			0	110	
Peers	Up	Going up	Blocked	Dormant	Configured
Status	0	0	0	1	1
SAs			Established	Total	
IKE (Phase-1)			0	0	
IPSec (Phase-2)			0	0	
Packet Statistics			In	Out	
Total			59	135	
Passed			59	135	
Dropped			0	0	
Encrypted			0	0	
Errors			0	0	

Fig. 225: **Monitoring->IPSec->IPSec Statistics**

The **Monitoring->IPSec->IPSec Statistics** menu consists of the following fields:

### Fields in the Licences menu

Field	Description
<b>IPSec Tunnels</b>	Shows the IPSec licences currently in use ( <b>In Use</b> ) and the maximum number of licenses usable ( <b>Maximum</b> ).

### Fields in the Peers menu



Field	Description
<b>Status</b>	<p>Displays the number of IPSec tunnels by their current status.</p> <ul style="list-style-type: none"> <li>• <b>Up</b>: Currently active IPSec tunnels.</li> <li>• <b>Going up</b>: IPSec tunnels currently in the tunnel setup phase.</li> <li>• <b>Blocked</b>: IPSec tunnels that are blocked.</li> <li>• <b>Dormant</b>: Currently inactive IPSec tunnels.</li> <li>• <b>Configured</b>: Configured IPSec tunnels.</li> </ul>

#### Fields in the **SAs** menu.

Field	Description
<b>IKE (Phase-1)</b>	Shows the number of active phase 1 SAs ( <b>Established</b> ) from the total number of phase 1 SAs ( <b>Total</b> ).
<b>IPSec (Phase-2)</b>	Shows the number of active phase 2 SAs ( <b>Established</b> ) from the total number of phase 2 SAs ( <b>Total</b> ).

#### Fields in the **Packet Statistics** menu.

Field	Description
<b>Total</b>	Shows the number of all processed incoming ( <b>In</b> ) or outgoing ( <b>Out</b> ) packets.
<b>Passed</b>	Shows the number of incoming ( <b>In</b> ) or outgoing ( <b>Out</b> ) packets forwarded in plain text.
<b>Dropped</b>	Shows the number of all rejected incoming ( <b>In</b> ) or outgoing ( <b>Out</b> ) packets.
<b>Encrypted</b>	Shows the number of all incoming ( <b>In</b> ) or outgoing ( <b>Out</b> ) packets protected by IPSec.
<b>Errors</b>	Shows the number of incoming ( <b>In</b> ) or outgoing ( <b>Out</b> ) packets for which processing led to errors.

## 20.3 ISDN/Modem

### 20.3.1 Current Calls

In the **Monitoring->ISDN/Modem->Current Calls** menu, a list of the existing ISDN connections (incoming and outgoing) is displayed.

[Current Calls](#)   [Call History](#)

---

Automatic Refresh Interval  Seconds  

View  per page   << >>   Filter in      

#	Service	Remote Number	Interface	Direction	Charge	Duration	Stack	Channel	Status
Page: 1									

Fig. 226: **Monitoring->ISDN/Modem->Current Calls**

### Values in the Current Calls list

Field	Description
<b>Service</b>	Displays the service to or from which the call is connected: <i>PPP, IPSec, X.25, POTS.</i>
<b>Remote Number</b>	Displays the number that was dialed (in the case of outgoing calls) or from which the call was made (in the case of incoming calls).
<b>Interface</b>	Displays additional information for PPP connections.
<b>Direction</b>	Displays the send direction: <i>Incoming, Outgoing.</i>
<b>Charge</b>	Displays the costs of the current connection.
<b>Duration</b>	Displays the duration of the current connection.
<b>Stack</b>	Displays the related ISDN port (STACK).
<b>Channel</b>	Displays the number of the ISDN B channel.
<b>Status</b>	Displays the state of the connection: <i>null, c-initiated, ovl-send, oc-procd, c-deliverd, c-present, c-recvd, ic-procd, up, discon-req, discon-ind, suspd-req, re-sum-req, ovl-recv.</i>

## 20.3.2 Call History

In the **Monitoring->ISDN/Modem->Call History** menu, a list of the last 20 ISDN calls (incoming and outgoing) completed since the last system start is displayed.

Current Calls
Call History

Automatic Refresh Interval  Seconds

View  per page << >> Filter in

#	Service	Remote Number	Interface	Direction	Charge	Start Time	Duration
Page: 1							

Fig. 227: **Monitoring->ISDN/Modem->Call History**

### Values in the Call History list

Field	Description
<b>Service</b>	Displays the service to or from which the call was connected: <i>PPP, IPsec, X.25, POTS.</i>
<b>Remote Number</b>	Displays the number that was dialled (in the case of outgoing calls) or from which the call was made (in the case of incoming calls).
<b>Interface</b>	Displays additional information for PPP connections.
<b>Direction</b>	Displays the send direction: <i>Incoming, Outgoing.</i>
<b>Charge</b>	Displays the costs of the connection.
<b>Start Time</b>	Displays the time at which the call was made or received.
<b>Duration</b>	Displays the duration of the connection.

## 20.4 Interfaces

### 20.4.1 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.

**Statistics**

Show Transfer Totals Automatic Refresh Interval 60 Seconds Apply

View 20 per page << >> Filter in None equal Go

No.	Description	Type	Tx Packets	Tx Bytes	Tx Errors	Rx Packets	Rx Bytes	Rx Errors	Status	Unchanged for	Action
1	en1-0	Ethernet	6.69K	5.21M	0	14.23K	1.40M	0		2d 2h 2m 59s	
2	en1-4	Ethernet	0	0	0	0	0	0		2d 2h 3m 2s	
3	Peer-1	Tunnel	0	0	0	0	0	0		0d 0h 5m 27s	

Page: 1, Items: 1 - 3

Fig. 228: **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
<b>No.</b>	Shows the serial number of the interface.
<b>Description</b>	Displays the name of the interface.
<b>Type</b>	Displays the interface text.
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Tx Bytes</b>	Displays the total number of octets sent.
<b>Tx Errors</b>	Shows the total number of errors sent.
<b>Rx Packets</b>	Shows the total number of packets received.
<b>Rx Bytes</b>	Displays the total number of bytes received.
<b>Rx Errors</b>	Shows the total number of errors received.
<b>Status</b>	Shows the operating status of the selected interface.
<b>Unchanged for</b>	Shows the length of time for which the operating status of the interface has not changed.
<b>Action</b>	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.

**Statistics**

Show:	Transfer Totals	Automatic Refresh Interval:	300	Seconds	<b>Apply</b>
Description	en1-5				
MAC Address	00:09:4f:5e:db:66				
IP Address / Netmask					
NAT	Disabled				
Tx Packets	0				
Tx Bytes	0				
Rx Packets	0				
Rx Bytes	0				
TCP Connections					
State	Local Address	Local Port	Remote Address	Remote Port	

Fig. 229: **Monitoring->Interfaces->Statistics->** 

#### Values in the Statistics list

Field	Description
<b>Description</b>	Displays the name of the interface.
<b>MAC Address</b>	Displays the interface text.
<b>IP Address / Netmask</b>	Shows the IP address and the netmask.
<b>NAT</b>	Indicates if NAT is activated for this interface.
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Tx Bytes</b>	Displays the total number of octets sent.
<b>Rx Packets</b>	Shows the total number of packets received.
<b>Rx Bytes</b>	Displays the total number of bytes received.

#### Fields in the TCP Connections menu

Field	Description
<b>Status</b>	Displays the status of an active TCP connection.
<b>Local Address</b>	Displays the local IP address of the interface for an active TCP connection.
<b>Local Port</b>	Displays the local port of the IP address for an active TCP connection.
<b>Remote Address</b>	Displays the IP address to which an active TCP connection exists.
<b>Remote Port</b>	Displays the port to which an active TCP connection exists.

## 20.5 WLAN

### 20.5.1 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.

WLAN1
WLAN2
VSS
Client Management
Bridge Links
Client Links

Automatic Refresh Interval <input type="text" value="60"/> Seconds <span style="float: right;">Apply</span>		
WLAN1 Statistics		
Mbps	Tx Packets	Rx Packets
<b>802.11a/b/g</b>		
54	0	0
48	0	0
36	0	0
24	0	0
18	0	0
12	0	0
11	0	0
9	0	0
6	0	0
5	0	0
2	0	0
1	0	0
<b>802.11n</b>		
144,4	0	0
139	0	0
115,6	0	0
86,7	0	0
72,2	0	0
65	0	0
57,8	0	0
43,3	0	0
28,9	0	0
21,7	0	0
14,4	0	0
7,2	0	0
<b>Total</b>	0	0

Advanced

Fig. 230: **Monitoring->WLAN->WLAN**

#### Values in the WLAN list

Field	Description
<b>mbps</b>	Displays the possible data rates on this wireless module.
<b>Tx Packets</b>	Shows the total number of packets sent for the data rate shown in <b>mbps</b> .

Field	Description
<b>Rx Packets</b>	Shows the total number of received packets for the data rate shown in <b>mbps</b> .

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  Seconds

#	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

Fig. 231: Monitoring->WLAN->WLAN->Advanced

#### Values in the Advanced list

Field	Description
<b>Description</b>	Displays the description of the displayed value.
<b>Value</b>	Displays the statistical value.

#### Meaning of the list entries

Description	Meaning
<b>Unicast MSDUs transmitted successfully</b>	Displays the number of MSDUs successfully sent to unicast addresses since the last reset. An acknowledgement was received for each of these packets.
<b>Multicast MSDUs transmitted successfully</b>	Displays the number of MSDUs successfully sent to multicast addresses (including the broadcast MAC address).
<b>Transmitted MPDUs</b>	Displays the number of MPDUs received successfully.
<b>Multicast MSDUs received successfully</b>	Displays the number of successfully received MSDUs that were sent with a multicast address.
<b>Unicast MPDUs re-</b>	Displays the number of successfully received MSDUs that were

Description	Meaning
<b>ceived successfully</b>	sent with a unicast address.
<b>MSDUs that could not be transmitted</b>	Displays the number of MSDUs that could not be sent.
<b>Frame transmissions without ACK received</b>	Displays the number of sent frames for which an acknowledgment frame was not received.
<b>Duplicate received MSDUs</b>	Displays the number of MSDUs received in duplicate.
<b>CTS frames received in response to an RTS</b>	Displays the number of received CTS (clear to send) frames that were received as a response to RTS (request to send).
<b>Received MPDUs that couldn't be decrypted</b>	Displays the number of received MSDUs that could not be encrypted. One reason for this could be that a suitable key was not entered.
<b>RTS frames with no CTS received</b>	Displays the number of RTS frames for which no CTS was received.
<b>Corrupt Frames Received</b>	Displays the number of frames received incompletely or with errors.

## 20.5.2 VSS

In the **Monitoring->WLAN->VSS** menu, current values and activities of the configured wireless networks are displayed.




<a href="#">WLAN1</a> <a href="#">WLAN2</a> <a href="#">VSS</a> <a href="#">Client Management</a> <a href="#">Bridge Links</a> <a href="#">Client Links</a>										
Automatic Refresh Interval <input type="text" value="60"/> Seconds <input type="button" value="Apply"/>										
Client Node Table										
MAC Address	IP Address	Uptime	Tx Packets	Rx Packets	Signal dBm (RSSI1, RSSI2, RSSI3)	Noise dBm	Data Rate mbps	Rx Discards	Tx Discards	
Feigenblatt (vss7-10 )										
98:d6:f7:61:06:48	10.0.0.15	0 Day(s) 0:0:15	11	17	-89(-89,-103,-105)	-105	1	0	0	

Fig. 232: **Monitoring->WLAN->VSS**


### Values in the VSS list

Field	Description
<b>MAC Address</b>	Shows the MAC address of the associated client.
<b>IP Address</b>	Shows the IP address of the client.
<b>Uptime</b>	Shows the time in hours, minutes and seconds for which the cli-




Field	Description
	ent is logged in.
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Rx Packets</b>	Shows the total number of packets received.
<b>Signal dBm</b> (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
<b>Noise dBm</b>	Shows the received noise strength in dBm.
<b>Data Rate mbps</b>	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.
<b>Rx Discards</b>	Displays the number of received data packets that have been discarded if the bandwidth for receive traffic has been limited in the <b>Wireless LAN-&gt;WLAN-&gt;Wireless Networks (VSS)</b> ->  menu using the field <b>Rx Shaping</b>
<b>Tx Discards</b>	Displays the number of data packets that were queued for transmission and have been discarded if the bandwidth for transmit traffic has been limited in the <b>Wireless LAN-&gt;WLAN-&gt;Wireless Networks (VSS)</b> ->  menu using the field <b>Rx Shaping</b> .

### 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.

<a href="#">WLAN1</a> <a href="#">WLAN2</a> <a href="#">VSS</a> <a href="#">Client Management</a> <a href="#">Bridge Links</a> <a href="#">Client Links</a>						
Automatic Refresh Interval		300	Seconds	<a href="#">Apply</a>		
Client MAC Address	IP Address	Up Time	Signal dBm (RSSI1, RSSI2, RSSI3)	Noise dBm	SNR dB	Data Rate mbps
00:0c:84:03:8b:9a	10.0.0.234	0 Day(s) 0:0:14	-90(-92,-90,-88)	-87	-3	18
Rate	Tx Packets		Rx Packets			
802.11 a/b/g						
54	4		0			
48	0		0			
36	0		0			
24	0		3			
18	0		130			
12	0		78			
11	143		0			
9	0		0			
6	0		16			
5.5	0		0			
2	0		0			
1	4		0			
802.11n						
300	0		0			
270	0		0			
240	0		0			
180	0		0			
150	0		0			
135	0		0			
120	0		0			
90	0		0			
60	0		0			
45	0		0			
30	0		0			
15	0		0			
Total	0		0			
<a href="#">Back</a>						

Fig. 233: **Monitoring->WLAN->VSS-><connected client>->** 

#### Values in the list <Connected Client>

Field	Description
<b>Client MAC Address</b>	Shows the MAC address of the associated client.
<b>IP Address</b>	Shows the IP address of the client.
<b>Uptime</b>	Shows the time in hours, minutes and seconds for which the client is logged in.
<b>Signal dBm(RSSI1, RSSI2, RSSI3)</b>	Shows the received signal strength in dBm.
<b>Noise dBm</b>	Shows the received noise strength in dBm.
<b>SNR dB</b>	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"> <li>• &gt; 25 dB excellent</li> <li>• 15 – 25 dB good</li> <li>• 2 – 15 dB borderline</li> <li>• 0 – 2 dB bad.</li> </ul>
<b>Data Rate mbps</b>	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.
<b>Rate</b>	Displays the possible data rates on the wireless module.
<b>Tx Packets</b>	Shows the number of sent packets for the data rate.
<b>Rx Packets</b>	Shows the number of received packets for the data rate.

### 20.5.3 Client Management

The **Monitoring->WLAN->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.

WLAN1	WLAN2	VSS	Client Management	Bridge Links	Client Links
View 20 per page Filter in None equal Go					
VSS Description	Network Name (SSID)	MAC Address	Active Clients	2,4/5 GHz changeover	Denied Clients soft/hard
vss7-10	default	00:a0:f9:0b:cf:e0	0	0	0/0
Page: 1, Items: 1 - 1					

Fig. 234: **Monitoring->WLAN->Client Management**

#### Values in the list Client Management

Field	Description
<b>VSS Description</b>	Displays the unique description of the wireless network (VSS).
<b>Network Name (SSID)</b>	Displays the name of the wireless network (SSID).

Field	Description
<b>MAC Address</b>	Displays the MAC address being used for this VSS.
<b>Active Clients</b>	Displays the number of active clients.
<b>2,4/5 GHz changeover</b>	Displays the number of clients who have been moved to a different frequency band by the <b>2,4/5 GHz changeover</b> function.
<b>Denied Clients soft/hard</b>	Displays the number of rejected clients after the absolute number of permitted clients has been reached.

## 20.5.4 Bridge Links

In the **Monitoring->WLAN->Bridge Links** menu, current values and activities of the bridge links are displayed.

[WLAN1](#)
[WLAN2](#)
[VSS](#)
[Client Management](#)
[Bridge Links](#)
[Client Links](#)

Automatic Refresh Interval  Seconds


Bridge Link Table										
Bridge Link Description	Remote MAC	First seen	Last seen	Tx Packets	Rx Packets	Signal dBm (RSSI1, RSSI2, RSSI3)	Noise dBm	Tx Data Rate mbps	Rx Data Rate mbps	
wds1-0, Uptime: 0d 1h 19m 54s (WLAN1, Bridge Link Client)										
wbi7-50	00:00:00:00:00:00			0	0	0(0,0,0)	0	0	0	
wds1-1, Uptime: 0d 1h 13m 35s (WLAN2, Bridge Link Master, No slaves connected)										

Fig. 235: **Monitoring->WLAN->Bridge Links**

### Values in the Bridge Links list

Field	Description
<b>Bridge Link Description</b>	Shows the name of the bridge link.
<b>Remote MAC</b>	Shows the MAC address of the bridge link partner.
<b>First seen</b>	Displays the time of the first registered attempted contact of the bridge link partner.
<b>Last seen</b>	Displays the time of the last registered attempted contact of the bridge link partner.
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Rx Packets</b>	Shows the total number of packets received.
<b>Signal dBm (RSSI1, RSSI2, RSSI3)</b>	Shows the received signal strength in dBm.
<b>Noise dBm</b>	Shows the received noise strength in dBm.
<b>Tx Data Rate mbps</b>	Shows the current clock rate of data sent on this bridge link in

Field	Description
	Mbps.
<b>Rx Data Rate mbps</b>	Shows the current clock rate of data received on this bridge link in Mbps.
<b>Uptime</b>	Shows the time in hours, minutes and seconds for which the bridge link in question is active.

### Bridge link details

You can use the  icon to open an overview of further details of the bridge links.

WLAN1 WLAN2 VSS Client Management **Bridge Links** Client Links

Bridge Link Description	Remote MAC	First seen	Last seen	Signal dBm (RSSI1, RSSI2, RSSI3)	Noise dBm	Tx Data Rate mbps	Rx Data Rate mbps
wbl7-50	00:00:00:00:00:00			0(0,0,0)	0	0	0
<b>Rate</b>		<b>Tx Packets</b>			<b>Rx Packets</b>		
<b>802.11a/b/g</b>							
54	0				0		
48	0				0		
36	0				0		
24	0				0		
18	0				0		
12	0				0		
11	0				0		
9	0				0		
6	0				0		
5	0				0		
2	0				0		
1	0				0		
<b>802.11n</b>							
144,4	0				0		
139	0				0		
115,6	0				0		
86,7	0				0		
72,2	0				0		
65	0				0		
57,8	0				0		
43,3	0				0		
28,9	0				0		
21,7	0				0		
14,4	0				0		
7,2	0				0		
<b>Total</b>	<b>0</b>				<b>0</b>		

Back

Fig. 236: Monitoring->WLAN->Bridge Links-> 

### Values in the Bridge Links list

Field	Description
<b>Bridge Link Description</b>	Shows the name of the bridge link.
<b>Remote MAC</b>	Shows the MAC address of the bridge link partner.
<b>First seen</b>	Displays the time of the first registered attempted contact of the bridge link partner.
<b>Last seen</b>	Displays the time of the last registered attempted contact of the bridge link partner.
<b>Signal dBm (RSSI1, RSSI2, RSSI3)</b>	Shows the received signal strength in dBm.
<b>Noise dBm</b>	Shows the received noise strength in dBm.
<b>Tx Data Rate mbps</b>	Shows the current clock rate of data sent on this bridge link in Mbps.
<b>Rx Data Rate mbps</b>	Shows the current clock rate of data received on this bridge link in Mbps.
<b>Rate</b>	For each of the specified data rates, displays the values for <b>Tx Packets</b> and <b>Rx Packets</b> .
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Rx Packets</b>	Shows the total number of packets received.

## 20.5.5 Client Links

In the **Monitoring->WLAN->Client Links** menu, current values and activities of the configured client links are displayed.

[WLAN1](#)
[WLAN2](#)
[VSS](#)
[Client Management](#)
[Bridge Links](#)
[Client Links](#)

Automatic Refresh Interval  Seconds

Client Link Table

Client Link Description	AP MAC Address	Up Time	Tx Packets	Rx Packets	Signal dBm (RSSI1, RSSI2, RSSI3)	Noise dBm	Data Rate mbps
WLAN1 ( )							
sta1-0		0d 20h 41m 42s	0	0	0(0,0,0)	0	0


Fig. 237: **Monitoring->WLAN->Client Links**

### Values in the Client Links list

Field	Description
<b>Client Link Description</b>	Shows the name of the client link.
<b>AP MAC Address</b>	Shows the MAC address of the client link partner.

Field	Description
<b>Uptime</b>	Shows the time in hours, minutes and seconds for which the client link in question is active.
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Rx Packets</b>	Shows the total number of packets received.
<b>Signal dBm</b> (RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
<b>Noise dBm</b>	Shows the received noise strength in dBm.
<b>Data Rate mbps</b>	Shows the current clock rate of data received on this client link in Mbps.

### Client Link Details

You can use the  icon to open an overview of further details of the client links.

[WLAN1](#) [WLAN2](#) [VSS](#) [Client Management](#) [Bridge Links](#) [Client Links](#)

Automatic Refresh Interval <input type="text" value="60"/> Seconds <a href="#">Apply</a>					
AP MAC Address	Uptime	Signal dBm(RSSI1, RSSI2, RSSI3)	Noise dBm	SNR dB	Data Rate mbps
	32d 23h 59m 36s	0(0,0,0)	0	0	0
Rate	Tx Packets		Rx Packets		
<b>802.11a/b/g</b>					
54	0	0	0	0	0
48	0	0	0	0	0
36	0	0	0	0	0
24	0	0	0	0	0
18	0	0	0	0	0
12	0	0	0	0	0
11	0	0	0	0	0
9	0	0	0	0	0
6	0	0	0	0	0
5	0	0	0	0	0
2	0	0	0	0	0
1	0	0	0	0	0
<b>802.11n</b>					
144,4	0	0	0	0	0
139	0	0	0	0	0
115,6	0	0	0	0	0
86,7	0	0	0	0	0
72,2	0	0	0	0	0
65	0	0	0	0	0
57,8	0	0	0	0	0
43,3	0	0	0	0	0
28,9	0	0	0	0	0
21,7	0	0	0	0	0
14,4	0	0	0	0	0
7,2	0	0	0	0	0
Total	0	0	0	0	0

[Back](#)

Fig. 238: Monitoring->WLAN->Client Links-> 

#### Values in the Client Links list

Field	Description
<b>AP MAC Address</b>	Shows the MAC address of the client link partner.
<b>Uptime</b>	Shows the time in hours, minutes and seconds for which the client link in question is active.
<b>Signal dBm (RSSI1, RSSI2, RSSI3)</b>	Shows the received signal strength in dBm.
<b>Noise dBm</b>	Shows the received noise strength in dBm.
<b>SNR dB</b>	Shows the signal quality in dB.
<b>Data Rate mbps</b>	Shows the current clock rate of data received on this client link in Mbps.
<b>Rate</b>	For each of the specified data rates, displays the values for <b>Tx</b>



Field	Description
	<b>Packets</b> and <b>Rx Packets</b> .
<b>Tx Packets</b>	Shows the total number of packets sent.
<b>Rx Packets</b>	Shows the total number of packets received.

## 20.6 Bridges

### 20.6.1 br<x>

In the **Monitoring->Bridges->br<x>** menu, the current values of the configured bridges are shown.

br0

Automatic Refresh Interval  Seconds

MAC Address	Port
00:a0:f9:0b:08:98	en1-0

Fig. 239: **Monitoring->Bridges**

#### Values in the br<x> list

Field	Description
<b>MAC Address</b>	Shows the MAC addresses of the associated bridge.
<b>Port</b>	Shows the port on which the bridge is active.

## 20.7 HotSpot Gateway

### 20.7.1 HotSpot Gateway

A list of all linked hotspot users is displayed in the **Monitoring->HotSpot Gateway->Hot-Spot Gateway** menu.

**HotSpot Gateway**

Automatic Refresh Interval  Seconds

Authenticated HotSpot User

User Name	IP Address	Physical Address	Logon	Interface

Fig. 240: **Monitoring->HotSpot Gateway->HotSpot Gateway**

#### Values in the HotSpot Gateway list

Field	Description
<b>User Name</b>	Displays the user's name.
<b>IP Address</b>	Shows the IP address of the user.
<b>Physical Address</b>	Shows the physical address of the user.
<b>Logon</b>	Displays the time of the notification.
<b>Interface</b>	Shows the interface used.

## 20.8 QoS

In the **Monitoring->QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

### 20.8.1 QoS

A list of all interfaces for which QoS was configured is displayed in the **Monitoring->QoS->QoS** menu.

**QoS**

QoS

Interface	QoS Queue	Send	Dropped	Queued

Fig. 241: **Monitoring->QoS->QoS**

#### Values in the QoS list

Field	Description
<b>Interface</b>	Shows the interface for which QoS has been configured.

Field	Description
<b>QoS Queue</b>	Shows the QoS queue, which has been configured for this interface.
<b>Send</b>	Shows the number of sent packets with the corresponding packet class.
<b>Dropped</b>	Shows the number of rejected packets with the corresponding packet class in case of overloading.
<b>Queued</b>	Shows the number of waiting packets with the corresponding packet class in case of overloading.

## Index

- Interface 75
- Accept Client FQDN 474
- Accept Router Advertisement 138 ,  
309 , 320
- Access 482
- Access Control 170 , 209
- Access Filter 280
- Access Level 98
- Action 175 , 175 , 241 , 280 , 418 ,  
421 , 478 , 491 , 528
- Action to be performed 507
- Active Radio Profile 194
- Additional freely accessible Domain  
Names 520
- Additional IPv4 Traffic Filter 359 , 362
- Address assignment 470
- Address / Prefix 427
- Address / Subnet 427
- Address Mode 137 , 340
- Address Range 427
- Address Type 427
- Admin Status 254
- Administrative FQDNs 474
- Administrative Status 354 , 445
- Advertise 141
- Advertisement send interval 536
- Airtime fairness 156 , 198
- Alert Service 556
- Alive Check 85 , 377 , 383
- All Multicast Groups 301
- Allowed Addresses 170 , 209
- Allowed HotSpot Client 522
- Always on 306 , 313 , 318 , 324 , 332  
, 396 , 403
- AP MAC Address 175
- APN 462
- ARP Lifetime 284
- ARP Processing 204
- Assigned Wireless Network (VSS)  
194
- ATM Interface 339
- ATM PVC 318
- ATM Service Category 343
- Authentication 311 , 316 , 322 , 327 ,  
334 , 399 , 406
- Authentication Method 354 , 372
- Authentication Type 83 , 88
- Auto Subnet Configuration 141
- Autonomous Flag 143
- Autosave Mode 107 , 491
- Bandwidth 154 , 197
- Based on Ethernet Interface 136
- Beacon Period 171 , 201
- Blacklist blocktime 209
- Block after connection failure for 311 ,  
316 , 322 , 327 , 334 , 399 , 406
- Block Time 89 , 377
- Bridge Link Name (ID) 176
- Burst size 270
- CA Certificate 103
- CA Certificates 377
- CA Name 491
- Call Number 330
- Callback 408
- Callback Mode 327
- CAPWAP Encryption 193
- Category 478
- Certificate is CA Certificate 100
- Certificate Request Description 103 ,  
491
- Certificate Revocation List (CRL)  
Checking 100
- Change-over Tolerance 536
- Channel 154 , 175 , 194
- Channel Bundling 329
- Channel Plan 159 , 201
- Class ID 264 , 270
- Class map 264
- Client Band select 169 , 207
- Client Link Description 175
- Client Type 342
- Code 429
- Command Mode 491
- Command Type 491
- Common Name 105

- Compare Condition 485
- Compare Value 485
- Compression 406
- Config Mode 357
- Configuration contains certificates/keys 491
- Congestion Avoidance (RED) 272
- Connected 175
- Connected clients 214
- Connection Idle Timeout 306, 313, 318, 324, 332, 396, 403
- Connection State 260, 276, 524
- Connection Type 324, 396
- Consider 249
- Continuity Check (CC) End-to-End 348
- Continuity Check (CC) Segment 348
- Control Mode 267, 350
- COS Filter (802.1p/Layer 2) 260, 276, 524
- Count 491
- Country 105
- Create NAT Policy 308, 314, 319, 325, 333, 397, 405
- CSV File Format 491
- Custom 105
- Custom DHCP Options 462
- Cyclic Background Scanning 197
- D Channel Mode 368
- Data Packets Sequence Numbers 394
- Day 478
- Default Ethernet for PPPoE Interfaces 340
- Default Idle Timeout 522
- Default Route 308, 314, 319, 325, 333, 357, 397, 405, 413
- Default User Password 83
- Description 93, 100, 110, 193, 197, 228, 231, 240, 254, 260, 264, 270, 276, 280, 306, 313, 318, 324, 332, 339, 354, 362, 372, 380, 385, 392, 396, 403, 413, 425, 426, 427, 428, 429, 432, 445, 464, 485, 491, 524, 528
- Destination 418, 421
- Destination Port/Range 241, 254, 260, 276, 524
- Destination Address / Length 231
- Destination Interface 231, 301
- Destination IP Address/Netmask 227, 241, 254, 362
- Destination IP Address 485, 491, 511
- Destination IPv4 Address/Netmask 260, 276, 524
- Destination IPv6 Address/Length 260, 276, 524
- Destination Port 228, 362
- Destination Port Range 429
- Device 193
- DH Group 372
- DHCP Client on Interface 284
- DHCP Broadcast Flag 144
- DHCP Client 138
- DHCP Client 309, 320
- DHCP Hostname 144, 340
- DHCP MAC Address 144, 340
- DHCP Mode 145
- DHCP Options 460
- DHCP Server 138
- Direction 264, 289
- Distribution Policy 249, 251
- Distribution Mode 249
- Distribution Ratio 251
- DNS assignment via DHCP 284
- DNS domains search list 471
- DNS Hostname 447
- DNS Negotiation 311, 316, 322, 330, 334, 400, 407
- DNS Propagation 145
- DNS Server 336, 387, 411, 458, 471
- Domain 448
- Domain at the HotSpot Server 520
- Dropping Algorithm 272
- DSCP / TOS Value 228
- DSCP/Traffic Class Filter (Layer 3)

- 260 , 276 , 524
- DTIM Period 171 , 201
- DUID 474
- Dynamic blacklisting 209
- E-mail 105
- EAP Preauthentication 167 , 205
- Enable authentication 536
- Enable update 454
- Enabled 413
- Encapsulation 339
- Encrypt configuration 491
- Encryption 89 , 327 , 399 , 406
- Encryption Method 267
- End-to-End Pending Requests 346
- End-to-End Send Interval 346
- Entries 330
- Entry active 83 , 88
- Ethernet Interface 535
- Event 556
- Event List 485 , 491
- Event List Condition 491
- Event Type 485
- Exclude from NAT (DMZ) 284
- External Filename 108 , 109
- Facility 552
- Failed attempts per Time 209
- File Encoding 108 , 109
- File Name 491
- File Name in Flash 491
- Filter 264
- Force certificate to be trusted 100
- Forward 448
- Forward to 448
- Fragmentation Threshold 159 , 201
- From Interface 237
- Frozen Parameters 256
- Function Button Status 485
- Gateway 460
- Gateway Address 231
- Gateway IP Address 227
- General Prefix 141
- General Prefix active 237
- Generate Private Key 103
- Generation Mode 143
- GEO Zone Status 485
- Group Description 83 , 249 , 251 , 284
- Group ID 507
- Hello Intervall 394
- High Priority Class 264
- Host 448
- Host Name 454
- IGMP Proxy 299
- IGMP Snooping 171
- IGMP State Limit 297
- Incoming ISDN Number 408
- Incoming Phone Number 368
- Index Variables 485 , 491
- Interface 72 , 73 , 226 , 234 , 240 , 251 , 267 , 282 , 289 , 297 , 350 , 445 , 448 , 454 , 459 , 470 , 491 , 510 , 520 , 530
- Interface Selection 284
- Interface Action 510
- Interface Mode 136 , 445
- Interface Status 485
- Interface Traffic Condition 485
- Interfaces 264
- Internet Key Exchange 354
- Interval 485 , 491 , 507 , 511
- Intra-cell Repeating 166 , 204
- IP Version of the tunneled Networks 354
- IP Address 340 , 342 , 464 , 535 , 552 , 563
- IP Address Assignment 357
- IP Address / Netmask 137 , 289
- IP Address Mode 308 , 314 , 319 , 325 , 333 , 397 , 405
- IP Address Range 336 , 387 , 411 , 458
- IP Assignment Pool 325 , 357
- IP Assignment Pool (IPCP) 397 , 405
- IP Compression 383
- IP Pool Name 336 , 387 , 411 , 458 , 459
- IP Version 428
- IP Version 445

- IPv4 427
- IPv4 Address 447
- IPv4 Back Route Verify 364
- IPv4 Proxy ARP 364
- IPv4-DNS-Server 448
- IPv6 138 , 309 , 320 , 427
- IPv6 Address 447
- IPv6 Addresses 138
- IPv6 Mode 138 , 309 , 320
- IPv6-DNS-Server 448
- Key Size 491
- Key Value 413
- Language for login window 520
- Last Member Query Interval 297
- Layer 4 Protocol 228
- LCP Alive Check 311 , 316 , 322 , 334 , 399 , 406
- LDAP URL Path 110
- Lease Time 460
- Level 552
- Level No. 93
- Licence Key 68
- Licence Serial Number 68
- Lifetime 372 , 380
- Link Prefix 141
- Local Certificate 372
- Local Certificate Description 108 , 109 , 491
- Local File Name 491
- Local GRE IP Address 413
- Local Hostname 392
- Local ID 354
- Local ID Type 354 , 372
- Local ID Value 372
- Local IP Address 284
- Local IP Address 227 , 308 , 314 , 319 , 325 , 333 , 357 , 394 , 397 , 405 , 413
- Local IPv6 Network 359
- Local PPTP IP Address 316
- Local WLAN SSID 491
- Locality 105
- Location 193
- Login Frameset 522
- Long Retry Limit 201
- Loopback End-to-End 346
- Loopback Segment 346
- MAC Address 136 , 340 , 464
- Mail Exchanger (MX) 455
- Matching String 556
- Max. number of clients - hard limit 169 , 207
- Max. number of clients - soft limit 169 , 207
- Max. Period Active Scan 160
- Max. Period Passive Scan 160
- Max. queue size 272
- Max. Scan Duration 160
- Max. Transmission Rate 198
- Maximum Burst Size (MBS) 343
- Maximum Number of Dialup Retries 311 , 316 , 322 , 327 , 334
- Maximum Response Time 297
- Maximum Retries 394
- Maximum Time between Retries 394
- Maximum Upload Speed 267 , 270 , 350
- Members 425 , 426 , 432
- Menus 94
- Message Compression 556
- Message Timeout 556
- Metric 227 , 231 , 234 , 357
- Metric Offset for Active Interfaces 289
- Metric Offset for Inactive Interfaces 289
- MIB Variables 491
- MIB/SNMP Variable to add/edit 491
- Min. Period Active Scan 160
- Min. Period Passive Scan 160
- Min. queue size 272
- Minimum Time between Retries 394
- MobiKE 364
- Mode 103 , 175 , 228 , 284 , 297 , 330 , 368 , 372 , 385
- Monitored Interface 485
- Monitored Subsystems 556
- Monitored Variable 485
- Monitored Certificate 485

- Monitored GEO Zone 485
- Monitored Interface 510
- Monitored IP Address 507
- Monitoring Mode 538
- MTU 312, 413
- Multicast Group Address 301
- Name 193, 237, 385, 470
- NAT method 240
- NAT Traversal 377
- Netmask 284, 340, 342
- Network Configuration 284
- Network Address 284
- Network Name (SSID) 166, 173, 175, 204
- New Destination IP Address/Netmask 244
- New Destination Port 244
- New Source IP Address/Netmask 244
- New Source Port 244
- Number of Admitted Connections 363
- Number of Messages 556
- Number of Spatial Streams 154, 197
- Number of Used Ports 330
- OAM Flow Level 346
- On Link Flag 143
- Operation Band 154, 197
- Operation Mode 154, 194, 197
- Organization 105
- Organizational Unit 105
- Original Destination Port/Range 241
- Original Destination IP Address/Netmask 241
- Original Source Port/Range 241
- Original Source IP Address/Netmask 241
- OSPF Mode 330, 400, 407
- Outbound Interface 270
- Outgoing ISDN Number 408
- Outgoing Phone Number 368
- Overbooking allowed 270
- Overwrite similar certificate 491
- Password 98, 103, 108, 109, 306, 313, 318, 324, 332, 385, 392, 396, 403, 454, 482, 491, 528
- Password for protected Certificate 491
- Peak Cell Rate (PCR) 343
- Peer Address 354
- Peer ID 354
- Phase-1 Profile 363
- Phase-2 Profile 363
- PIN 462
- Policy 85, 89
- Pool Usage 459
- Pop-Up window for status indication 522
- Port 456
- Post Login URL 520
- PPPoE Ethernet Interface 306
- PPPoE Interfaces for Multilink 306
- PPPoE Mode 306
- PPTP Address Mode 316
- PPTP Ethernet Interface 313
- PPTP Mode 403
- Pre-empt mode (go back into master state) 536
- Preferred Lifetime 143
- Preshared Key 167, 173, 176, 205, 354
- Primary IPv4 DNS Server 445
- Primary IPv6 DNS Server 445
- Prioritisation Algorithm 267
- Prioritize TCP ACK Packets 311, 316, 322, 334, 342, 399
- Priority 83, 88, 270, 445
- Priority Queueing 270
- Propagate PMTU 383
- Proposals 372, 380
- Protocol 234, 241, 254, 260, 276, 362, 429, 456, 491, 524, 552
- Protocol Header Size below Layer 3 267
- Provider 339, 454
- Provider Name 456
- Provisioning Server 462
- Proxy ARP 144
- Proxy ARP Mode 330, 400, 407
- Proxy Interface 299



- Public Interface 364
- Public Interface Mode 364
- Public Source IPv4 Address 364
- Query Interval 297
- Queues/Policies 267
- RA Encrypt Certificate 103
- RA Sign Certificate 103
- RADIUS Dialout 85
- RADIUS Secret 83
- Radius Server 205
- RADIUS Server Group ID 385
- Real Time Jitter Control 267
- Reboot after execution 491
- Reboot device after 491
- Receive Version 287
- Recipient 556
- Remaining Validity 485
- Remote File Name 491
- Remote GRE IP Address 413
- Remote Hostname 392
- Remote IP Address 393
- Remote IPv6 Network 359
- Remote PPTP IP Address 316 , 403
- Remote PPTP IP Address Host Name 403
- Remote User (for Dialin only) 324
- Reporting Method 282
- Response 447
- Retries 85
- Roaming Profile 160
- Robustness 297
- Role 385
- Route 234
- Route Active 231
- Route Announce 287
- Route Class 226
- Route Entries 308 , 314 , 319 , 325 , 333 , 357 , 397 , 405 , 413
- Route Selector 252
- Route Type 226 , 231
- Router Preference 145
- Router Lifetime 145
- RTS Threshold 159 , 201
- RTT Mode (Realtime Traffic Mode) 270
- Rule Chain 280 , 282 , 530
- Rx Shaping 171 , 210
- Save configuration 94
- Scan channels 160
- Scan Interval 160
- Scan Threshold 160
- SCEP URL 103
- Schedule (Start / Stop Time) 478
- Secondary IPv4 DNS Server 445
- Secondary IPv6 DNS Server 445
- Security Mode 167 , 173 , 205
- Security Policy 137 , 138 , 308 , 309 , 314 , 319 , 320 , 357 , 359
- Segment Pending Requests 346
- Segment Send Interval 346
- Select radio 491
- Select vendor 462 , 462
- Selected Channel 154
- Selected Channels 159
- Selected Ports 409
- Selection 428
- Send Version 287
- Send WOL packet over Interface 528
- Server 456
- Server Address 491
- Server IP Address 83 , 88
- Server Timeout 85
- Server URL 491
- Service 241 , 254 , 260 , 276 , 418 , 421 , 524
- Set COS value (802.1p/Layer 2) 264
- Set DSCP/Traffic Class Filter (Layer 3) 264
- Set interface status 491
- Set status 491
- Setup Mode 141
- Severity 556
- Short Guard Interval 159 , 201
- Short Retry Limit 201
- Signal 175
- Silent Deny 282
- SNTP Server 471
- Source 418 , 421

- Source Address / Length 231
- Source Interface 228 , 254 , 301
- Source IP Address/Netmask 228 ,  
241 , 254 , 362
- Source IP Address 485 , 491 , 507 ,  
511
- Source IPv4 Address/Netmask 260 ,  
276 , 524
- Source IPv6 Address/Length 260 ,  
276 , 524
- Source Location 491
- Source Port 228 , 362
- Source Port Range 429
- Source Port/Range 241 , 254 , 260 ,  
276 , 524
- Special Handling Timer 254
- Specific Ports 409
- Start Mode 363
- Start Time 490
- State/Province 105
- Static Addresses 143
- Static Interface Identifier 474
- Status 485
- Stop Time 490
- Subject 556
- Subject Name 491
- Subnet ID 141
- Successful Trials 485 , 507
- Summary 105
- Sustained Cell Rate (SCR) 343
- Switch to SNMP Browser 94
- Synchronisation Mode 539
- TACACS+ Secret 88
- Target MAC-Address 528
- TCP Port 89
- TCP-MSS Clamping 144
- Terms &Conditions 520
- Throughput 214
- Throughput/client 215
- Ticket Type 522
- Time Condition 490
- Timeout 89
- Timestamp 552
- Tracking IP Address 252
- Traffic Shaping 270
- Traffic Direction 485
- Traffic shaping 267
- Transfer Mode 368
- Transfer own IP address over ISDN/  
GSM 368
- Transferred Traffic 485
- Transmit Key 167 , 173 , 205
- Transmit Power 154 , 194
- Transmit Router Advertisement 138
- Transparent MAC Address 73
- Trials 511
- Trigger 510
- Trigger Status 491
- Tunnel Profile 396
- Tx Shaping 171 , 210
- Type 237 , 260 , 276 , 339 , 429 , 524  
, 528
- Type of Messages 552
- Type of traffic 240
- U-APSD 166
- UDP Destination Port 393
- UDP Port 85
- UDP Source Port 393
- UMTS/LTE Interface 332
- Unsuccessful Trials 485 , 507
- Update Interval 456
- Update Path 456
- URL SCEP Server URL 491
- Usage Area 154
- Usage Type 327 , 406
- Use CRL 491
- Use PFS Group 380
- Used Channel 194
- Used Prefix / Length 237
- Used Secondary Channel 154
- User 98
- User Defined Channel Plan 160 , 201
- User must change password 98
- User Name 306 , 313 , 318 , 324 ,  
332 , 396 , 403 , 454 , 482
- Users 385
- Valid Lifetime 143
- Vendor Description 462 , 462

- Vendor Mode 83
- Vendor Option String 462
- Version Check 491
- Virtual Channel Connection (VCC) 343 , 346
- Virtual Channel Identifier (VCI) 339
- Virtual Interface Priority 535
- Virtual Path Connection (VPC) 346
- Virtual Path Identifier (VPI) 339
- Virtual Router Interface 535
- Virtual Router ID 535 , 538 , 539
- Virtual Router IP Address 535
- VLAN 210 , 306
- VLAN ID 136 , 210 , 306
- VLAN Identifier 149
- VLAN Members 149
- VLAN Name 149
- Wake-On-LAN Filter 528
- Wake-On-LAN Rule Chain 528
- Walled Garden 520
- Walled Garden URL 520
- Weight 270
- Wildcard 455
- Wildcard MAC Address 73
- Wildcard Mode 73
- Wireless Mode 156 , 198
- WLC SSID 491
- WMM 166 , 204
- WPA Cipher 167 , 173 , 205
- WPA Mode 167 , 173 , 205
- WPA2 Cipher 167 , 173 , 205
- Write certificate in configuration 491
- XAUTH Profile 363
- 2,4/5 GHz changeover 579
- ACCESS\_ACCEPT 81
- ACCESS\_REJECT 81
- ACCESS\_REQUEST 81
- ACCOUNTING\_START 81
- ACCOUNTING\_STOP 81
- Action 222 , 547 , 566 , 572
- Action if license not registered 476
- Action if server not reachable 476
- Active Clients 579
- ADSL Logic 546
- Alert Service 559
- Alive Check 567
- Answer to client request 515
- AP discovered 212
- AP MAC Address 582 , 584
- AP managed 212
- AP offline 212
- As DHCP Server 444
- As IPCP Server 444
- Attacked Access Point 220
- Authentication for PPP Dialin 91
- Authentication Method 567
- Back Route Verify 235
- Blacklisted 480
- BOSS 546
- Bridge Link Description 580 , 581
- Bytes 567
- Cache Hitrate (%) 451
- Cache Hits 451
- Cache Size 442
- CAPI Server TCP Port 483
- Certificate Request 102
- Channel 570
- Charge 570 , 571
- Class 541
- Client Link Description 582
- Client MAC Address 578
- Compression 78
- Configuration Interface 71
- Configuration Encryption 547
- Confirm Admin Password 60
- Connected clients/VSS 212
- Contact 57
- Corrupt Frames Received 575
- CPU usage [%] 212
- CTS frames received in response to an RTS 575
- Current File Name in Flash 547
- Current Local Time 63
- Data Rate mbps 576 , 578 , 582 , 584
- Date 565
- Default Route Distribution 291
- Delete 220 , 233
- Delete complete IPSec configuration

- 388
- Denied Clients soft/hard 579
- Description 566 , 567 , 572 , 573 , 575
- Destination File Name 547
- Destination IP Address 233
- Details 566
- DHCP Server 187
- Dialling Number 513
- Direction 570 , 571
- DNS domains search list 472
- DNS Requests 451
- DNS Server 473
- Domain Name 442
- Done 222
- Drop non-members 150
- Drop untagged frames 150
- Dropped 569 , 586
- DSA Key Status 77
- Duplicate received MSDUs 575
- Duration 570 , 571
- Dynamic RADIUS Authentication 389
- Enable BRRP 539
- Enable IPsec 388
- Enable server 483
- Enable VLAN 151
- Encrypted 569
- Encryption Algorithms 77
- Error 222
- Errors 567 , 569
- Expires 541
- Extended Route 233
- Factory Reset Firewall 424
- Fallback interface to get DNS server 442
- Faxheader 483
- Filename 547
- Filtered Input Interface(s) 476
- Firewall Status 423
- First seen 220 , 580 , 581
- First Timeserver 64
- Forwarded Requests 451
- Frame transmissions without ACK received 575
- Garbage Collection Timer 292
- Gateway 233
- GRE Window Adaption 410
- GRE Window Size 410
- Hashing Algorithms 77
- Hold Down Timer 293
- Host for multiple locations 523
- HTTPS TCP Port 452
- IGMP State Limit 300
- IGMP Status 300
- Ignore Certificate Request Payloads 390
- IKE (Phase-1) 569
- IKE (Phase-1) SAs 567
- Image already exists. 222
- Include certificates and keys 547
- Incoming Number 513
- Interface 150 , 187 , 233 , 235 , 515 , 570 , 571 , 586 , 586
- Interface Description 71
- Interface is UPnP controlled 515
- Internal Time Server 64
- Invalid DNS Packets 451
- IP Address 576 , 578 , 586
- IP Address / Netmask 573
- IP Address Range 187
- IPsec (Phase-2) 569
- IPsec (Phase-2) SAs 567
- IPsec Debug Level 388
- IPsec over TCP 389
- IPsec Tunnels 568
- IPv4 Firewall Status 423
- ISDN Theft Protection Service 513
- ISDN Timeserver 64
- Last seen 220 , 580 , 581
- LED mode 57
- Level 565
- Licence Key 477
- Licence Status 477
- License valid until 477
- Local Address 573
- Local Certificate 452
- Local ID 567
- Local IP Address 567

- Local Port 567 , 573
- Location 57
- Log Format 555
- Log out immediately 541
- Logged Actions 423
- Logging Level 78
- Login Grace Time 78
- Logon 586
- Logout Options 542
- Loopback active 238
- MAC Address 573 , 576 , 579 , 585
- Management VID 151
- Manual WLAN Controller IP Address 57
- Max. incoming control connections per remote IP Address 410
- Maximum Message Level of Syslog Entries 57
- Maximum E-mails per Minute 559
- Maximum Groups 300
- Maximum Number of Accounting Log Entries 57
- Maximum number of concurrent connections 76
- Maximum Number of History Entries 476
- Maximum Number of Syslog Entries 57
- Maximum Sources 300
- Maximum TTL for Negative Cache Entries 442
- Maximum TTL for Positive Cache Entries 442
- mbps 574
- Memory usage [%] 212
- Message 565
- Messages 567
- Metric 233
- Mode 235 , 300
- Mode / Bridge Group 71
- Monitored Interfaces 513
- MSDUs that could not be transmitted 575
- MTU 567
- Multicast MSDUs transmitted successfully 575
- Multicast MSDUs received successfully 575
- Multicast Routing 296
- NAT 573
- NAT active 238
- NAT Detection 567
- Negative Cache 442
- Negotiation Type 567
- Netmask 233
- Network Name (SSID) 220
- Network Name (SSID) 579
- New File Name 547
- No. 235 , 565 , 572
- Noise dBm 576 , 578 , 580 , 581 , 582 , 584
- Number of Dialling Retries 514
- Other Inactivity 423
- Outgoing Number 513
- Overview 213
- Packets 567
- Passed 569
- Password 559
- Physical Address 586
- Poisoned Reverse 291
- POP3 Timeout 559
- POP3 Server 559
- Port 238 , 585
- Positive Cache 442
- Power Off Timeout 59
- PPTP Inactivity 423
- PPTP Passthrough 238
- Primary DHCP Server 465
- Prioritize SIP Calls 437
- Protocol 233
- PVID 150
- QoS Queue 586
- Queued 586
- Rate 578 , 581 , 584
- Received DNS Packets 451
- Received MPDUs that couldn't be decrypted 575
- Region 178 , 187

- Remote Address 573
- Remote ID 567
- Remote IP 566
- Remote IP Address 541
- Remote IP Address 567
- Remote MAC 580 , 581
- Remote Networks 566
- Remote Number 570 , 571
- Remote Port 567 , 573
- Restore Default Settings 74
- Retransmission Timer 293
- RFC 2091 Variable Timer 291
- RFC 2453 Variable Timer 291
- RIP UDP Port 291
- Rogue Client MAC Address 220
- Route Timeout 292
- Route Type 233
- RSA Key Status 77
- RTS frames with no CTS received  
575
- RTSP Port 439
- RTSP Proxy 439
- Running 222
- Rx Bytes 572 , 573
- Rx Errors 572
- Rx Packets 572 , 573 , 574 , 576 ,  
578 , 580 , 581 , 582 , 584
- Schedule Interval 502
- Second Timeserver 64
- Secondary DHCP Server 465
- Security Algorithm 566
- Select file 547
- Send 586
- Send Certificate Chains 390
- Send Certificate Request Payloads  
390
- Send CRLs 390
- Send Initial Contact Message 389
- Send Key Hash Payloads 390
- Sender E-mail Address 559
- Server preference 473
- Server Failures 451
- Service 570 , 571
- Set Date 63
- Set Time 63
- Show passwords and keys in clear text  
61
- Signal 216
- Signal dBm 220
- Silent Deny 238
- SIP Port 437
- SIP Proxy 437
- Slave AP LED mode 187
- Slave AP location 187
- SMS Device 560
- SMTP Authentication 559
- SMTP Port 559
- SMTP Server 559
- SNMP Listen UDP Port 80
- SNMP multicast discovery 80
- SNMP Read Community 60
- SNMP Trap Broadcasting 562
- SNMP Trap Community 562
- SNMP Trap UDP Port 562
- SNMP Version 80
- SNMP Write Community 60
- SNR dB 578 , 584
- SNTP Server 473
- Source File Name 547
- Source Location 222 , 547
- SSH Port 76
- SSH service active 76
- SSID 220
- Stack 570
- Start Time 571
- Static Blacklist 220
- Status 566 , 568 , 570 , 572 , 573
- Subsystem 565
- Successfully Answered Queries 451
- Sync SAs with ISP interface state 389
- System Admin Password 60
- System Logic 546
- System Name 57
- TCP Inactivity 423
- TCP Keepalives 78
- Test Ping Address 543
- Test Ping Mode 543
- Third Timeserver 64

Throughput 216  
 Time 565  
 Time Update Interval 64 , 66  
 Time Update Policy 64  
 Time Zone 63  
 Timeout 514  
 Total 569  
 Traceroute Address 544  
 Traceroute Mode 544  
 Transmitted MPDUs 575  
 Tx Bytes 572 , 573  
 Tx Errors 572  
 Tx Packets 572 , 573 , 574 , 576 ,  
 578 , 580 , 581 , 582 , 584  
 Type 572  
 Type of attack 220  
 UDP Destination Port 401  
 UDP Inactivity 423  
 UDP Source Port Selection 401  
 Unchanged for 572  
 Unicast MPDUs received successfully  
 575  
 Unicast MSDUs transmitted successfully  
 575  
 Update Timer 292  
 UPnP Status 516  
 UPnP TCP Port 516  
 Uptime 576 , 578 , 580 , 582 , 584  
 URL 222 , 547  
 URL / IP Address 480  
 URL Path Depth 476  
 Use Interface 543  
 Use Zero Cookies 389  
 User 541  
 User Name 559 , 586  
 Value 575  
 VSS Description 579  
 Web Filter Status 476  
 Whitelisted 480  
 WINS Server 442  
 WLAN Controller: VSS throughput  
 212  
 Zero Cookie Size 389  
 Access Filter 275  
 Access Profiles 91  
 Actions 491  
 Active Clients 215  
 Address List 426  
 Administration 151  
 Alert Recipient 556  
 Alert Settings 559  
 Black / White List 480  
 Bridge Links 176 , 580  
 Cache 450  
 Call History 570  
 Certificate List 99  
 Certificate Servers 110  
 Client Link 172  
 Client Links 582  
 Client Management 217 , 579  
 Controlled Interfaces 349  
 CRLs 108  
 Current Calls 569  
 Date and Time 61  
 DHCP Configuration 458  
 DHCP Relay Settings 464  
 DHCPv6 Global Options 472  
 DHCPv6 Server 470  
 DNS Servers 444  
 DNS Test 543  
 Domain Forwarding 448  
 Drop In Groups 283  
 Dynamic Hosts 450  
 DynDNS Provider 455  
 DynDNS Update 453  
 Filter List 478  
 Firmware Maintenance 222  
 General 187 , 476 , 516  
 General Prefix Configuration 236  
 Global Settings 442  
 GRE Tunnels 412  
 Groups 424 , 428 , 431  
 History 481  
 Hosts 506  
 HotSpot Gateway 519  
 HTTP 74  
 HTTPS 74  
 HTTPS Server 452

- Interface Assignment 281 , 530
- Interfaces 70 , 134 , 509 , 515 , 554
- IP Pool Configuration 457
- IP Pools 336 , 386 , 411
- IP/MAC Binding 463
- IPSec Peers 352
- IPSec Statistics 568
- IPSec Tunnels 566
- IPv4 Filter Rules 416
- IPv4 Route Configuration 224
- IPv4 Routing Table 233
- IPv4/IPv6 Filter 259
- IPv6 Route Configuration 230
- IPv6 Routing Table 234
- ISDN 323
- ISDN Login 74
- Load Balancing Groups 248
- Log out Users 541
- NAT Configuration 239
- NAT Interfaces 238
- Neighbor APs 218
- OAM Controlling 345
- Options 90 , 234 , 299 , 387 , 401 ,  
410 , 422 , 437 , 483 , 502 , 512 ,  
523 , 539 , 545 , 554
- Passwords 59
- Phase-1 Profiles 370
- Phase-2 Profiles 379
- Ping 74
- Ping Generator 510
- Ping Test 542
- Port Configuration 150
- PPPoA 317
- PPPoE 305
- PPTP 312
- PPTP Tunnels 402
- Profiles 338
- QoS Classification 263
- QoS Interfaces/Policies 266
- Radio Profiles 196
- Radio Settings 152
- RADIUS 81
- RIP Filter 288
- RIP Interfaces 286
- RIP Options 291
- Rogue APs 219
- Rogue Clients 220
- RTSP Proxy 438
- Rule Chains 279
- Service Categories 342
- Service List 429
- Slave Access Points 192 , 213
- SNMP 74 , 79
- SNMP Trap Hosts 563
- SNMP Trap Options 561
- Special Session Handling 253
- SSH 74 , 75
- Stateful Clients 473
- Static Hosts 447
- Statistics 451 , 571
- Syslog Servers 551
- System 56
- System Licences 66
- System Messages 565
- System Reboot 549
- TACACS+ 87
- Telnet 74
- Traceroute Test 544
- Trigger 484
- Tunnel Profiles 391
- UMTS/LTE 331
- User 481
- Users 95 , 395
- Virtual Routers 532
- VLANs 149
- VR Synchronisation 538
- VSS 576
- Wake-On-LAN Filter 524
- Wireless Networks (VSS) 163 , 203 ,  
217
- WLAN Controller 212
- WOL Rules 528
- XAUTH Profiles 384
- Access Rules 273
- Additional IPv4 Traffic Filter 351
- Addresses 426
- Administration 177
- Administrative Access 74



- Alert Service 556
- ATM 337
- Bridges 585
- BRRP 531
- CAPI Server 481
- Certificates 99
- Controller Configuration 187
- DHCP Server 457
- DHCPv6 Server 468
- Diagnostics 542
- DNS 440
- Drop In 283
- DynDNS Client 453
- Factory Reset 550
- Forwarding 301
- General 295
- Global Settings 56
- GRE 412
- HotSpot Gateway 517 , 585
- HTTPS 452
- IGMP 296
- Interface Mode / Bridge Groups 68
- Interfaces 424 , 571
- Internal Log 565
- IP Accounting 554
- IP Configuration 134
- IPSec 351 , 566
- IPv6 General Prefixes 236
- ISDN Theft Protection 512
- ISDN/Modem 569
- L2TP 391
- Load Balancing 248
- Log out Users 541
- Maintenance 221
- Monitoring 211
- NAT 238
- Neighbor Monitoring 218
- Policies 416
- PPTP 402
- QoS 259 , 586
- Real Time Jitter Control 349
- Reboot 549
- Remote Authentication 81
- RIP 286
- Routes 224
- RTSP 438
- Scheduling 484
- Services 429
- SIA 563
- SIP 437
- Slave AP configuration 191
- SNMP 561
- Software & Configuration 544
- Surveillance 506
- Syslog 551
- UPnP 514
- VLAN 147
- Wake-On-LAN 524
- Web Filter 475
- WLAN 152
- External Reporting 551
- Firewall 415
- LAN 134
- Maintenance 541
- Networking 224
- VPN 351
- Wireless LAN 152
- Wireless LAN Controller 181
- DHCP-Client (Configuration example) 465
- DHCP-Relay-Server (Configuration example) 465
- DHCP-Server (Configuration example) 465
- NAT (Configuration example) 246
- SIF (Configuration example) 433
- #
- #1#2, #3 106
- A**
- Access Type 133
- Active IPSec Tunnels 54
- Active Sessions (SIF, RTP, etc... ) 54
- Actual Network 125 , 132
- ADSL Line Profile 123
- APN (Access Point Name) 125

- Assistants 52
- Authentication Method 131
- Autoconfiguration on Bootup 115
- B**
- Bearer Service 119
- BOSS Version 54
- C**
- Cell ID 132
- Cloud NetManager address 57
- Cloud NetManager communication 57
- Configuration Access 91
- Configuration example - DHCP-Client 465
- Configuration example - DHCP-Relay-Server 465
- Configuration example - DHCP-Server 465
- Configuration example - Load balancing 256
- Configuration example - NAT 246
- Configuration example - Scheduling 503
- Configuration example - SIF 433
- Configuration example - Time-controlled Tasks 503
- Configuration example - WLAN 178
- Configured Speed / Mode 113
- CPU Usage 54
- Current Speed / Mode 113
- D**
- Description - Connection Information - Link 56
- Device 132
- Downstream 122
- DSL Chipset 121
- DSL Configuration 120
- DSL Mode 122
- DSL Modem 120
- E**
- Ethernet Ports 111
- Ethernet Interface Selection 113
- F**
- Fallback Number 125
- Fixed IP Address 131
- H**
- Home PLMN 132
- I**
- ICC ID 132
- IMEI 132
- Incoming Service Type 125
- Interface - Connection Information - Link 55
- Internet + Dialup 303
- IP Address Owner 531
- ISDN Configuration 115
- ISDN Configuration Type 115
- ISDN Port 119
- ISDN Ports 114
- ISDN Usage External 54
- L**
- Last Command 132
- Last configuration stored 54
- Last Reply 132
- Load balancing (Configuration example) 256
- Local Services 440
- Location Area Code 132
- M**
- Maximum Upstream Bandwidth 122
- Memory Usage 54
- Mobile Network Provider 130
- Modem Model 132
- Modem Status 125
- Monitoring 565
- MSN 119

MSN Recognition 119  
 MSN Configuration 117  
 Multicast 294

**N**

Name 133  
 Network Provider 125  
 Network Quality 125 , 132

**O**

Oper Status 132  
 Operation Mode (Active) 491  
 Operation Mode (Inactive) 491

**P**

Password 131  
 Physical Connection 121  
 Physical Interfaces 111  
 PLMN 133  
 Port Configuration 112  
 Port Name 115  
 Port Usage 115  
 Preferred Network Type 125  
 Primary IP Address 531  
 PUK 125

**R**

Radio1 214  
 Result of Autoconfiguration 115  
 Roaming Mode 130  
 Role 176  
 Routing Protocols 286  
 Rx Data Rate mbps 580 , 581

**S**

Scheduling (Configuration example)  
     503  
 Selected PLMN 132  
 Serial Number 54  
 Service 119  
 Service Center Address 132

Show Manufacturer Names 57  
 Signal dBm (RSSI1, RSSI2, RSSI3)  
     576 , 578 , 580 , 581 , 582 , 584  
 SIM Card Uses PIN 125  
 State 133  
 Status 53  
 Subscriber Number 132  
 Switch Port 113  
 System Management 53  
 System Date 54

**T**

Time-controlled Tasks (Configuration  
     example) 503  
 Transmit Shaping 122  
 Tx Data Rate mbps 580 , 581

**U**

UMTS/LTE 123  
 UMTS/LTE Status 125  
 Upstream 122  
 Uptime 54  
 Username 131

**V**

Virtual Router 531  
 Virtual Router Backup 531  
 Virtual Router Master 531  
 VoIP 437  
 VRRP Advertisement 531  
 VRRP router 531

**W**

Walled Network / Netmask 520  
 WAN 303  
 WEP Key 1-4 167 , 173 , 205  
 WLAN 574  
 WLAN (Configuration example) 178  
 WLANx 574

**X**

X.31 (X.25 in D Channel)	116
X.31 TEI Service	116
X.31 TEI Value	116