Manual
bintec Rxxx2/RTxxx2

Reference

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.

Table of Contents

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 R series

1.1.1 Setting up and connecting

Note

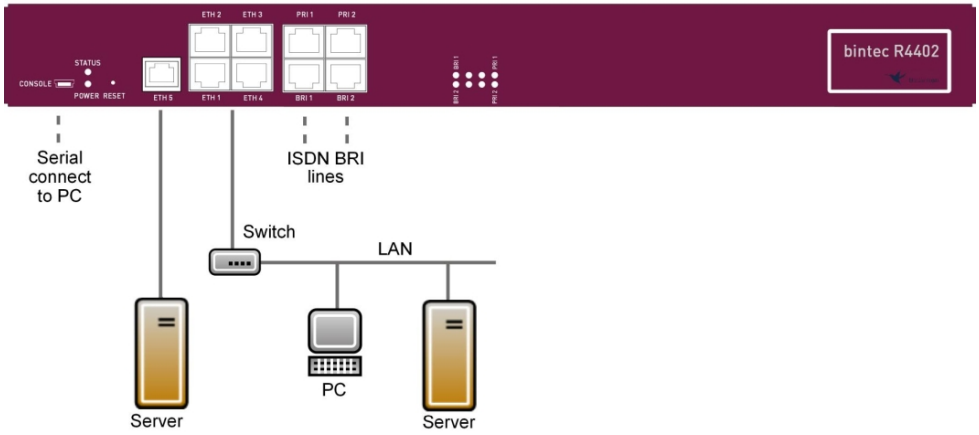
All you need for this is the cable supplied with the equipment.

Caution

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 an ISDN interface of the device, if any, 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.



When setting up and connecting, carry out the steps in the following sequence (refer to the connection diagrams for the individual devices in chapter on page):

(1) LAN

For the standard configuration of your device via Ethernet, connect the first switch port (**ETH1**) of your device to your LAN using the Ethernet cable supplied. The device automatically detects whether it is connected to a switch or directly to a PC.

(2) ADSL (only **bintec R3002**)

Connect the DSL interface (**DSL**) of your device to the DSL output of the splitter using the DSL cable supplied.

(3) SHDSL (only **bintec R3802**)

Connect the SHDSL interface (**SHDSL**) of your device to the SHDSL connection using the DSL cable supplied.

(4) VDSL (only **bintec R3502**)

Connect the VDSL2 interface (**VDSL**) of your device to the VDSL connection using the VDSL cable supplied.

(5) Mains connection

Connect the device to a plug socket. The power connection is located on the back of the device.

You can set up further connections as required:

- ISDN-BRI

  (see *Variable switching of S0 interfaces* on page 30)

  Connect the ISDN BRI interface (**BRI1** or **BRI2**) of the device to your ISDN socket using the ISDN BRI cable provided.

- ISDN-PRI (only **bintec R4402**)

  Connect the ISDN PRI interface (**PRI-1** or **PRI-2**) of the device to your PRI connection

using the ISDN PRI cable provided.

- Other LANs

  Connect any other terminals in your network to the remaining switch ports **ETH2**, **ETH3**, **ETH4** or **ETH5**) of your device using other Ethernet cables.

- Serial connection

  For alternative configuration possibilities, connect the serial interface of your PC (**COM1** or **COM2**) to the serial interface of the gateway (**console**). However, configuration via the serial interface is not provided by default.

The device is now ready for configuration with the **GUI**. Chapter *Basic configuration* on page 34 provides a detailed step-by-step guide to the basic functions on your device.

Installation

The devices are optionally equipped as a table top unit or for installation in 19 inch cabinet.

Use as a table-top device

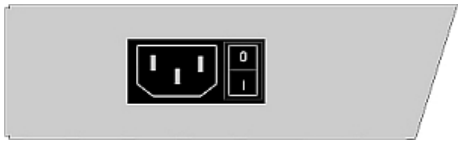
Affix the rubber feet supplied to the marked areas on the underside of the device. Place your device on a solid, level base.

The 19- inch cabinet installation

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

1.1.2 Connectors

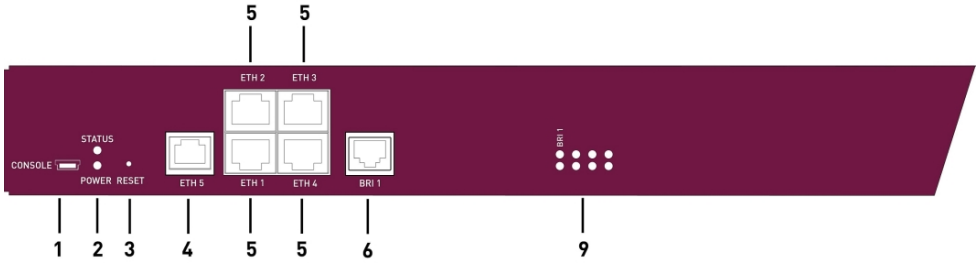
The network connection and the on/off switch are located on the back of the device. All other connections are located on the front of the device.



Connectors bintec R1202

bintec R1202 has a 4-port Ethernet switch, a serial interface, an ETH5 interface and an ISDN BRI interface.

The connections are arranged as follows:



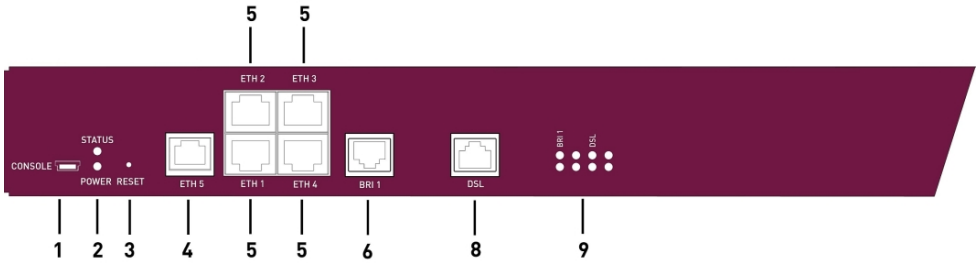
Front of bintec R1202

1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1	ISDN BRI interface
9	LED	LED display

Connectors bintec R3002, bintec R3502 and bintec 3802

bintec R3002, **bintec R3502** and **bintec 3802** have a 4-port Ethernet switch, a serial interface, an ETH5 interface and an ISDN BRI interface as well as a DSL interface.

The connections are arranged as follows:



Front of bintec R3002, bintec R3502, bintec R3802

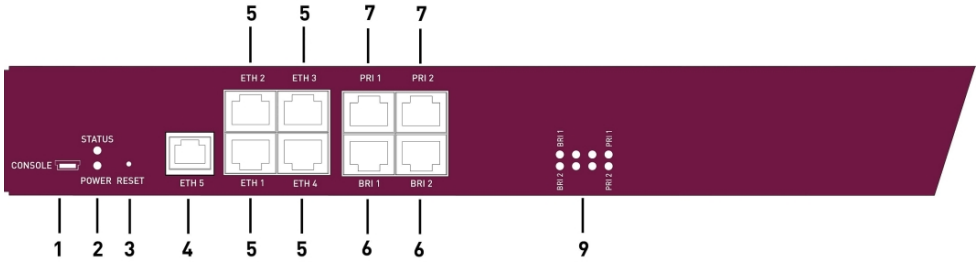
1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1	ISDN BRI interface

8	DSL	DSL interface (ADSL2+ interface for **bintec R3002**, VDSL2 interface for **bintec R3502**, SHDSL interface for **bintec R3802**)
9	LED	LED display

Connectors bintec R4402

bintec R4402 has a 4-port Ethernet switch, a serial interface, an ETH5 interface, two ISDN BRI interfaces and two ISDN PRI interfaces.

The connections are arranged as follows:



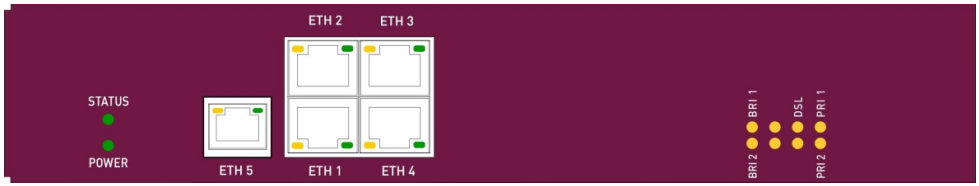
Front of bintec R4402

1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1 - BRI2	ISDN BRI interface
7	PRI1 - PRI2	ISDN-PRI interface
9	LED	LED display

1.1.3 LEDs

The device LEDs provide information on certain activities and statuses of the device.

The LEDs are arranged as follows:



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

LED status display

LED	Colour	Status	Information
POWER	green	on	The 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.
ETH 1 to 5	green	on	The device is connected to the Ethernet at 1 Gbps
	green	flashing	Data traffic with 1 Gbps.
	orange	on	The device is connected to the Ethernet at 100 mbps.
	orange	flashing	Data traffic with 100 mbps.
	green and orange	on	The device is connected to the Ethernet at 10 mbps.
	green and orange	flashing	Data traffic with 10 mbps.
BRI 1 to 2	orange	on	D-channel is active.
		flashing	At least one B-channel is active.
PRI 1 to 2	orange	on	D-channel is active.
		flashing	At least one B-channel is active.
		off	The device is terminated or the connected could not be established.
DSL	orange	on	DSL synchronisation successful. The DSL connection is active (ADSL/SHDSL/VDSL).
		flashing	Data traffic via the DSL connection (ADSL/SHDSL/VDSL).

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

LED.

LED BRRP display

LED	Colour	Status	Information
STATUS	green	lights	The device is functioning as a master router.
STATUS	green	off	The device is functioning as a backup router.
STATUS	green	flashing	The device is being initialised.

1.1.4 Scope of supply

Your device is supplied with the following parts:

Scope of supply	bintec R1202	bintec R3002	bintec R3502
Cable sets/mains unit/ other	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfad-heive	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfad-heive 2 ADSL cable (for An-nex A and for Annex B)	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfad-heive VDSL cablel
Software	Companion DVD, Dime Manager (on DVD)	Companion DVD, Dime Manager (on DVD)	Companion DVD, Dime Manager (on DVD)
Documentation	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if re-quired	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if re-quired	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if re-quired
Online documentation	User´s Guide (auf DVD) Workshops MIB-Referenz	User´s Guide (auf DVD) Workshops MIB-Referenz	User´s Guide (auf DVD) Workshops MIB-Referenz

Scope of supply	bintec R3802	bintec R4402	
Cable sets/mains unit/ other	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfad-heive SHDSL cable	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfad-heive ISDN-PRI cable	
Software	Companion DVD, Dime Manager (on DVD)	Companion DVD, Dime Manager (on DVD)	
Documentation	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if re-quired	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if re-quired	
Online documentation	User´s Guide (auf DVD) Workshops MIB-Referenz	User´s Guide (auf DVD) Workshops MIB-Referenz	

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 of the devices the **bintec R series** are summarized in the following table:

General product features

Property	bintec R series
Dimensions and weights:	
Equipment dimensions without cable (B x H x D):	19" housing (482.6 mm x 220 mm x 45 mm)
Weight	approx. 2.0 kg

Property	bintec R series
Transport weight (incl. documentation, cables, packaging)	approx. 2.6 kg
Memory	64 MB RAM, 16 MB flash ROM
Power consumption of the device	max. 15 Watt, normally 13 Watt
Voltage supply	Voltage Range 85 ~ 264 V AC Frequency Range 47 ~ 63 Hz Efficiency (Typ.) 79 %
Environmental requirements:	
Storage temperature	-25 °C to +70 °C
Operating temperature	0 °C to +40 °C
Relative atmospheric humidity	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored
Room classification	Only use in dry rooms.
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

Interfaces, sockets, LEDs

Property	bintec R1202	bintec R3002	bintec R3502
Available interfaces:			
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, MDIX
ETH5	Permanently installed (twisted pair only),	Permanently installed (twisted pair only),	Permanently installed (twisted pair only),

Property	bintec R1202	bintec R3002	bintec R3502
	10/100/1000 mbps, autosensing, MDIX	10/100/1000 mbps, autosensing, MDIX	10/100/1000 mbps, autosensing, MDIX
ISDN BRI (S0)	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode
Console/RS232	Baudrates: 1200 - 115200 Baud	Baudrates: 1200 - 115200 Baud	Baudrates: 1200 - 115200 Baud
ADSL2+ interface	-	Internal ADSL2+ modem for Annex A and Annex B	-
VDSL2 interface	-	-	In accordance with ITU G.993.2; supports Baud plan ISDN 998. Autodetection of VDSL profile.
Available sockets:			
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket	5-pole mini USB socket
Ethernet interfaces	RJ45 socket	RJ45 socket	RJ45 socket
ISDN BRI interface	RJ45 socket	RJ45 socket	RJ45 socket
ADSL interface	RJ45 socket	-	-
VDSL2 interface	-	RJ45 socket	-
LEDs	13 (1x Power, 1x Status, 5x2 Ethernet, 1x Function)	14 (1x Power, 1x Status, 5x2 Ethernet, 2x Function)	14 (1x Power, 1x Status, 5x2 Ethernet, 2x Function)

Interfaces, sockets, LEDs

Property	bintec R3802	bintec R4402	
Available interfaces:			
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps,	Permanently installed (twisted pair only), 10/100/1000 mbps,	

Property	bintec R3802	bintec R4402	
	autosensing, MDIX	autosensing, MDIX	
ETH5	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, MDIX	
ISDN BRI (S0)	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode	
Console/RS232	Baudrates: 1200 - 115200 Baud	Baudrates: 1200 - 115200 Baud	
SHDSL interface	Supports SHDSL.bis. Internal SHDSL 8 wire modem. Bonding technology with 2-wire/4-wire/6-wire/8-wire as an inverse multiplexer - performed over IMA in accordance with the ATM forum.	-	
ISDN-PRI (2)	-	ISDN Primary Rate Interface TE or NT mode	
Available sockets:			
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket	
Ethernet interfaces	RJ45 socket	RJ45 socket	
ISDN BRI interface	RJ45 socket	RJ45 socket	
SHDSL interface	RJ45 socket	-	
ISDN-PRI interface	-	RJ45 socket	
LEDs	14 (1x Power, 1x	16 (1x Power, 1x	

Property	bintec R3802	bintec R4402	
	Status, 5x2 Ethernet, 2x Function)	Status, 5x2 Ethernet, 4x Function)	

1.1.6 Reset

Resetting the device enables you to return your device to a predefined initial state. This may be necessary if you have made incorrect configuration settings or the device is to be reprogrammed.

Manually resetting the device

You can reset the device to the ex works state with the **RESET** button. Depending on how long it is pressed for, the **RESET** button performs two different functions:

- After pressing briefly once, the device reboots.
- Hold the **RESET** button until the **STATUS** LED starts to flash. The device performs a factory reset. This means the device is returned to its ex works state. The boot configuration is deleted and all passwords are reset.

1.2 bintec RT series

1.2.1 Setting up and connecting

Note

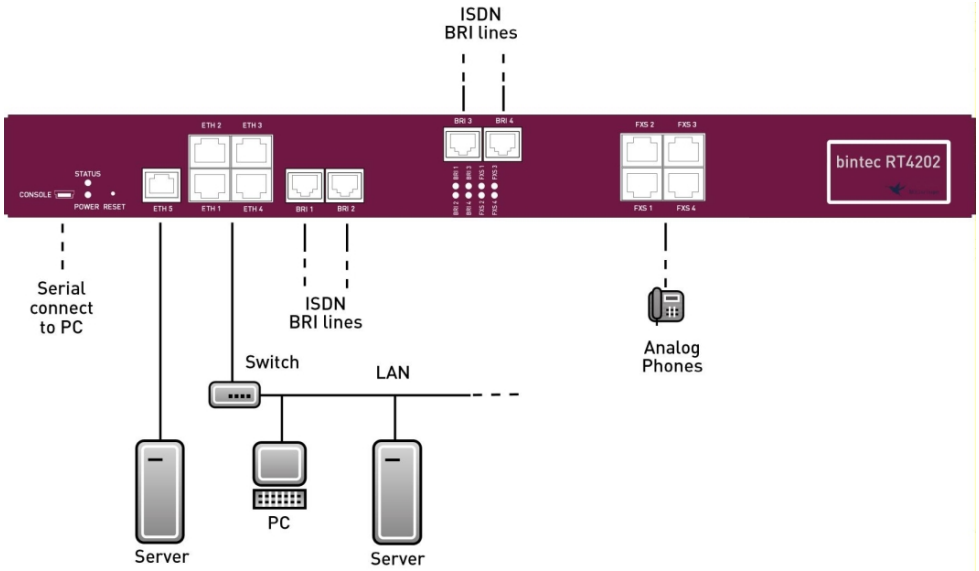
All you need for this is the cable supplied with the equipment.

Caution

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 an ISDN interface of the device, if any, 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.



When setting up and connecting, carry out the steps in the following sequence (refer to the connection diagrams for the individual devices in chapter on page):

(1) LAN

For the standard configuration of your device via Ethernet, connect the first switch port (**ETH1**) of your device to your LAN using the Ethernet cable supplied. The device automatically detects whether it is connected to a switch or directly to a PC.

(2) ADSL (only **bintec RT3002**)

Connect the DSL interface (**DSL**) of your device to the DSL output of the splitter using the DSL cable supplied.

(3) Mains connection

Connect the device to a plug socket. The power connection is located on the back of the device.

You can set up further connections as required:

- ISDN-BRI

  (see *Variable switching of S0 interfaces* on page 30)

  Connect the ISDN BRI interface (**BRI1, BRI2** or **BRI3, BRI4**) of the device to your ISDN socket using the ISDN BRI cable provided.

- Other LANs

  Connect any other terminals in your network to the remaining switch ports **ETH2**, **ETH3**, **ETH4** or **ETH5**) of your device using other Ethernet cables.

- Serial connection

For alternative configuration possibilities, connect the serial interface of your PC (**COM1** or **COM2**) to the serial interface of the gateway (**console**). However, configuration via the serial interface is not provided by default.

- Analog telephone /analog fax (only **bintec RT4202**)

  Connect your analog telephone or your analog fax to the **FXS** connections.

The device is now ready for configuration with the **GUI**. Chapter *Basic configuration* on page 34 provides a detailed step-by-step guide to the basic functions on your device.

Installation

The devices are optionally equipped as a table top unit or for installation in 19 inch cabinet.

Use as a table-top device

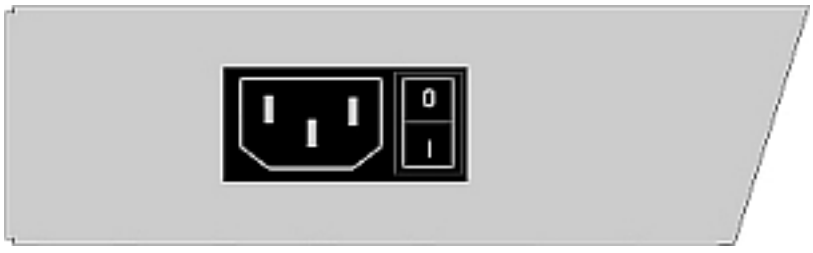
Affix the rubber feet supplied to the marked areas on the underside of the device. Place your device on a solid, level base.

The 19- inch cabinet installation

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

1.2.2 Connectors

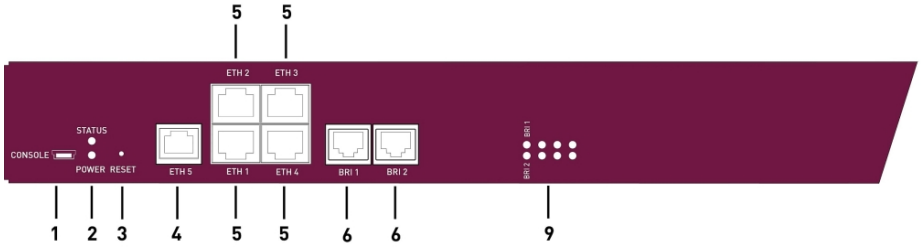
The network connection and the on/off switch are located on the back of the device. All other connections are located on the front of the device.



bintec RT1202

bintec RT1202 has a 4-port Ethernet switch, a serial interface, an ETH5 interface and two ISDN BRI interfaces.

The connections are arranged as follows:



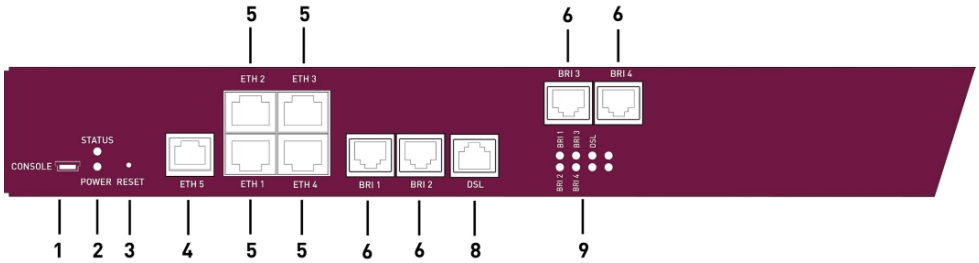
Front of bintec RT1202

1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1 - BRI2	ISDN BRI interface
9	LED	LED display

bintec RT3002

bintec RT3002 have a 4-port Ethernet switch, a serial interface, an ETH5 interface, four ISDN BRI interfaces as well as a DSL interface.

The connections are arranged as follows:



Front of bintec RT3002

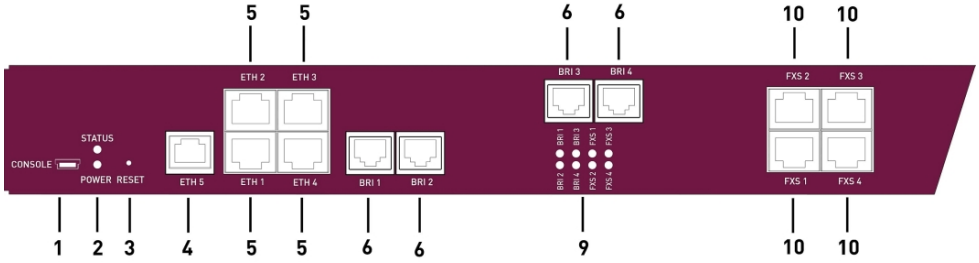
1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1 - BRI4	ISDN BRI interface

8	DSL	ADSL2+ interface
9	LED	LED display

bintec RT4202

bintec RT4202 has a 4-port Ethernet switch, a serial interface, an ETH5 interface, four ISDN BRI interfaces and four FXS interfaces.

The connections are arranged as follows:



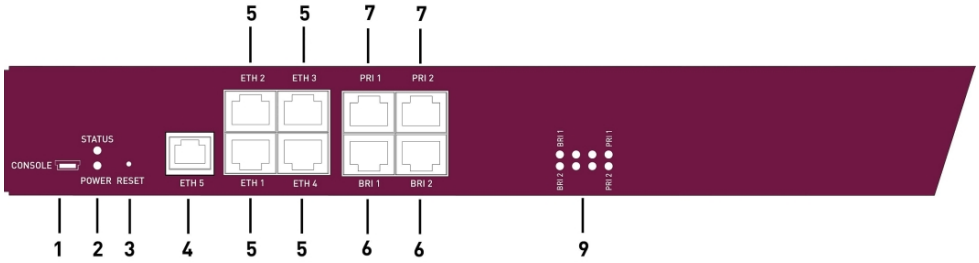
Front of bintec RT4202

1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1 - BRI4	ISDN BRI interface
9	LED	LED display
10	FXS1 - FXS4	FXS interfaces

bintec RT4402

bintec RT4402 has a 4-port Ethernet switch, a serial interface, an ETH5 interface, two ISDN BRI interfaces and two ISDN PRI interfaces.

The connections are arranged as follows:



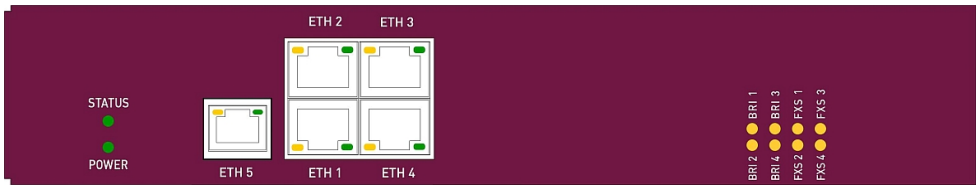
Front of bintec RT4402

1	CONSOLE	Serial interface
2	POWER / STATUS	LED display for power and status
3	RESET	Reset button
4	ETH5	Ethernet interface
5	ETH1 - ETH4	10/100/1000 Base-T Ethernet interface
6	BRI1 - BRI2	ISDN BRI interface
7	PRI1 - PRI2	ISDN-PRI interface
9	LED	LED display

1.2.3 LEDs

The device LEDs provide information on certain activities and statuses of the device.

The LEDs are arranged as follows:



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

LED status display

LED	Colour	Status	Information
POWER	green	on	The 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.

LED	Colour	Status	Information
	green	off	During operation: An error has occurred.
ETH 1 to 5	green	on	The device is connected to the Ethernet at 1 Gbps
	green	flashing	Data traffic with 1 Gbps.
	orange	on	The device is connected to the Ethernet at 100 mbps.
	orange	flashing	Data traffic with 100 mbps.
	green and orange	on	The device is connected to the Ethernet at 10 mbps.
	green and orange	flashing	Data traffic with 10 mbps.
BRI 1 to 4	orange	on	D-channel is active.
		flashing	At least one B-channel is active.
PRI 1 to 2	orange	on	D-channel is active.
		flashing	At least one B-channel is active.
FXS 1 to 4	orange	on	Incoming call to terminal.
		off	The device is terminated or the connected could not be established.
DSL	orange	on	DSL synchronisation successful. The DSL connection is active (ADSL/SHDSL/VDSL).
		flashing	Data traffic via the DSL connection (ADSL/SHDSL/VDSL).

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

LED BRRP display

LED	Colour	Status	Information
STATUS	green	lights	The device is functioning as a master router.
STATUS	green	off	The device is functioning as a backup router.
STATUS	green	flashing	The device is being initialised.

1.2.4 Scope of supply

Your device is supplied with the following parts:

Scope of supply	bintec RT1202	bintec RT3002
Cable sets/mains unit/ other	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfadheive	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfadheive 2 ADSL cable (for Annex A and for Annex B)
Software	Companion DVD, Dime Manager (on DVD)	Companion DVD, Dime Manager (on DVD)
Documentation	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if required	Quick Install Guide and safety notices (printed) Installation poster (printed) Release Notes, if required
Online documentation	User´s Guide (auf DVD) Workshops MIB-Referenz	User´s Guide (auf DVD) Workshops MIB-Referenz

Scope of supply	bintec RT4202	bintec RT4402
Cable sets/mains unit/ other	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfadheive	Ethernet cable ISDN-BRI cable Serial cable Network cable 19.inch installation kit 4x rubber feet - selfadheive ISDN-PRI cable
Software	Companion DVD, Dime Manager (on DVD)	Companion DVD, Dime Manager (on DVD)
Documentation	Quick Install Guide and safety notices (printed)	Quick Install Guide and safety notices (printed)

Scope of supply	bintec RT4202	bintec RT4402
	Installation poster (printed) Release Notes, if required	Installation poster (printed) Release Notes, if required
Online documentation	User´s Guide (auf DVD) Workshops MIB-Referenz	User´s Guide (auf DVD) Workshops MIB-Referenz

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 of the devices the **bintec RT series** are summarized in the following table:

General product features

Property	bintec RT series
Dimensions and weights:	
Equipment dimensions without cable (B x H x D):	19" housing (482.6 mm x 220 mm x 45 mm)
Weight	approx. 2.0 kg
Transport weight (incl. documentation, cables, packaging)	approx. 2.6 kg
Memory	64 MB RAM, 16 MB flash ROM
Power consumption of the device	max. 15 Watt, normally 13 Watt
Voltage supply	Voltage Range 85 ~ 264 V AC Frequency Range 47 ~ 63 Hz Efficiency (Typ.) 79 %
Environmental requirements:	
Storage temperature	-25 °C to +70 °C
Operating temperature	0 °C to +40 °C

Property	bintec RT series
Relative atmospheric humidity	10 % to 90 % non-condensing in operation, 5 % to 95 % non-condensing when stored
Room classification	Only use in dry rooms.
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

Interfaces, sockets, LEDs

Property	bintec RT1202	bintec RT3002
Available interfaces:		
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX
ETH5	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX
ISDN BRI (S0)	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode
Console/RS232	Baudrates: 1200 - 115200 Baud	Baudrates: 1200 - 115200 Baud
ADSL2+ interface	-	Internal ADSL2+ modem for Annex A and Annex B
Available sockets:		
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket
Ethernet interfaces	RJ45 socket	RJ45 socket

Property	bintec RT1202	bintec RT3002
ISDN BRI interface	RJ45 socket	RJ45 socket
ADSL interface	RJ45 socket	-
LEDs	14 (1x Power, 1x Status, 5x2 Ethernet, 2x Function)	17 (1x Power, 1x Status, 5x2 Ethernet, 5x Function)

Interfaces, sockets, LEDs

Property	bintec RT4202	bintec RT4402
Available interfaces:		
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX
ETH5	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX
ISDN BRI (S0)	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode	Euro-ISDN (point-to-multipoint/point-to-point connection) Only TE mode
Console/RS232	Baudrates: 1200 - 115200 Baud	Baudrates: 1200 - 115200 Baud
FXS (internal)	4x for connection of analog telephones or FAX	-
ISDN-PRI (2)	-	ISDN Primary Rate Interface TE or NT mode
Available sockets:		
Serial interface V.24	5-pole mini USB socket	5-pole mini USB socket
Ethernet interfaces	RJ45 socket	RJ45 socket
ISDN BRI interface	RJ45 socket	RJ45 socket
FXS	4x RJ45 socket	-

Property	bintec RT4202	bintec RT4402
ISDN-PRI interface	-	RJ45 socket
LEDs	20 (1x Power, 1x Status, 5x2 Ethernet, 8x Function)	16 (1x Power, 1x Status, 5x2 Ethernet, 4x Function)

1.2.6 Reset

Resetting the device enables you to return your device to a predefined initial state. This may be necessary if you have made incorrect configuration settings or the device is to be reprogrammed.

Manually resetting the device

You can reset the device to the ex works state with the **RESET** button. Depending on how long it is pressed for, the **RESET** button performs two different functions:

- After pressing briefly once, the device reboots.
- Hold the **RESET** button until the **STATUS** LED starts to flash. The device performs a factory reset. This means the device is returned to its ex works state. The boot configuration is deleted and all passwords are reset.

1.3 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.

1.4 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* .

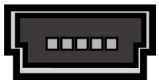
1.5 Pin Assignments

1.5.1 Serial interface

Your device has a serial interface for connection to a console. This supports Baud rates from 1200 to 115200 Bps.

The interface is designed as a 5-pole mini USB socket.

1 5



The pin assignment is as follows:

Pin assignment of the mini USB socket

Pin	Position
1	Not used
2	TxD
3	RxD
4	Not used
5	GND

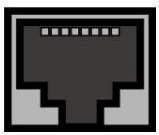
1.5.2 Ethernet interface

The devices have an Ethernet interface with an integrated 4-port switch (ETH1 - ETH4) and a separate Ethernet interface (ETH5).

The 4-port switch is used to connect individual PCs or additional switches. The ETH5 interface can be used to connect an optional DSL modem or a DMZ.

The connection is made via an RJ45 socket.

1 8



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

RJ45 socket for Ethernet connection

Pin	Position
1	Pair 0 +

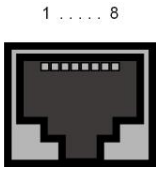
Pin	Position
2	Pair 0 -
3	Pair 1 +
4	Pair 2 +
5	Pair 2 -
6	Pair 1 -
7	Pair 3 +
8	Pair 3 -

The Ethernet 10/100/1000 BASE-T interface does not have an Auto-MDI-X function.

1.5.3 ADSL interface

The ADSL interface on **bintec R3002** and **RT3002** is connected via an RJ45 plug. The cable supplied connects the RJ45 plug needed for the device to an RJ11 plug provided for Annex A. The second cable supplied connected the RJ45 plug with an RJ45 plug for Annex B.

The following pins are used for the ADSL connection:



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

RJ45 socket for ADSL connection bintec R3002 and RT3002

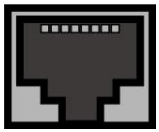
Pin	Position
1	Not used
2	Not used
3	Not used
4	Line 1a
5	Line 1b
6	Not used
7	Not used
8	Not used

1.5.4 SHDSL interface

The SHDSL interface on **bintec R3802** is connected via an RJ45 connector. The cable supplied connects the RJ45 connector needed for the device to an RJ45 connector needed for the SHDSL connection.

The following pins are used for the SHDSL connection:

1 8



The pin assignment for the SHDSL interface (RJ45 connector) is as follows:

RJ45 socket for SHDSL connection bintec R3802

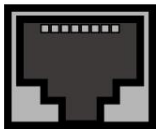
Pin	Position
1	Line a4
2	Line b4
3	Line a3
4	Line a1
5	Line b1
6	Line b3
7	Line a2
8	Line b2

1.5.5 VDSL2 interface

The VDSL2 interface on **bintec R3502** is connected via an RJ45 plug.

The following pins are used for the VDSL connection:

1 8



The pin assignment for the VDSL2 interface (RJ45 connector) is as follows:

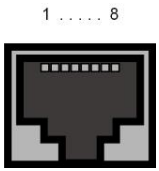
RJ45 socket for VDSL connection bintec R3502

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

1.5.6 ISDN-PRI interface

Both of the ISDN PRI interfaces on **bintec R4402** are connected via an RJ45 plug. The cable supplied connects the RJ45 plug needed for the device to an RJ45 plug needed for the PRI connection.

The following pins are used for the connection:



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

RJ45 socket for ISDN PRI connection

Pin	Position
1	T+
2	T-
3	Not used
4	R+
5	R-
6	Not used
7	Not used
8	Not used

Note for NTs in Germany

Note

In Germany, "Transmit" (NT-->TE) is often designated "S2Mab" (a and b) on the plug and "Receive" (TE-->NT) "S2Man" (a and b).

1.5.7 ISDN BRI interface

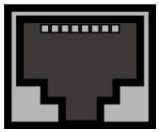
The devices **bintec R1202**, **R3002**, **R3502** and **R3802** have an ISDN BRI interface, which e.g. can be used for backup functions. The devices **bintec R4402** and **RT1202** have two ISDN BRI interfaces. The devices **bintec RT3002** and **RT4202** have four ISDN BRI interfaces.

The devices **bintec R1202**, **R3002**, **R3502** and **R3802** can only be operated in TE mode.

The devices **bintec R4402** and **bintec RT series** can be operated in TE mode or in NT mode.

The connection is made via an RJ45 socket:

1 8



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

RJ45 socket for ISDN connection in TE mode

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

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

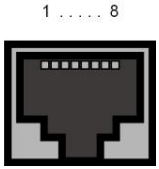
RJ45 socket for ISDN connection in NT mode

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

1.5.8 FXS interface

bintec RT4202 has four FXS interfaces.

The connection is made via an RJ45 socket.



The pin assignment for the FXS interface (RJ45 connector) is as follows:

RJ45 connector for FXS 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

Chapter 2 Variable switching of S0 interfaces

2.1 Switching the S0 interfaces from external to internal

The devices **bintec R4402**, **bintec RT1202**, **bintec RT3002**, **bintec RT3502** and **bintec RT4202** have two or four BRI connections. All BRI connections can be operated as internal or as external S0 connections. The external S0 connections are used for connection to the network operator's ISDN network. The internal S0 connections are provided for connecting various ISDN terminals (telephone, PC, etc.). In the ex works state, the BRI connections are configured as external connections.

The two S0 interfaces BRI-1 and BRI-2 can be switch from external (ex works state) to internal via a link plug field on the PCB for the device. Additional interfaces BRI-3 and BRI-4 can be switched via the link plugs on the side of the ISDN-L module.

If you use a S0 interface as an internal connection, you can specify for each interface whether or not the connection is powered via your device when the conncted terminal does not have its own power supply. The respective link plugs must be moved to do this.

In addition, you can switch the 100 Ohm terminators on/off for each interface via additional link plugs. You require terminators:

- if you connect an external connection directly with the external NTBA
- for a point-to-point connection
- if the bus starts directly with the connection of your device

You can also connect the interfaces BRI-3 and BRI-4 to each other. This can guarantee the power supply for a terminal on an BRI interface switched to internal mode in the event that your device is switched off or the power supply fails. For example, an external S0 can be placed on an internal S0. In this case, an idle relay loops through from external S0 to internal S0 and so creates an emergency supply for the internal S0 bus/telephone.

Warning

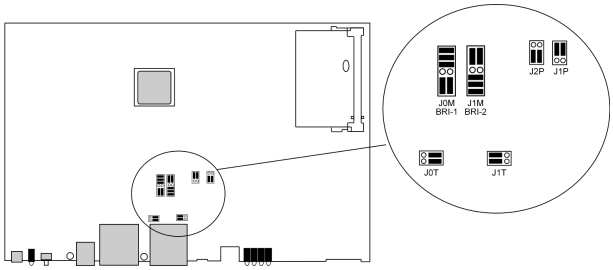
Always remove the power cord before opening the device. This is the only way of ensuring that the internal mains unit is completely dead. If you do not remove the power cord, there is a risk of injury or death.

Note that the device should only be opened by trained service personnel.

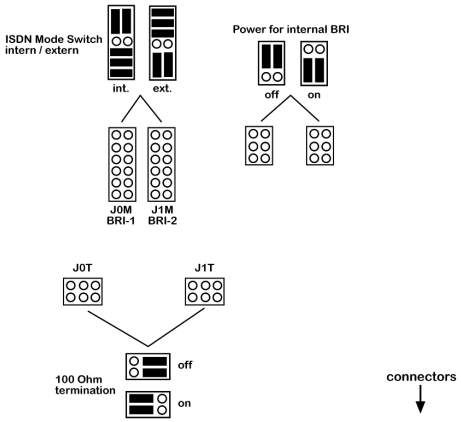
To carry out the switch proceed as follows:

Unscrew the two screws on the back of the device and slide the cover upwards.

The link plugs for the BRI-1 and BRI-2 interfaces can be found on all devices on the main PCB behind the terminal block.

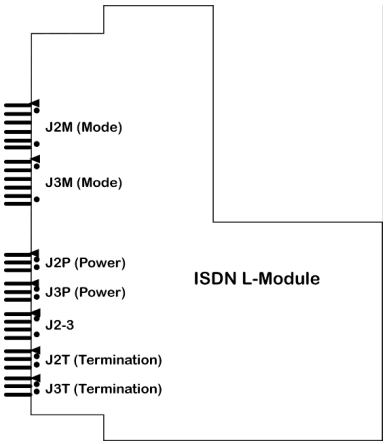


Insert the link plugs for interfaces BRI-1 and BRI-2 as shown in the following figure:

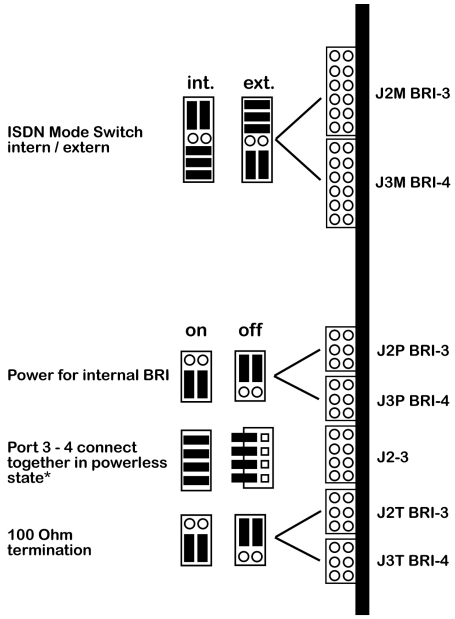


Use	Interface	Link plug area	Position	Position
Internal/external switching	BRI-1	J0M	Internal 	external 
Internal/external switching	BRI-2	J1M	Internal 	external 
Power supply for internal connection	BRI-1	J0P	Off 	On 
Power supply for internal connection	BRI-2	J1P	Off 	On 
100 Ohm terminator	BRI-1	J0T	Off 	On 
100 Ohm terminator	BRI-2	J1T	Off 	On 

You can also switch the interfaces BRI-3 and BRI-4. The link plugs are on the side of the ISDN-L module.



Insert the link plugs for interfaces BRI-3 and BRI-4 as shown in the following figure:



* "on" position ist only allowed if J3M BRI-3" is in "int." Mode and "J4M BRI-4" is in "ext." Mode

* "on" is only permitted, if J3M BRI-3 is set to internal mode and J4M BRI-4 is set to external mode.

Use	Interface	Link plug area	Position	Position
Internal/external switching	BRI-3	J2M		

Use	Interface	Link plug area	Position	Position
				
Internal/external switching	BRI-4	J3M	Internal 	external 
Power supply for internal connection	BRI-3	J2P	Off 	On 
Power supply for internal connection	BRI-4	J3P	Off 	On 
100 Ohm terminator	BRI-3	J2T	Off 	On 
100 Ohm terminator	BRI-4	J3T	Off 	On 
Connection of BRI-3 and BRI-4	-	J2-3	Off 	On 

Chapter 3 Basic configuration

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

The way to obtain the basic configuration is explained below step-by-step. Detailed knowledge of networks is not necessary. A detailed online help system gives you extra support.

The **Companion DVD** also supplied includes all the tools that you need for the configuration and management of your device.

3.1 Presettings

3.1.1 Preconfigured data

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 38.

3.1.2 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 40.

3.2 System requirements

Your bintec elmeg gateway contains extensive features for encrypted data transfer and Internet access for both individual users and companies.

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

- Microsoft Windows operating system Windows 2000 or higher
- Internet Explorer 6 or 7, Mozilla Firefox Version 1.2 or higher
- Installed network card (Ethernet)
- DVD drive
- TCP/IP protocol installed (see *Configuring a PC* on page 37)
- High colour display (more than 256 colours) for correct representation of the graphics.

3.3 Preparation

To prepare for configuration, you need to...

- gather the data required for the basic configuration and the Internet connection
- Check whether the PC from which you want to perform the configuration meets the necessary requirements.

You can also...

- install the **Dime Manager** software, which provides more tools for working with your device. This installation is optional and not essential for the configuration or operation of the device.

3.3.1 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.

If necessary, you can use the sample values.

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

- Basic configuration (if your device is in the ex works state)
- Internet access (optional)

The following table shows examples of possible values for the necessary access data. You can enter your personal data in the "Your values" column, so that you can refer to these

values later when needed.

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

Basic configuration

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

Basic information

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

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 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	*GoInternet*	
Protocol	*PPP over Ethernet (PPPoE)*	
Encapsulation	*bridged-no-fcs*	
VPI (Virtual Path Identifier)	*1*	
VCI (Virtual Circuit Identifier)	*32*	
Your user name	*MyName*	
Password	*TopSecret*	

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)	*000123456789*	

Access data	Example value	Your values
T-Online number (usually 12 digits)	*06112345678*	
Joint user account	*0001*	

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.

You user name could, for example, look like this:

000123456789061123456 78#0001@t-online.de

3.3.2 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.

- Make sure that the TCP/IP protocol is installed on the PC.
- Assign fixed IP address to your PC.

Checking the TCP/IP protocol

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

(1) Click the Windows Start button and then **Settings** -> **Control Panel** -> **Network Connections** (Windows XP) or **Control Panel** -> **Network and Sharing Center**-> **Change Adapter Settings** (Windows 7).

(2) Click on **LAN Connection**.

(3) Click on **Properties** in the status window.

(4) Look for the **Internet Protocol (TCP/IP)** entry in the list of network components.

Installing the TCP/IP protocol

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

(1) First click **Properties**, then **Install** in the status window of the **LAN Connection**.

(2) Select the **Protocol** entry.

(3) Click **Add**.

(4) Select **Internet Protocol (TCP/IP)** and click on **OK**.

(5) Follow the on-screen instructions and restart your PC when you have finished.

Allocating PC IP address

Allocate an IP address to your PC as follows:

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

(2) Choose **Use next IP address** and enter a suitable IP address.

Entering the gateway IP address in your PC

Then continue by entering the IP address of the gateway in the configuration of your PC as follows:

(1) In **Internet Protocol (TCP/IP)** -> **Properties** under **Default gateway**, enter the IP address of your gateway.

(2) Enter the IP address of your device under **Use next DNS server address**.

(3) Click **OK**.

(4) Close the status window with**OK**.

The computer now has an IPSec configuration.

Note

You can now launch the **GUI** for configuration by entering the IP address of your device (192.168.0.250) in a supported browser (Internet Explorer 6 or later, Mozilla Firefox 1.2 or later) and entering the pre-configured login information (**User**: *admin*, **Password**: *admin*).

3.4 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.

3.5 Setting up an internet connection

You can establish various types of internet connection with your device. The most common configuration is described below. The **GUI** internet wizard can be used to help configure alternative configuration types.

3.5.1 Internet connection over internal ADSL modem

The devices **R3002** and **RT3002** have an integrated ADSL2+ modem for establishing a fast internet connection. To make it easier to configure an ADSL internet connection, the **GUI** has a **Assistants** 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.

3.5.2 Other internet connections

In addition to an ADSL connection over the internal ADSL2+ modem, 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**.

3.5.3 Testing the configuration

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

Carry out the following steps to test your device:

(1) Test the connection to your device. Click **Run** in the Start menu and enter `ping`, followed by a space and the IP address of your system (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* 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 one or more WANs).

3.6 Software Update

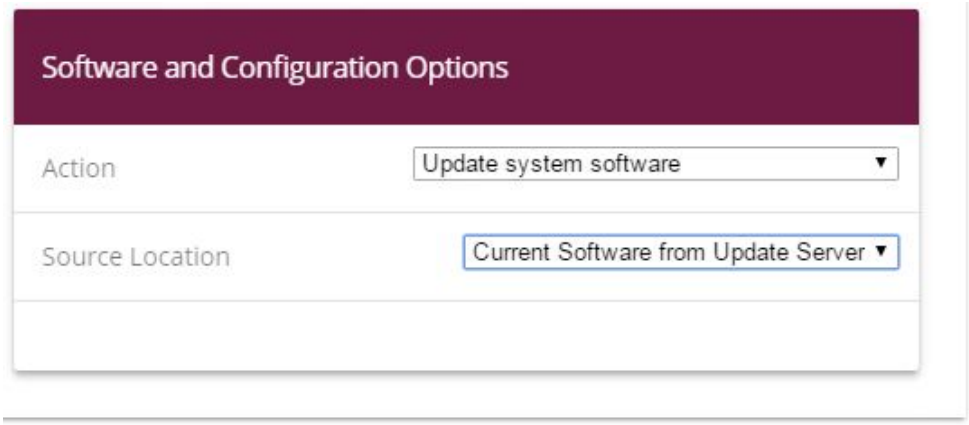
The range of functions of bintec elmeg devices is continuously being extended. These extensions are made available to you by bintec elmeg GmbH free of charge. Checking for new software versions and the installation of updates can be carried out easily with the **GUI**. An existing internet connection is needed for an automatic update.

Proceed as follows:

(1) Go to the **Maintenance**->**Software &Configuration** menu.

(2) Select under **Action** *`Update system software`*and under **Source Location** *`Current Software from Update Server`*

(3) Confirm with **Go**.



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

Caution

Once you have clicked on **GO** , the update cannot be cancelled/interrupted. If an error occurs during the update, do not re-start the device and contact support.

Chapter 4 Access and configuration

This chapter describes all the access and configuration options.

4.1 Access Options

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

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

- Via your LAN
- Via the serial interface
- Via an ISDN connection

4.1.1 Access via LAN

Access via one of the Ethernet interfaces of your device allows you to 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.

4.1.1.1 HTTP/HTTPS

With a current web browser, you can use the HTML interfaces 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*

4.1.1.2 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 48.

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 48.

4.1.1.3 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 47).

(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 *Call up the GUI .* on page 51.

(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 47.

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 the device.

(2) Continue with *Login* on page 47.

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.

4.1.2 Access via the Serial Interface

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

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

Windows

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

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

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

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

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

Check

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

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

(1) Click on **File** ->**Properties**.

(2) Click **Configure** in the **Connect to** tab.
The following settings are necessary:
- Bits per second: *9600*
- Data bits: *8*
- Parity: *open*
- Stopbits: *1*
- Flow control: *open*

(3) Enter the values and click **OK**.

(4) Make the following settings in the **Settings** tab:
- Emulation: *VT100*

(5) Click **OK**.

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

If you use HyperTerminal, there may be problems with displaying umlauts and other special characters. If necessary, therefore, set HyperTerminal to *Autodetection* instead of *VT 100*.

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 9600 -c/dev/ttyS1`

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

4.1.3 Access over ISDN

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

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

Note

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

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

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

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

(1) Connect your device to the ISDN.

(2) Log in as administrator on your device in the remote LAN in the usual way.

(3) In the SNMP shell, type in `isdnlogin <number of the ISDN connection of your device>`, e.g. `isdnlogin 1234`.

(4) The login prompt appears. You are now in the SNMP shell of your device.

Continue with *Logging in for Configuration* on page 48.

4.2 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.

4.2.1 User names and passwords in ex works state

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

User names and passwords in ex works state

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

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

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

Caution

All bintec elmeg devices are delivered with the same username and password. As long as the password remains unchanged, they are therefore not protected against unauthorised use. How to change the passwords is described in *Passwords* on page 67.

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.

4.2.2 Logging in for Configuration

Set up a connection to the device. The access options are described in *Access Options* on page 42.

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. `R4402:>`. 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**.

4.3 Configuration options

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

You can configure your device in the following ways:

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

Note

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

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

Types of connections and configurations

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

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

Note

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

4.3.1 GUI (Graphical User Interface)

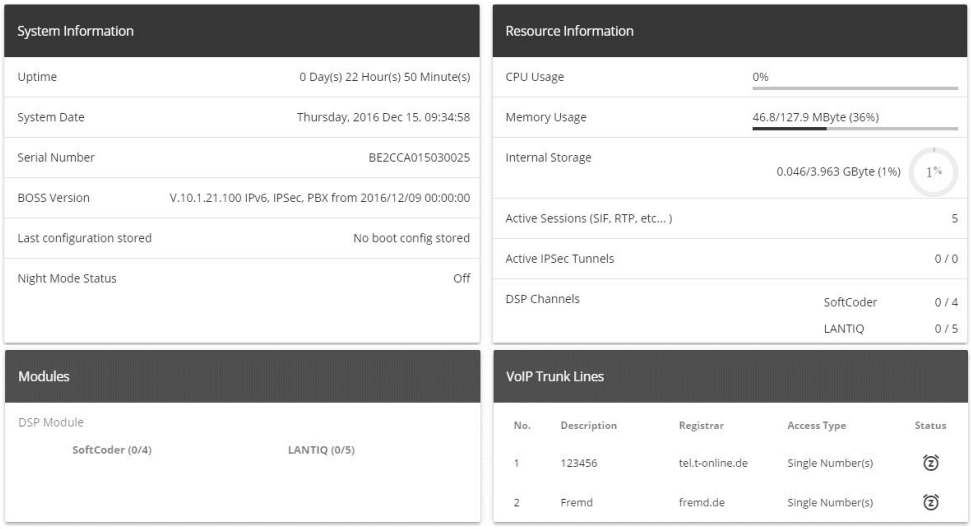
The **GUI** is a web-based graphic user surface that you can use from any PC with an up-to-date Web browser via an HTTP or HTTPS connection.

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 *Software &Configuration* on page 505 of *www.bintec-elmeg.com* and installed on your device. To do this, proceed as described in *Options* on page 505.

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.



4.3.1.1 Call up the 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 37).

(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**.

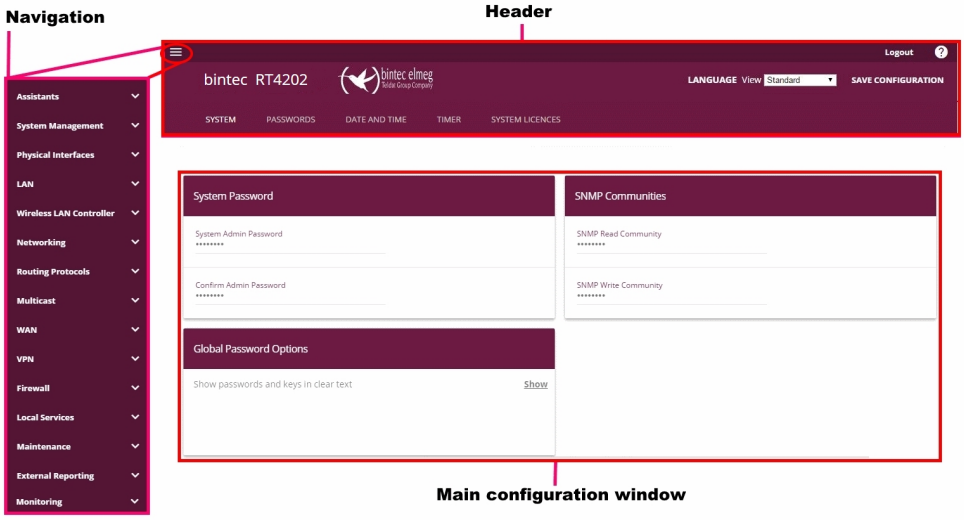
You are now in the status menu of your device's **GUI** (see *Status* on page 61).

4.3.1.2 Operating elements

GUI window

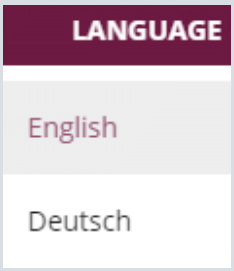
The **GUI** window is divided into three areas:

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

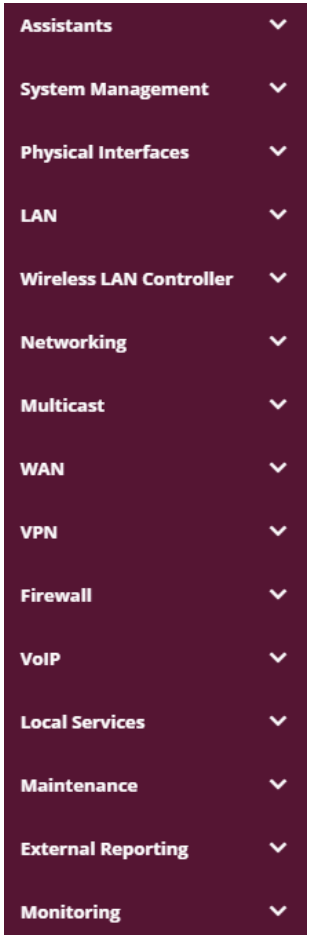


Header

Configuration interface header bar

Menu	Function
	Opens the navigation bar.
	**Logout**: 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: • Continue with the configuration, • Save the configuration and close the window, • Exit the configuration without saving.
	**Online Help**: Click this button if you want help with the menu now active. The description of the sub-menu where you are now is displayed.
	**Language**: From the dropdown menu, select the language in which the configuration interface is to be displayed. Here, you can select the language in which you want to carry out the configuration. *German* and *English* are available.
	**View**: Select the desired view from the dropdown menu. Standard and SNMP browsers can be selected.
	Save configuration button. If you click the **Save configuration** button, you will be asked "Do you really want to save the current configuration as a boot configuration?" You can • Save configuration • Save configuration with boot backup

Navigation bar



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

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

If you go to the sub-menu you want, the entry selected will be displayed in color. After selecting the sub-menu the navigation bar will be closed.

Status page

If you open the configuration interface 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 configuration interface are triggered by means of the following buttons:

Buttons

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

GUI buttons for special functions

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

Various icons indicate the following possible actions or statuses:

Symbols

Icon	Function
	Deletes the list entry.
	Displays the menu for changing the settings of an entry.
	Displays the details for an entry.
	Voicemail message can be intercepted.
	Messages will be saved.
	Select the button to go to the **elmeg** IP1x0 telephone user interface administrator page.
	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 `Inactive`.
	Sets the status of the entry to `Active`.
	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 that data traffic is encrypted.
	Triggers a WLAN bandscan.
	Displays the next page in a list.

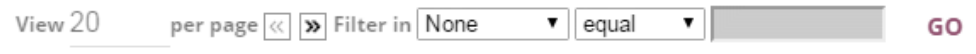
Icon	Function
«	Displays the previous page in a list.

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

List options

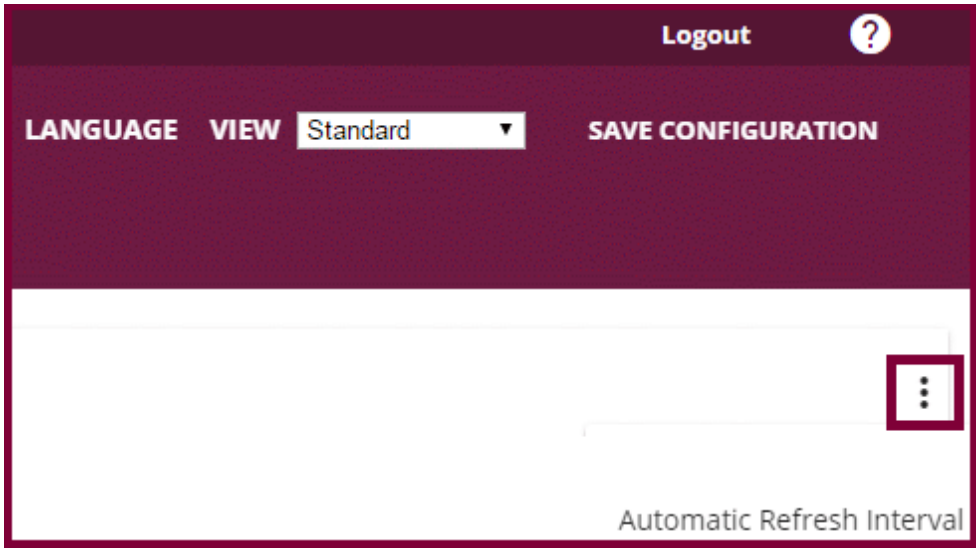
Menu	Function
Update Interval	Here you can set the interval in which the view is to be updated. To do this, enter a period in seconds in the input field and confirm it with APPLY.
Filter	You can have the list entries filtered and displayed according to certain criteria. You can determine the number of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

Configuration of the update interval



Filter list

On the **status page** you can open the option **Automatic Refresh Interval** using the button ⋮.



Click **Automatic Refresh Interval**.

Enter the time and click APPLY .

Structure of the configuration menu

The menus contain the following basic structures:

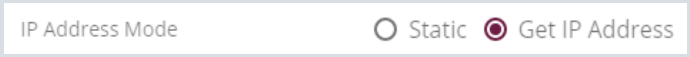
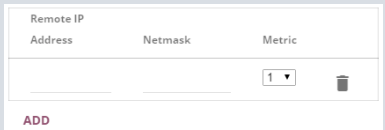
Menu structure

Menu	Function
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.

Menu	Function
Sub-menu 	The **New** button is available in each menu in which a list of all the configured entries is displayed. Click the button to display the configuration menu for creating a new list entry.
Sub-menu 	Click this button to process the existing list entry. You go to the configuration menu.
Menu 	Click this tab to display extended configuration options.

The following options are available for the configuration:

Configuration elements

Menu	Function
Eingabefelder	e.g. empty text field  Text field with hidden input  Enter the data.
Radiobuttons	e.g.  Select the corresponding option.
Checkbox	e.g. activation by selecting checkbox 
Dropdown-Menüs	e.g.  Click the arrow to open the list. Select the required option using the mouse.
Interne Listen	e.g.  Click ADD. A new list entry is created. Enter the corresponding data. If list input fields remain empty, these are not saved when you confirm with **OK**. Delete the entries by clicking the icon.

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.

4.3.1.3 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*.

4.3.2 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 5 Assistants

The **Assistants** menu offers step-by-step instructions for basic configuration tasks.

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

Chapter 6 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 licenses are managed and the access and authentication methods are configured.

6.1 Status

If you log into the **GUI**, your device displays the status page in the **Users** view.

Here you can find links to the configuration assistants that will support you with an easy configuration of the most important settings.

In addition, you can carry out a **Firmware Update**. Click **Update** to start the process.

Note

Do not interrupt the Internet connection or the power supply.

After installation of the new system software, the system must be restarted.

In the **Full Access** and **Expert** views of your device, the status page displays 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!

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

Fields in the System Information menu

Field	Value
Uptime	Displays the time past since the device was rebooted.
System Date	Displays the current system date and system time.
Serial Number	Displays the device serial number.
BOSS Version	Displays the currently loaded version of the system software.
Back-up of configuration on SD card	Only with inserted SD cart visible (if supported by you device). Indicates whether a backup configuration is available on the SD card or not.
Last configuration stored	Displays day, date and time of the last saved configuration (boot configuration in flash).
Night Mode Status	Displays whether your device is in normal operation (*Off*) or in night operation (*On*).

Fields in the Resource Information menu

Field	Value
CPU Usage	Displays the CPU usage as a percentage.
Memory Usage	Displays the usage of the working memory in MByte in relation to the available total working memory in MByte. The usage is also displayed in brackets as a percentage.
Memory Card	Shows the status of any optional external memory card that has been inserted, and the size of the memory in GBytes or MBytes.
ISDN Usage Internal	Shows the number of active B channels and the maximum number of available B channels for internal connections.
ISDN Usage External	Shows the number of active B channels and the maximum number of available B channels for external connections.
Active Sessions (SIF, RTP, etc...)	Displays the total number of sessions which are counted by the stateful inspection function of the device. A value is displayed if one or more of the following functions is enabled: • SIF • TDCR • IP load balancing .

Field	Value
Active IPSec Tunnels	Displays the number of currently active IPSec tunnels in relation to the number of configured IPSec tunnels.
DSP Channels	Shows the currently used DSP channels.

Fields in the Modules menu

Field	Value
DSP Module	Shows the type of plugged DSP module if any. An acquired fax licence, if any, can be displayed.

Fields in the VoIP Trunk Lines menu

Field	Value
No.	Displays the consecutive number of the SIP provider (your IP telephony provider).
Description	Displays the description of the SIP provider that has been entered upon creation of the provider.
Registrar	Displays the server your system connects to in order to enable IP phone calls.
Access Type	Displays if your connection is a point to multipoint or point to point (DDI) connection.
Status	Displays the current status of the connection to this SIP provider.

Fields in the Physical Interfaces menu

Field	Value
Interface - **Connection Information** - **Link**	The physical interfaces are listed here and their most important settings are shown (ISDN: only the first 4 ports are listed). The system also displays whether the interface is connected or active. Interface specifics for Ethernet interfaces: • IP address • Netmask • Not configured Interface specifics for ISDN interfaces: • Configured • Not configured

Field	Value
	Interface specifics for xDSL interfaces: • Last Change • DSL operation mode • DSL Speed • DSL Volume Interface specifics for LTE connection: • Current quality of the UMTS/LTE connection

Fields in the WAN Interfaces menu

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

6.2 Global Settings

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

6.2.1 System

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

The menu consists of the following fields:

Fields in the menu Basic Settings

Field	Value
System Name	Enter the system name of your device. This is also used as the PPP host name. A character string with a maximum of 255 characters is possible. The device type is entered as the default value.
Location	Enter the location of your device.

Field	Value
Contact	Enter the relevant contact person. Here you can enter the e-mail address of the system administrator, for example. A character string with a maximum of 255 characters is possible.
Maximum Number of Syslog Entries	Enter the maximum number of syslog messages that are stored internally in the device. Possible values are *0* to *1000*. The default value is *50*. You can display the stored messages in **Monitoring**->**Internal Log**.
Maximum Message Level of Syslog Entries	Select the priority of system messages above which a log should be created. 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 *Debug*. Possible values: • *Emergency*: Only messages with emergency priority are recorded. • *Alert*: Messages with emergency and alert priority are recorded. • *Critical*: Messages with emergency, alert and critical priority are recorded. • *Error*: Messages with emergency, alert, critical and error priority are recorded. • *Warning*: Messages with emergency, alert, critical, error and warning priority are recorded. • *Notice*: Messages with emergency, alert, critical, error, warning and notice priority are recorded. • *Information* (default value): Messages with emergency, alert, critical, error, warning, notice and information priority are recorded. • *Debug*: All messages are recorded.

Field	Value
Maximum Number of Accounting Log Entries	Enter the maximum number of login process entries that are stored internally in the device. Possible values are `0` to `1000`. The default value is `20`.
Cloud NetManager communication	Only for devices with support for being managed by the Cloud NetManager. Enable or disable the option **Cloud NetManager communication.** The function is enabled by default.
Cloud NetManager address	Only for devices with support for being managed by the Cloud NetManager. 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.
Manual WLAN Controller IP Address	This function is only available on devices with a wireless LAN controller. Enter the IP address of the WLAN controller. The value can only be modified it the WLAN controller function is enabled.
LED mode	Only for WLAN devices Select the LEDs' lighting behaviour. Possible values: • `Status` (default value): The LEDS display their default behaviour. • `Flashing`: Only the status LED flashes once per second. • `Off`: All LEDs are disabled.
Show Manufacturer Names	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., `00:a0:f9:37:12:c9`, `BintecCo_37:12:c9` is displayed if this option is enabled.

Field	Value
Autosave Configuration	Here you can choose whether configuration changes are automatically saved. The option is enabled per default. You can find a detailed description of this function below.

Autosave Configuration

Whenever you make a change to the current configuration using the GUI, this change becomes immediately active once you confirm the change (e.g. with the **OK** button). Additionally, the status of the configuration is stored, the syslog (syslogl evel = *debug*) shows *new config state: modified*. As soon as this state has been reached, and the next bit of HTTP(S) traffic between the browser and the GUI is registered, the change is confirmed and cleared for saving. The syslog shows *new config state: confirmed*.

As soon as this state has been reached and the configuration session via the browser is terminated without the user actively saving the new configuration, your device automatically saves the new configuration once the HTTP(S) session has timed out. The syslog first informs about the termination of the active session (e.g. *delete httpSessionStat entry admin at Fri Apr 21 11:04:34 2017 (keep alive timeout)*), and then confirms the configuration *auto save on session termination*.

In case a configuration error has locked you out of the GUI, the implicit confirmation of the change (*new config state: confirmed*) does not take place, and it is not saved after session termination. A reboot of your device then resets the change.

6.2.2 Passwords

Setting the passwords is another basic system setting.

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 unauthorized use.

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

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

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

Fields in the System Password menu.

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

Fields in the SNMP Communities menu.

Field	Value
SNMP Read Community	Enter the password for the user name `read` .
SNMP Write Community	Enter the password for the user name `write` .

Fields in the Global Password Options menu

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

6.2.3 Date and Time

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

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

Fields in the menu Manual Time Settings

Field	Description
Set Date	Clicking into the field for adding a date brings up a standard calender. Clicking the desired date will enter it into the configuration interface.
Set Time	Enter a new time. Format: • **Hour**: hh • **Minute**: mm

Fields in the menu Automatic Time Settings (Time Protocol)

Field	Description
ISDN Timeserver	Only for devices with an ISDN interface. Determine whether the system time is to be updated via ISDN. 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. The function is activated by selecting *Enabled*. The function is disabled by default.
First Timeserver	Enter the primary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.

Field	Description
Second Timeserver	Enter the secondary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Third Timeserver	Enter the third time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol via UDP port 123. • *Time Service / UDP*: This server uses the Time service with UDP port 37. • *Time Service / TCP*: This server uses the Time service with TCP port 37. • *None*: This time server is not currently used for the time request.
Time Update Interval	Enter the time interval in minutes at which the time is automatically updated. The default value is *1440*.
Time Update Policy	Enter the time period after which the system attempts to contact the time server again following a failed time update. Possible values: • *Normal* (default value): The system attempts to contact the

Field	Description
	time server after 1, 2, 4, 8, and 16 minutes. • *Aggressive*: For ten minutes, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. • *Endless*: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds and then every 10 seconds. If certificates are used to encrypt data traffic in a VPN, it is extremely important that the correct time is set on the device. To ensure this is the case, for **Time Update Policy**, select the value *Endless*.
Internal Time Server	Select whether the internal timeserver is to be used. The function is activated by selecting *Enabled*. Time requests from a client will be answered with the current system time. This is given as GMT, without offset. The function is disabled by default. Time requests from a client are not answered.

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

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

6.2.4 System licenses

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

The following licence types exist:

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

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

Entering licence data

You can obtain the licence data for extra licenses via the online licensing pages in the support section at *www.bintec-elmeg.com* . Please follow the online licensing instructions. (Please also note the information on the licence card for licenses 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 licenses**->**New** menu.

In the **System Management**->**Global Settings**->**System licenses**->**New** menu, a list of all registered licenses 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 licenses for a device, click the **Default licenses** button (standard licenses).

6.2.4.1 Edit or New

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

Activating extra licenses

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

The menu consists of the following fields:

Fields in the Basic Settings menu.

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

Note

If *Not OK* is displayed as the status:

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

If *Not Supported* is displayed as the status, you have entered a license for a subsystem 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 licenses**->**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.

6.3 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)

6.3.1 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.

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

Fields in the Interfaces menu.

Field	Description
Interface Description	Displays the name of the interface.
Mode / Bridge Group	Select whether you want to run the interface in *Routing Mode* or whether you want to assign the interface to an existing (*br0*, *br1* etc.) or new bridge group (*New Bridge Group*). When selecting *New Bridge Group*, a new bridge group is automatically created after you click the **OK** button.
Configuration Interface	Select the interface via which the configuration is to be carried out. Possible values: • *Select one* (default value): Ex works setting The right configuration interface must be selected from the other options. • *Ignore*: No interface is defined as configuration interface. • *<Interface name>*: 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.

6.3.1.1 Add

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

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 WIxxxxn and RS series

For WLAN clients in bridge mode (so-called MAC Bridge) you can also edit additional set-

tings via the icon.

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

(1) Select **GUI** menu **Wireless LAN**->**WLAN**->**Radio Settings** and click the icon to modify an entry.

(2) Select **Operation Mode** = *Access Client* and save the settings with **OK**.

(3) Select the **System Management**->**Interface Mode / Bridge Groups**->**Interfaces** menu. The additional interface **sta1-0** is displayed.

(4) For interface **sta1-0** select Mode / Bridge Group = *br0 (<IPAddress>)* and **Configuration Interface**= *en1-0* and save the settings with **OK**.

(5) Click the **Save configuration** button to save all of the configuration settings. You can use the MAC Bridge.

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

Fields in the Layer-2.5 Options menu.

Field	Value
Interface	Shows the interface that is being edited.
Wildcard Mode	Select the Wildcard mode you want to use on the interface. Possible values: • *none* (default value): Wildcard mode is not used. • *static*: With this setting, you must enter the MAC address of a device that is connected over IP under **Wildcard MAC Address**. Each packet without IP and without ARP is forwarded to this device. This occurs even when the device is no longer connected. • *first*: 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. • *last*: 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 ap-

Field	Value
	pears, it is forwarded to the MAC address from which the last non-IP unicast frame or non-ARP unicast frame was received on the Ethernet interface of the device. This wildcard MAC address is renewed with each non-IP unicast frame or non-ARP unicast frame.
Wildcard MAC Address	Only for **Wildcard Mode** = *static* Enter the MAC address of a device that is connected over IP.
Transparent MAC Address	Only for **Wildcard Mode** = *static*, *first* Choose whether or not the **Wildcard MAC Address** are used in addition as WLAN MAC address to establish the connection to the access point. The function is enabled with *Enabled*. The function is disabled by default.

6.4 Administrative Access

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

6.4.1 Access

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

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

Note

Not all of the options above will be available in every bintec elmeg device. Consult the data sheet of your device which connection types are supported!

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. If the option is activated, it is deactived again after ca. 30 minutes.

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

Fields in the menu Advanced Settings

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

6.4.1.1 Add

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

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

Fields in the menu Access

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

6.4.2 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.

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

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

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

Note

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

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

Fields in the menu SSH (Secure Shell) Parameters

Field	Value
SSH service active	Select whether the SSH Daemon is to be enabled for the interface. The function is activated by selecting *Enabled*. The function is enabled by default.
SSH Port	Here you can enter the port via which the SSH connection is to be established. The default value is *22*.
Maximum number of concurrent connections	Enter the maximum number of simultaneously active SSH connections. The default value is *1*.

Fields in the menu Authentication and Encryption Parameters

Field	Value
Encryption Algorithms	Select the algorithms that are to be used to encrypt the SSH connection. Possible options: • *3DES* • *Blowfish* • *AES-128* • *AES-256* By default *3DES*, *Blowfish* and *AES-128* are enabled.
Hashing Algorithms	Select the algorithms that are to be available for message au-

Field	Value
	thentication of the SSH connection. Possible options: • *MD5* • *SHA-1* • *RipeMD 160* By default *MD5*, *SHA-1* and *RipeMD 160* are enabled.

Fields in the menu Key Status

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

Field	Value
ED25519 Key Status	Shows the status of the ED25519 key. If an ED25519 key has not been generated yet, *Not generated* is displayed and a link, *Generate*, is provided. If you select the link, the generation process is triggered and the view is updated. The *Generating* status is displayed. When generation has been completed successfully, the status changes from *Generating* to *Generated*. If an error occurs during the generation, *Not generated* and the *Generate* link are displayed again. You can then repeat generation. If the *Unknown* status is displayed, generation of a key is not possible, for example because there is not enough space in the FlashROM.

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

Fields in the menu Advanced Settings

Field	Value
Login Grace Time	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. The default value is *600* seconds.
Compression	Select whether data compression should be used. The function is activated by selecting *Enabled*. The function is disabled by default.
TCP Keepalives	Select whether the device is to send keepalive packets. The function is activated by selecting *Enabled*. The function is enabled by default.
Logging Level	Select the syslog level for the syslog messages generated by the SSH Daemon. Possible settings: • *Information* (default value): Fatal and simple errors of the SSH Daemon and information messages are recorded.

Field	Value
	• *Fatal*: Only fatal errors of the SSH Daemon are recorded. • *Error*: Fatal and simple errors of the SSH Daemon are recorded. • *Debug*: All messages are recorded.

6.4.3 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.

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

Fields in the Basic Settings menu.

Field	Value
SNMP Version	Select the SNMP version your device is to use to listen for external SNMP access. Possible values: • *v1*: SNMP Version 1 • *v2c*: Community-Based SNMP Version 2 • *v3*: SNMP Version 3 By default, *v1*, *v2c* and *v3* are enabled. If no option is selected, the function is deactivated.

Field	Value
SNMP Listen UDP Port	Shows the UDP port (*161*) at which the device receives SNMP requests. The value cannot be changed.
SNMP multicast discovery	Enable or disable the function **SNMP multicast discovery**. The function is enabled with *Enabled*. The function is enabled by default.

Tip

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

6.5 Remote Authentication

This menu contains the settings for user authentication.

6.5.1 RADIUS

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

RADIUS can be used for:

- Authentication
- Accounting
- Exchange of configuration data

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

If the RADIUS server is used for accounting, your device sends an accounting message at the start of the connection and a message at the end of the connection. These start and

end messages also contain statistical information about the connection (IP address, user name, throughput, costs).

RADIUS packets

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

Packet types

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

6.5.1.1 Edit or New

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

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

Fields in the Basic Parameters menu.

Field	Value
Authentication Type	Select what the RADIUS server is to be used for. Possible values: • *PPP Authentication* (default value only for PPP connections): The RADIUS server is used for controlling access to a network. • *Accounting* (for PPP connections only): The RADIUS server is used for recording statistical call data. • *Login Authentication*: The RADIUS server is used for controlling access to the SNMP shell of your device. • *IPSec Authentication*: The RADIUS server is used for sending configuration data for IPSec peers to your device. • *WLAN (802.1x)*: The RADIUS server is used for controlling access to a wireless network. • *XAUTH*: The RADIUS server is used for authenticating IPSec peers via XAuth.
Vendor Mode	Only for **Authentication Type** = *Accounting* In hotspot applications, select the mode define by the provider. In standard applications, leave the value set to *Default*. Possible values for hotspot applications: • *France Telecom*: For France Telecom hotspot applications. • *bintec HotSpot Server*: For hotspot applications.
Server IP Address	Enter the IP address of the RADIUS server.
RADIUS Secret	Enter the shared password used for communication between

Field	Value
	the RADIUS server and your device.
Default User Password	Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server.
Priority	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. Possible values from `0` (highest priority) to `7` (lowest priority). The default value is `0`. See also **Policy** in the Advanced Settings.
Entry active	Select whether the RADIUS server configured in this entry is to be used. The function is activated by selecting `Enabled`. The function is enabled by default.
Group Description	Define a new RADIUS group description or assign the new RADIUS entry to a predefined group. The configured RADIUS servers for a group are queried according to **Priority** and the **Policy** . Possible values: • `New` (default value): Enter a new group description in the text field. • `Default Group 0`: Select this entry for special applications, such as Hotspot Server configuration. • `<Group Name>`: Select a predefined group from the list.

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

Fields in the Advanced Settings menu.

Field	Value
Policy	Select how your device is to react if a negative response to a request is received.

Field	Value
	Possible values: • *Authoritative* (default value): A negative response to a request is accepted. • *Non-authoritative* : A negative response to a request is not accepted. A request is sent to the next RADIUS server until your device receives a response from a server configured as authoritative.
UDP Port	Enter the UDP port to be used for RADIUS data. 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. The default value is *1812*.
Server Timeout	Enter the maximum wait time between ACCESS_REQUEST and response in milliseconds. After timeout, the request is repeated according to **Retries** or the next configured RADIUS server is requested. Possible values are whole numbers between *50* and *50000*. The default value is *1000* (1 second).
Alive Check	Here you can activate a check of the accessibility of a RADIUS server in **Status** *Down* . An Alive Check is carried out regularly (every 20 seconds) by sending an ACCESS_REQUEST to the IP address of the RADIUS server. If the server is reachable, **Status** is set to *alive* again. If the RADIUS server is only reachable over a switched line (dialup connection), this can cause additional costs if the server is *down* for a long time. The function is activated by selecting *Enabled*. The function is enabled by default.
Retries	Enter the number of retries for cases when there is no response to a request. If an response has still not been received after

Field	Value
	these attempts, the **Status** is set to *down*. In **Alive Check** = *Enabled* your device attempts to reach the server every 20 seconds. If the server responds, **Status** is set back to *alive* . Possible values are whole numbers between *0* and *10*. The default value is *1*. To prevent **Status** being set to *down*, set this value to *0*.
RADIUS Dialout	Only for **Authentication Type** = *PPP Authentication* and *IPSec Authentication*. 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. The function is activated by selecting *Enabled*. The function is disabled by default. If the function is active, you can enter the following options: • *Reload Interval*: Enter the time period in seconds between update intervals. The default entry here is *0* i.e. an automatic reload is not carried out.

6.5.2 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.

6.5.2.1 Edit or New

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

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

Fields in the Basic Parameters menu.

Field	Description
Authentication Type	Displays which TACACS+ function is to be used. The value cannot be changed. Possible values: • *Login Authentication*: Here, you can define whether the current TACACS+ server is to be used for login authentication to your device.
Server IP Address	Enter the IP address of the TACACS+ server that is to be requested for login authentication.
TACACS+ Secret	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.
Priority	Assign a priority to the current TACACS+ server. The server with the lowest value is the one used first for TACACS+ login authentication. If no response is given or access is denied (only if **Policy** = *Non-authoritative*), the entry with the next-highest priority is used. The available values are *0* to *9*, the default value is *0*.
Entry active	Select whether this server is to be used for login authentication. The function is activated by selecting *Enabled*. The function is enabled by default.

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

Fields in the Advanced Settings menu.

Field	Description
Policy	Select the interpretation of the TACACS+ response. Possible values: • *Non-authoritative* (default value): The TACACS+ servers are queried in order of their priority (see **Priority**) until a positive response is received or a negative response has been received from an authoritative server. • *Authoritative*: A negative response to a request is accepted, i.e. a request is not sent to another TACACS+ server. The device's internal user administration is not turned off by TACACS+. It is checked after all TACACS+ servers have been queried.
TCP Port	Shows the default TCP port (*49*) used for the TACACS+ protocol. The value cannot be changed.
Timeout	Enter time in seconds for which the NAS is to wait for a response from TACACS+. If a response is not received during the wait time, the next configured TACACS+ server is queried (only if **Policy** = *Non-authoritative*) and the status of the current server is set to *Blocked*. The possible values are *1* to *60*, the default value is *3*.
Block Time	Enter the time in seconds for which the status of the current server shall remain blocked. When the block has ended, the server is set to the status specified in the **Entry active** field. The possible values are *0* to *3600*, the default value is *60*. The value *0* means that the server is never set to *Blocked* status and thus no other servers are queried.
Encryption	Select whether data exchange between the TACACS+ server and the NAS is to be encrypted with MD5. The function is activated by selecting *Enabled*.

Field	Description
	The function is enabled by default. 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.

6.5.3 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.

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

Fields in the Global RADIUS Options menu.

Field	Description
Authentication for PPP Dialin	By default, the following authentication sequence is used for incoming calls with RADIUS: First CLID, then PPP and then PPP with RADIUS. Options: • *Inband*: Only inband RADIUS requests (PAP,CHAP, MS-CHAP V1 & V2) (i.e. PPP requests without CLID) are sent to the RADIUS server defined in **Server IP Address**. • *Outband (CLID)* : Only outband RADIUS requests (i.e. requests for calling line identification = CLID) are sent to the RADIUS server. *Inband* is enabled by default, *Outband (CLID)* is diabled by default.

6.6 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.

6.6.1 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 *Mini Call Center*, *Charges*, *Phonebook*, *PBX User Access* , *Initial operation*, *Export*, *User* are preconfigured for PABX systems. You can change these using the icon or reset them to the default settings using the icon .

6.6.1.1 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.

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

Fields in the menu Basic Settings

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

Fields in the menu Buttons

Field	Description
Save configuration	If you activate the button **Save configuration** the user is permitted to save configurations.

Note

Note that the passwords in the saved file can be viewed in clear text.

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

Fields in the menu Navigation Entries

Field	Description
Menus	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. 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  . Each element in the navigation bar can have three values. Click the icon  in the row you want to display these three values.

Field	Description
	Possible values: • *Deny*: The menu and all its lower-level menus are blocked. • *Allow*: The menu is released. Lower-level menus may need to be specifically released. • *Allow all*: The menu and all its lower-level menus are released. You can select *Allow* and *Allow all* in the corresponding row to assign elements to the current access profile. Elements that are assigned to the current access profile are flagged with the icon . indicates a menu that is blocked, but which has at least one released sub-menu.

6.6.2 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.

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.

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.

6.6.2.1 Edit or New

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

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

Fields in the menu Basic Settings

Field	Description
User	Enter a unique name for the user.

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

6.7 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.

6.7.1 Certificate List

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

6.7.1.1 Edit

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

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

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

Fields in the Edit parameters menu.

Field	Description
Description	Shows the name of the certificate, key, or request.
Certificate is CA Certificate	Mark the certificate as a certificate from a trustworthy certification authority (CA). Certificates issued by this CA are accepted during authentication.

Field	Description
	The function is enabled with *True*. The function is disabled by default.
Certificate Revocation List (CRL) Checking	Only for **Certificate is CA Certificate** = *True* 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. Possible settings: • *Disabled*: No CRLs check. • *Always*: CRLs are always checked. • *Only if a CRL Distribution Point is present* (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. • *Use settings from superior certificate*: The settings of the higher level certificate are used, if one exists. It is does not, the same procedure is used as that described under "Only if a CRL Distribution Point is present".
Force certificate to be trusted	Define that this certificate is to be accepted as the user certificate without further checks during authentication. The function is enabled with *True*. The function is disabled by default.

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.

6.7.1.2 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.

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

Fields in the Certificate Request menu.

Field	Description
Certificate Request Description	Enter a unique description for the certificate.
Mode	Select the way in which you want to request the certificate. Possible settings: • `Manual` (default value): Your device generates a PKCS#10 for the key. This file can then be uploaded directly in the browser or copied in the menu using the **View details** field. This file must be provided to the CA and the received certificate must then be imported manually to your device. • `SCEP` : The key is requested from a CA using the Simple Certificate Enrolment Protocol.
Generate Private Key	Only for **Mode** = `Manual` Select an algorithm for key creation. `RSA` (default value) and `DSA` are available. Also select the length of the key to be created. Possible values: `512`, `768`, `1024`, `1536`, `2048`, `4096`. Please note that a key with a length of 512 bits could be rated

Field	Description
	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.
SCEP URL	Only for **Mode** = *SCEP* Enter the URL of the SCEP server, e.g. http://scep.bintec-elmeg.com:8080/scep/scep.dll Your CA administrator can provide you with the necessary data.
CA Certificate	Only for **Mode** = *SCEP* Select the CA certificate. • In *-- Download --*: In **CA Name**, enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. *cawindows*. Your CA administrator can provide you with the necessary data. If no CA certificates are available, the device will first download the CA certificate of the relevant CA. It then continues with the enrolment process, provided no more important parameters are missing. In this case, it returns to the **Generate Certificate Request** menu. If the CA certificate does not contain a CRL distribution point (Certificate Revocation List, CRL), and a certificate server is not configured on the device, the validity of certificates from this CA is not checked. • <name of an existing certificate>: If all the necessary certificates are already available in the system, you select these manually.
RA Sign Certificate	Only for **Mode** = *SCEP* Only for **CA Certificate** not = *-- Download --* Select a certificate for signing SCEP communication. The default value is *-- Use CA Certificate --*, i.e. the CA certificate is used.

Field	Description
RA Encrypt Certificate	Only for **Mode** = *SCEP* Only if **RA Sign Certificate** not = *-- Use CA Certificate --* If you use one of your own certificates to sign communication with the RA, you can select another one here to encrypt communication. The default value is *-- Use RA Sign Certificate --*, i.e. the same certificate is used as for signing.
Password	Only for **Mode** = *SCEP* 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.

Fields in the Subject Name menu.

Field	Description
Custom	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. If *Enabled* is selected, a subject name can be given in **Summary** with attributes not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE". If the field is not selected, enter the name components in **Common Name**, **E-mail**, **Organizational Unit**, **Organization**, **Locality**, **State/Province** and **Country**. The function is disabled by default.
Summary	Only for **Custom** = enabled. Enter a subject name with attributes not offered in the list. Example: "CN=VPNServer, DC=mydomain, DC=com, c=DE".
Common Name	Only for **Custom** = disabled. Enter the name according to CA.

Field	Description
E-mail	Only for **Custom** = disabled. Enter the e-mail address according to CA.
Organizational Unit	Only for **Custom** = disabled. Enter the organisational unit according to CA.
Organization	Only for **Custom** = disabled. Enter the organisation according to CA.
Locality	Only for **Custom** = disabled. Enter the location according to CA.
State/Province	Only for **Custom** = disabled. Enter the state/province according to CA.
Country	Only for **Custom** = disabled. Enter the country according to CA.

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

Fields in the Subject Alternative Names menu.

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

Fields in the Options menu

Field	Description
Autosave Mode	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. The function is enabled with *Enabled*. The function is enabled by default.

6.7.1.3 Import

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

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

Fields in the Import menu.

Field	Description
External Filename	Enter the file path and name of the certificate to be imported, or use **Browse...** to select it from the file browser.
Local Certificate Description	Enter a unique description for the certificate.
File Encoding	Select the type of coding so that your device can decode the certificate. Possible values: • *Auto* (default value): Activates automatic code recognition. If downloading the certificate in auto mode fails, try with a certain type of encoding. • *Base64* • *Binary*
Password	You may need a password to obtain certificates for your keys.

Field	Description
	Enter the password here.

6.7.2 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.

6.7.2.1 Import

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

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

Fields in the CRL Import menu.

Field	Description
External Filename	Enter the file path and name of the CRL to be imported, or use **Browse...** to select it from the file browser.
Local Certificate Description	Enter a unique description for the CRL.
File Encoding	Select the type of encoding, so that your device can decode the CRL. Possible values: • *Auto* (default value): Activates automatic code recognition. If downloading the CRL in auto mode fails, try with a certain type of encoding. • *Base64* • *Binary*

Field	Description
Password	Enter the password required for the import.

6.7.3 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.

6.7.3.1 New

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

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

Fields in the Basic Parameters menu.

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

Chapter 7 Physical Interfaces

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

7.1 AUX

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

7.1.1 AUX

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

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

PIN assignment modem cable

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

Fields in the Basic Settings menu.

Field	Description
AUX Port Status	Select whether the AUX port should be enabled or disabled. The port is enabled by choosing *Enabled*. The port is disabled by default.

Field	Description
Line Speed	Only for **AUX Port Status** = enabled Here you select the speed at which the gateway addresses the modem (in bps). Possible values: • *Default*: The Baud rate of the serial terminal connection is retained. (9600 in ex works state) All other values mean that the modem is addressed at the corresponding speed in bps. • *9600 bps* • *19200 bps* • *38400 bps* • *57600 bps* (default value): Recommended for communication with a GSM modem. • *115200 bps*: Recommended for communication with an analogue modem.
Incoming Service Type	Only for **AUX Port Status** = enabled Here you select the gateway subsystem to which an incoming call over the modem is to be assigned. Possible values: • *Disabled*: No call is accepted. • *ISDN Login* : The call is assigned to the ISDN Login subsystem. • *PPP Dialin* (default value): The call is assigned to the PPP subsystem.
SIM Card Uses PIN	Only for **AUX Port Status** = enabled Here you enter the PIN of your GSM modem, if your modem asks for it. Entering a wrong PIN blocks communication with the modem until the entry in the profile is corrected.
Modem Escape Char-	Only for **AUX Port Status** = enabled

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

7.2 Ethernet Ports

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

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

The logical Ethernet interface *en1-4* is assigned to the **ETH5** port 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 serial connection via the **Console** interface.

ETH1 - ETH4

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

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.

7.2.1 Port Configuration

Port Separation

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

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

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

Fields in the Switch Configuration menu.

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

Field	Description
	• *100 mbps / Half Duplex* • *10 mbps / Full Duplex* • *10 mbps / Half Duplex* • *Down*
Flow Control	Select whether a flow control should be conducted on the corresponding interface. Possible values: • *Disabled* (default value): No flow control is performed. • *Enabled*: Flow control is performed. • *Auto*: Automatic flow control is performed.

7.3 ISDN Ports

In this menu, you configure the ISDN interfaces of your device. Here you enter data such as the type of ISDN connection to which your gateway is connected. You can use the ISDN interfaces of your gateway for various types of use.

You must carry out two steps to configure the ISDN interfaces:

- 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.

7.3.1 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.

7.3.1.1 Edit

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

ISDN BRI interface

You can use the ISDN BRI interface of your gateway for both dialup connections and leased lines over ISDN.

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.
Autoconfiguration on Bootup	Select whether the ISDN switch type (D channel detection for switched line) is to be automatically identified. The function is enabled with *Enabled*. The function is enabled by default.
Result of Autoconfiguration	Shows the status of the ISDN Auto Config. Automatic D-channel detection runs until a setting is found, or until the ISDN protocol is selected manually under **Port Usage**. This field cannot be edited. The result of automatic configuration for the **Port Usage** and the **ISDN Configuration Type** is displayed. Possible values: • All possible values for the **Port Usage** and the **ISDN Configuration Type**. • *Running*: Detection is still running.
Port Usage	Only if **Autoconfiguration on Bootup** is disabled. Select the protocol that you want to use for the ISDN port. Possible values: • *Not used*: The ISDN connection is not used.

Field	Description
	• *Dialup (Euro ISDN)* • *Leased Line* • *Q-SIG*
ISDN Configuration Type	Only if **Autoconfiguration on Bootup** is disabled and for **Port Usage** = *Dialup (Euro ISDN)* or *Q-SIG* Select the ISDN connection type. Possible values: • *Point-to-Multipoint* (default value): Point-to-multipoint connection • *Point-to-Point*: Point-to-point ISDN access.
ISDN Switch Type	Only for **Port Usage** = *Leased Line* Select the ISDN protocol supplied by your provider. Possible values: • *Leased Line B1 64S*: Leased line over B channel 1 (64 kbps) • *Leased Line B1+B2 64S2*: Leased line over both B channels (128 kbps) • *Leased Line D+B1+B2 TS02*: Leased line over D-channel and both B channels (144 kbps) • *Leased Line B1+B2 Different Endpoints*: Leased line to two different endpoints. • *Leased Line B1+D TS01*: Leased line over B channel 1 and D-channel (80 kbps) • *Leased Line B2+D TS01*: Leased line over B channel 2 and D-channel (80 kbps) • *Leased Line B2 64S*: Leased line over B channel 2 (64 kbps)
Call Number	This parameter is exclusively used by Media Gateway. Only for **Port Usage** *Dialup (Euro ISDN)* and **ISDN Configuration Type** *Point-to-Point* Only for the devices **RTxxx2**

Field	Description
	Enter the basic number of the Point-to-Point. With incoming calls, this basis call number is cut off by the called party number With outgoing calls, this main number is attached to the number to be called (calling party number).

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

Fields in the Advanced Settings menu.

Field	Description
X.31 (X.25 in D Channel)	Select whether you want to use X.31 (X.25 in the D channel) e.g. for CAPI applications. The function is enabled with *Enabled*. The function is disabled by default.
X.31 TEI Value	Only if **X.31 (X.25 in D Channel)** is enabled 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. Possible values are *0* to *63*. The default value is *-1* (for automatic detection).
X.31 TEI Service	Only for **X.31 (X.25 in D Channel)** enabled Select the service for which you want to use X.31 TEI. Possible values: • *CAPI* • *CAPI Default* • *Packet Switch* (default value) *CAPI* and *CAPI Default* are only for the use of X.31 TEI for CAPI applications. For *CAPI*, the TEI value set in the CAPI application is used. For *CAPI Default*, the value of the CAPI application is ignored and the default value set here is always used.

Field	Description
	Packet Switch is set if you want to use X.31 TEI for the X.25 device.

ISDN-PRI interface

For a Primary Rate Interface (PRI, or S2M), the channels are transmitted in series in so-called time slots.

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

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.
Port Usage	Select whether the ISDN switch type (D channel detection for switched line) is to be automatically identified. Possible values: • *None* (default value): ISDN connection is not used. • *EURO ISDN S2M (TE)*: EURO ISDN S2M User Profile • *EURO ISDN S2M (NT)*: EURO ISDN S2M Network Profile • *Back to Back (dialup)*: Two S2M connections are directly coupled. • *Leased Line*: You can select a leased line. • *Q-SIG S2M (TE)*: Q-SIG S2M User Profile • *Q-SIG S2M (NT)*: Q-SIG S2M Network Profile
ISDN Line Framing	Only if **Port Usage** is selected. Select the framing type for layer 1. Possible values: • *CRC4 (Standard)* (default value) • *No CRC* The default value can be left in the majority of scenarios. You

Field	Description
	can use the *No CRC* option if required (e.g. in Sweden and France), if the device is to be connected to a PABX.
P-P Base Number	Only if **Port Usage** not *None*, *Back to Back (dialup)* or *Leased Line* Only for the devices **RTxxx2** Enter the main number of the connection. With incoming calls, this basis call number is cut off by the called party number With outgoing calls, this main number is attached to the number to be called (calling party number).
Channel Selection	Only if **Port Usage** = *EURO ISDN S2M (TE)*, *EURO ISDN S2M (NT)*, *Q-SIG S2M (TE)* or *Q-SIG S2M (NT)*. An additional option is provided in order to guarantee the compatibility with special providers: If you set the switch type appropriately, you can select a value for the variable **Channel Selection**. This defines how the B channel is selected for an outgoing call. Possible values: • *Any Channel* (default value): The device tells the PABX that all channels are available. The exchange of the PABX selects the channel to be used. • *No channel identification* : The device sends no IE (Information Element) for channel identification. The exchange selects the channel to be used. • *Submit preferred channel* : The device selects the channel to be used and signals this to the exchange. You can normally use the default value. It is only necessary to change the setting in a few special cases. If you encounter problems with outgoing calls, ask your provider whether a special value has to be set.

Field	Description
Clock Mode	Only if **Port Usage** = *Back to Back (dialup)* Defines which connection partner sends the clock signal for synchronization between the sender and the recipient. If the clock signal is not sent by the exchange itself, one of the connection partners must sent the signal. Possible values: • *Extern*: The device receives the clock signal. • *Internal*: The device sends the clock signal.
ISDN Switch Type	Only if **Port Usage** = *Leased Line*Select the ISDN connection type. Possible values: • *Leased Line (Custom Time Slots)*: Up to 31 PPP interfaces can be configured for leased lines to different destinations. • *Leased Line, 1 Hyperchannel (G.703 + G.704)*: 1984 kbps, structured • *Leased Line Unstructured G.703*: 2048 kbps, unstructured
Custom Time Slots	Only if **Port Usage** = *Leased Line* and **ISDN Switch Type** = *Leased Line (Custom Time Slots)*. You have the option to bundle any channels on the physical layer as so-called hyper channels. You can also group together channels as PPP multilink channel bundles. Timeslots divide the available 2 Mbps bandwidth of an S2M connection into logical channels. No distinction is made below between timeslots and channels, as the difference is immaterial for configuration purposes. A list of the channel bundles already configured is shown. Click **Add** to configure new channel bundles.

You can use the **Add** at **Custom Time Slots** to configure additional bundles.

Note

This function is only available for leased lines.

Fields in the New Bundle menu.

Field	Description
Description	Enter the name of the channel bundle.
Bundle Type	Displays the type of channel bundle. Possible values: • *PPP Multilink*: The channels are bundled as PPP Multilink channels. • *Physical (Hyperchannel)*: The channels are bundled as physical hyperchannels.
Timeslot Selection	Select between *Range Selection* and *Timeslot Matrix*.
Timeslot Range	Only if **Timeslot Selection** = *Range Selection* Shows the logical channels (timeslots) combined to form this channel bundle. • *From*: Shows the first of the channels used for this channel bundle. Possible values: *1* to *31*. • *to*: Shows the last of the channels used for this channel bundle. Possible values: *1* to *31*.
Timeslot Matrix	Only if **Timeslot Selection** = *Timeslot Matrix* shows a list of all channels in detail. If you do not wish to use all the channels between a certain start and end channel for a channel bundle, you can make a selective assignment here.
X.75 Layer 2 Mode	Here you define how the interface created by this channel bundle is to behave during connection setup. You only need to configure these parameters if you used X.75 in layer 2. Possible values: • *DCE* • *DTE*

7.3.2 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.

7.3.2.1 New

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

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

Fields in the Basic Parameters menu.

Field	Description
ISDN Port	Select the ISDN port for which the MSN is to be configured.
Service	Select the service to which a call is to be assigned on the **MSN** below. Possible values: • *ISDN Login* (default value): Enables login with *ISDN Login* • *PPP (Routing)*: Default setting for PPP routing. Contains automatic detection of the PPP connections stated below except *PPP DOVB*. • *IPSec*: Enables a number to be defined for IPSec callback. • *Other (PPP)*: Other services can be selected: *PPP 64k* (Allows 64 kpbs PPP data connections), *PPP 56k* (Allows 56 kpbs PPP data connections), *PPP V.110(9600) PPP V.110(14400)*, *PPP V.110(19200)*, *PPP V.110(38400)* (Allows PPP connections with V.110 and bitrates of 9,600 bps, 14,400 bps, 19,200 bps, 38,400 bps), *PPP V.120* (Allows PPP connections with V.120).
MSN	Enter the number used to check the called party number. For the call to be accepted, it is sufficient for the individual numbers

Field	Description
	in the entry to agree, taking account of **MSN Recognition**.
MSN Recognition	Select the mode your device is to use for the number comparison for **MSN** with the called party number of the incoming call. Possible values: • *Right to Left* (default value) • *Left to Right (DDI)*: Always select if your device is connected to a point-to-point connection.
Bearer Service	Select the type of incoming call (service detection). Possible values: • *Data + Voice* (default value): Both data and voice calls. • *Data*: data call • *Voice*: Voice call (modem, voice, analog fax)

7.4 DSL Modem

The ADSL modem on the **bintec R3002** and **bintec RT3002** is compatible with ANNEX A and ANNEX B standards and so can be used universally in several countries. It is particularly suitable for high-speed Internet access and remote access use in SMEs or remote offices.

The **bintec R3502** features an integrated VDSL2 modem which supports automatic switching to ADSL2+. If required, VDSL connection is available at any time.

In addition to the VDSL2 modem, the **bintec R3502** has five gigabit Ethernet ports, which can be configured for LAN, WAN or DMZ.

7.4.1 DSL Configuration

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

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

Fields in the DSL Port Status menu.

Field	Description
DSL Chipset	Shows the key of the installed chipset.
Physical Connection	Shows the current DSL operation mode. The value cannot be changed. Possible values: • *Unknown*: The ADSL link is not active. • *ANSI T1.413*: ANSI T1.413 • *ADSL1*: ADSL classic, G.DMT, ITU G.992.1 • *G.lite G992.2*: Splitterless ADSL, ITU G.992.2 • *ADSL2*: G.DMT.Bis, ITU G.992.3 • *ADSL2 DELT*: ADSL2 Double Ended Line Test • *ADSL2 Plus*: ADSL2 Plus, ITU G.992.5 • *ADSL2 Plus DELT*: ADSL2 Plus Double Ended Line Test • *READSL2*: Reach Extended ADSL2 • *READSL2 DELT*: Reach Extended ADSL2 Double Ended Line Test. • *ADSL2 ITU-T G.992.3 Annex M* • *ADSL2+ ITU-T G.992.5 Annex M* • *VDSL1 ITU-T G.993.1* • *VDSL1 ITU-T G.9930.2*

Fields in the Current Line Speed menu

Field	Description
Downstream	Displays the data rate in the receive direction (direction from CO/DSLAM to CPE/router) in bits per second. The value cannot be changed.
Upstream	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
DSL Mode	Only for devices with an ADSL modem (**bintec R3002** / **bintec RT3002**) Define which Annex of ITU-T Recommendation G.991.2 is used for the connection. Possible values: • *Annex A*: For applications in North America (provider-dependent). • *Annex B* (default value): For applications in Europe (provider-dependent) for example. Only for devices with a VDSL modem (**bintec R3502**) Select the DSL Mode. Possible values: • *Inactive*: The VDSL interface is not active. • *ETSI T1.413*: ETSI T1.413 • *ADSL1* :ADSL1 / G.DMT is used. • *ADSL Automode*: The ADSL mode is automatically adapted for the remote terminal. • *ADSL2*: ADSL2 / G.992.3 is used. • *ADSL2 Plus*: ADSL2 Plus / G.992.5 is used. • *VDSL* (default value): VDSL is used. • *VDSL/ADSL Multimode*: VDSL/ADSL multi mode is used.
DSL SyncType	Only for devices with an ADSL modem Select the ADSL synchronization type. Possible values: • *ADSL Automode* (default value): The ADSL mode is automatically adapted for the remote terminal. • *ADSL1* :ADSL1 / G.DMT is used. • *ADSL2*: ADSL2 / G.992.3 is used. • *ADSL2 Plus*: ADSL2 Plus / G.992.5 is used. • *Inactive*: The ADSL interface is not active.

Field	Description
	Only for **ADSL Mode** = *Annex A* • *Automode (Annex-M)*: The ADSL mode is automatically adapted to the other end with reference to G.992.3 Annex M. • *ADSL2 Plus (Annex-M)*: ADSL2 Plus / G.992.3 Annex M is used. • *ANSI T1.413*: ANSI T1.413 Only for **ADSL Mode** = *Annex B* • *ETSI T1.413*: ETSI T1.413
Transmit Shaping	Select whether the data rate in the send direction is to be reduced. This is only needed in a few cases for special DSLAMs. Possible values: • *Default (Line Speed)* (default value): The data rate in the send direction is not reduced. • *128,000 bps* to *2,048,000 bps*: The data rate in the send direction is reduced to a maximum of 128,000 bps to 2,048,000 bps in defined steps. • *User-defined*:The data rate is reduced to the value entered in **Maximum Upstream Bandwidth**.
Maximum Upstream Bandwidth	Only for **Transmit Shaping** = *User-defined* Enter the maximum data rate in the send direction in bits per second.
SNR Margin	The signal-to-noise ratio (SNR) can be controlled via the slider from 0 to 5 dB. Change the value only for DLS line problems.

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

Fields in the Advanced Settings menu.

Field	Description
DSL Line Profile	Only for devices with a VDSL modem Select the line profile for your internet service provider. Use the *Standard* profile if your provider does not appear in the list.

7.5 SHDSL

bintec R3802 has an integrated SHDSL modem. The device supports G.SHDSL according to ITU-T recommendations G.991.2 Annex A and B and SHDLS.bis according to G.991.2 Annex F and G. Depending on the device type and configuration the gateway transmits the data over a pair of wires at up to 5696 kbps, over two pairs of wires at up to 11392 kbps, over three pairs of wires at up to 17088 kbps or over four pairs of wires at up to 22784 kbps.

7.5.1 SHDSL Configuration

In the **SHDSL** menu you configure the SHDSL interface of your device.

Note

Ask your provider about any special features of your SHDSL connection.

Note

Agree the connection conditions for back-to-back connections (campus connect) with your remote terminal.

The SHDSL interfaces can be configured separately or as a bundle.

Choose the button to edit the predefined SHDSL interfaces. In the ex works state, the logical SHDSL interfaces *Shdsl-0* to *Shdsl-3* are each preset with one pair of wires.

Fields in the SHDSL Parameters menu.

Field	Description
ATM Interface	Displays the name of the ATM interface.
Device Mode	Define the role within the connection. Possible values: • *CPE (Customer Premises Equipment)* (default value): Mode for the user page of the SHDSL connection. • *CO (Central Office)*: Mode for the provider page of the SHDSL connection. Note: CPE on the one hand and CO on the other hand must al-

Field	Description
	ways be set for each SHDSL connection. All the pairs of wires should also be set to the same mode - no mixed mode is possible.
SHDSL Type	Define which Annex of ITU-T Recommendation G.991.2 is used for the connection. Possible values: • *Annex A*: For applications in North America (provider-dependent). • *Annex B* (default value): For applications in Europe (provider-dependent) for example.
Clock Rate	Define whether the clock rate should be negotiated. Possible values: • *Fixed*: The clock rate is predefined. • *Adaptive* (default value): The clock rate is negotiated depending on the line quality. Note that a fixed value must be set to use the IMA mode (see *Wire Mode*) on at least one side (CO or CPE).
Wire Mode	Define the number and combination of wires (depending on the device type) used for the SHDSL connection. Possible values: • *2 wire*: Two wires are used with m-pair bonding for a clock rate of 192 kbps to 5696 kbps. • *4 wire*: Four wires are used with m-pair bonding for a clock rate of 384 kbps to 11392 kbps. This option supports 4-wire mode under G991.2 and Globespan Enhanced Mode. • *4 wire standard*: Four wires are used for m-pair bonding with a clock rate of 384 kbps to 11392 kbps. This option supports 4-wire mode under G991.2 but not Globespan Enhanced Mode. • *4 wire IMA*: 4 wires are used with IMA for a clock rate of 384 kbps to 11392 kbps. • *6 wire*: 6 wires are used with m-pair bonding for a clock rate

Field	Description
	of 576 kbps to 17088 kbps. • *6 wire IMA*: 6 wires are used with IMA for a clock rate of 576 kbps to 17088 kbps. • *8 wire*: 8 wires are used with m-pair bonding for a clock rate of 768 kbps to 22784 kbps. • *8 wire IMA*: 8 wires are used with IMA for a clock rate of 768 kbps to 22784 kbps.
Additional Wire Pairs	Only for **Wire Mode** = *4 wire*, *4 wire standard*, *4 wire IMA*, *6 wire*, *6 wire IMA*. For **Wire Mode** = *4 wire*, *4 wire standard* or *4 wire IMA* the second pair of wires is defined here. For **Wire Mode** = *6 wire* or *6 wire IMA* the second and third pair of wires is defined here. Wire pairs already used in defined connections are not available for selection. If these continue to be used for this SHDSL connection, the existing connection must first be terminated.
Minimum Number of active Links	For **Wire Mode** = *4 wire IMA*, *6 wire IMA* or *8 wire IMA* the minimum number of active links is defined.
Requested Rate	Only for **Clock Rate** = *Fixed*. Select which speed should be used.
Line Speed Interval	Only for **Clock Rate** = *Adaptive*. Under **Minimum** select the minimum clock rate and under **Maximum** the maximum clock rate for the connection.

Chapter 8 LAN

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

8.1 IP Configuration

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

8.1.1 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

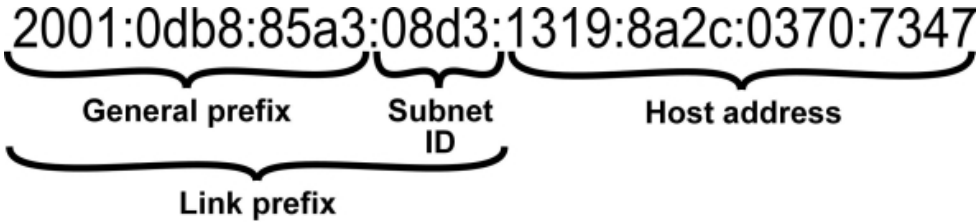
will only be able to access your device over this IP address. The device will no longer obtain an IP configuration dynamically over DHCP.

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:



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

8.1.1.1 Edit or New

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

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

Fields in the Basic Parameters menu.

Field	Description
Based on Ethernet Interface	This field is only displayed if you are editing a virtual routing interface. Select the Ethernet interface for which the virtual interface is to be configured.
Interface Mode	Only for physical interfaces in routing mode and for virtual interfaces. Select the configuration mode of the interface. Possible values: • *Untagged* (default value): The interface is not assigned for a specific purpose. • *Tagged (VLAN)*: This option only applies for routing interfaces. You use this option to assign the interface to a VLAN. This is done using the VLAN ID, which is displayed in this mode and can be configured. The definition of a MAC address in **MAC Address** is optional in this mode.
VLAN ID	Only for **Interface Mode** = *Tagged (VLAN)* This option only applies for routing interfaces. Assign the interface to a VLAN by entering the VLAN ID of the relevant VLAN. Possible values are *1* (default value) to *4094*.
MAC Address	Enter the MAC address associated with the interface. For virtual

Field	Description
	interfaces, you can use the MAC address of the physical interface under which the virtual interface was created by activating **Use built-in**, but VLAN IDs must be different. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed). If **Use built-in** is active, the predefined MAC address of the allocated physical interface is used. **Use built-in** is activated by default.

Fields in the Basic IPv4 Parameters menu.

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited.. • *Untrusted*: Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
Address Mode	Select how an IP address is assigned to the interface. Possible values: • *Static* (default value): The interface is assigned a static IP address in **IP Address / Netmask**. • *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
DHCP Metric	It is possible to assign a metric for gateway route received by an interface via DHCP. This may be necessary when configuring backup connections to ensure a clean switch to the backup and back again. The default value is *1*. In case of a backup solution, this option should be set to a higher value so the backup route does not receive a too high priority.

Field	Description
IP Address / Netmask	Only for **Address Mode** = *Static* With **Add**, add a new address entry, enter the **IP Address** and the corresponding **Netmask** of the virtual interface.

Fields in the Basic IPv6 Parameters menu.

Field	Description
IPv6	Select whether this interface should use Internet Protocol version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled*. The function is disabled by default.
Security Policy	Only for **IPv6** = *Enabled* Select the security settings to be used with the interface. Possible values: • *Trusted* (default value): All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. • *Untrusted*: Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. We recommend you use this setting if you want to use IPv6 outside of your LAN. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
IPv6 Mode	Only for **IPv6** = *Enabled* 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. Possible values: • *Router (Transmit Router Advertisement)* (default value): Select whether Router Advertisements are to be sent via the interface.

Field	Description
	Using Router Advertisements the list of prefixes is propagated and the router propagates itself as the standard gateway. The function is activated by selecting *Enabled*. The function is enabled by default. • *Host*: The interface is operated in host mode.
DHCP Server	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Router (Transmit Router Advertisement)* 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. Enable this option if hosts are to create IPv6 addresses through SLAAC. The function is activated by selecting *Enabled*. The function is enabled by default.
IPv6 Addresses	Only for **IPv6** = *Enabled* You can assign **IPv6 Addresses** to the selected interface.. **Add** allows you to create one or more address entries. A new windows opens that allows you to specify an IPv6 address consisting of a Link Prefix and a host identifier. If your device operates in host mode (**IPv6 Mode** = *Host*, **Accept Router Advertisement** *Enabled* and **DHCP Client** = *Enabled*), its IPv6 addresses are determined through SLAAC. You need not configure an IPv6 address manually, but you can enter addtional addresses if desired. If your device is operating in router mode (**IPv6 Mode** = *Router (Transmit Router Advertisement)*, and **DHCP Server** = *Enabled*), you need to configure its IPv6 addresses here.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Select if Router Advertisements are to be received on the selec-

Field	Description
	ted interface. Router Advertisements are used, e.g., to create the prefix list. The function is activated by selecting *Enabled*. The function is enabled by default.
DHCP Client	Only for **IPv6** = *Aktiviert* and **IPv6 Mode** = *Host* 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. The function is activated by selecting *Enabled*. The function is enabled by default.

Use **Add** to create more entries.

Fields in the Basic Parameters menu.

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

Fields in the Link Prefix menu.

Field	Description
Setup Mode	Select in which way the Link Prefix is to be determined. Possible values: • *From General Prefix* (default value): The Link Prefix is derived from a General Prefix. • *Static*: You can enter the link prefix.
General Prefix	Only for **Setup Mode** = *From General Prefix*

Field	Description
	Select the General Prefix the Link Prefix is to be derived from. You can choose from the General Prefixes available under **Network**->**IPv6 General Prefixes**->**General Prefix Configuration**->**New**.
Auto Subnet Configuration	Only if **Setup Mode** = *From General Prefix* and if a General Prefix has been selected. Select if the subnet is to be created automatically. Automatic subnet creation will use ID *0* for the first subnet, ID *1* for the second, etc. Possible values for the sub net ID are: *0* - *255*. 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. The function is activated by selecting *Enabled*. The function is enabled by default. If the function is disabled, you can define a subnet by entering a Subnet ID.
Subnet ID	Only if **Auto Subnet Configuration** is not active. 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. Possible values are *0* - *255*. Upon subnet creation the decimal ID value is converted to a hexadecimal one.
Link Prefix	Only for **Setup Mode** = *Static* You can specify the Link Prefix of an IPv6 address. This prefix must end with *::*. Its predetermined length is *64*.

Fields in the Host Address menu.

Field	Description
Generation Mode	Determine if the Host Identifier of the IPv6 address is to be automatically derived from the MAC address through EUI-64.

Field	Description
	The function is activated by selecting *Enabled*. The function is enabled by default. EUI-64 triggers the following process: • The hexadecimal 48 bit MAC address is split into 2 x 24 bit. • *FFFE* is inserted into the created gap in order to obtain 64 bit. • The hexadecimal notation of the 64 bit is converted to a binary notation. • Bit no. 7 of the first 8 bit field is set to *1*.
Static Addresses	Independently of the automatic creation described under **Generation Mode**, you can manually specify the Host Identifier of one or more IPv6 addresses with **Add**. Its predefined length is *64*. Start any entry with *::*.

The fields in the **Advanced** menu are part if 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
On Link Flag	Select whether the On-Link Flag (L-Flag) should be set. This allows the host to enter the prefix from the prefix list. The function is activated by selecting *True*. The function is enabled by default.
Autonomous Flag	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. The function is activated by selecting *True*. The function is enabled by default.
Preferred Lifetime	Enter a time period in seconds. During this time, addresses derived from the prefix through SLAAC are preferred. The default value is *604800* seconds.
Valid Lifetime	Enter a time period in seconds, for which the prefix is valid.

Field	Description
	The default value is *2592000* seconds. **Note** The value for the valid lifetime should be lower than the one configured for the option **Router Lifetime** under **Advanced IPv6 Settings**.

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

Fields in the Advanced IPv4 Settings menu.

Field	Description
DHCP MAC Address	Only for **Address Mode** = *DHCP* If **Use built-in** is activated (default setting), the hardware MAC address of the Ethernet interface is used. In the case of physical interfaces, the current MAC address is entered by default. If you disable **Use built-in**, you enter an MAC address for the virtual interface, e.g. *00:e1:f9:06:bf:03*. 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.
DHCP Hostname	Only for **Address Mode** = *DHCP* Enter the host name requested by the provider. The maximum length of the entry is 45 characters.
DHCP Broadcast Flag	Only for **Address Mode** = *DHCP* Choose whether or not the BROADCAST bit is set in the DHCP requests for your device. Some DHCP servers that assign IP addresses by UNICAST do not respond to DHCP requests with the set BROADCAST bit. In this case, it is necessary to send DHCP requests in which this bit is not set. In this case, disable this option. The function is activated by selecting *Enabled*. The function is enabled by default.

Field	Description
Create Default Route	Only for **Address Mode** = *DHCP* Select, whether a default route is to be defined for this interface. The function is activated by selecting *Enabled*. The function is enabled by default.
Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of defined remote terminals. The function is activated by selecting *Enabled*. The function is disabled by default.
TCP-MSS Clamping	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. The function is activated by selecting *Enabled*. The function is disabled by default. Once enabled, the default value *1350* is entered in the input field.

Fields in the Advanced IPv6 Settings menu

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

Note

The value for the **Router Lifetime** should be higher than the shortest valid lifetime for a link prefix configured for this interface under **Basic IPv6 Parameters**.

Field	Description
Router Preference	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** = *Enabled* 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. Possible values: • *High* • *Medium* (default value) • *Low*
DHCP Mode	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** = *Enabled* Select the information to be forwarded to the DHCP client. **Note** To achieve this, your router must not be set up as a DHCP server. By selecting *Other - DNS Servers, SIP Servers* (default value) no address- related information, such as i.e. DNS, VoIP, etc., is passed through. 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. By selecting *Managed - IPv6 Address Management* hosts receive IPv6 addresses as well as not address-related information through DHCP.
DNS Propagation	Only for **IPv6 Mode** = *Router (Transmit Router Advertisement)* and **Transmit Router Advertisement** *Enabled* Select if an in which way DNS server addresses are to be propagated in Router Advertisements. A maximum of two DNS server addresses is propagated.

Field	Description

	Possible values:
	• *Off*: No DNS server address propagation
	• *Self*: The device sends its own IP adderss as DSN server address. If the device has multiple addresses, they are used in the following order:
	  • Global addresses
	  • ULA (Unique Local Addresses)
	  • Link local addresses
	• *Other*: 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.

8.2 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 predefined 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.

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**.

8.2.1 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.

8.2.1.1 Edit or New

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

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

Fields in the Configure VLAN menu.

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

8.2.2 Port Configuration

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

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

Fields in the Port Configuration menu.

Field	Description
Interface	Shows the port for which you define the PVID and processing

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

8.2.3 Administration

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

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

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

Field	Description
Enable VLAN	Enable or disable the specified bridge group for VLAN. The function is enabled with *Enabled*. The function is not activated by default.

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 controller and access points.

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.

Note

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

9.1.1 Wireless LAN Controller Wizard

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

9.1.1.1 Basic Settings

The wireless LAN controller uses the following settings:

Regulatory domain

Select the regulation area here. The selection here determines the countries that you can select for the option **Region**. The default value is *ETSI* (European Telecommunications Standards Institute).

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 controller and access points.

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

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

If you wish to use a bintec elmeg Gateway for example as a DHCP server, click on the **GUI** menu for this device under **Local Services**->**DHCP Server**->**DHCP Configuration**->**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.

9.1.1.2 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.

9.1.1.3 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.

9.1.1.3.1 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.

IGMP Snooping

IGMP snooping reduces the data traffic and thus the network load.

The function is activated by selecting *Enabled*.

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, WPA 2, WPA3 or a combination.

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 unauthorized access!

Radius Server

When using *WPA Enterprise*, 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 Preauthentification

For **Security Mode** = *WPA Enterprise*, select whether the EAP preauthentification 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.

9.1.1.4 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 is 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 licenses available, the message "The maximum number of access points that can be supported has been exceeded". Please check your licenses. If this message is displayed then you should obtain additional licenses 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 up-

dated.

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 Neighbor scan** 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.

9.1.2 Wireless LAN Controller VLAN Configuration

In order to separate WLANs (VSS) from each other, you can activate the VLAN function and assign a VLAN ID during the configuration of a VSS. For the separation from other interfaces to work properly, you need to create a virtual interface with its own IP configuration, and, if applicable, a corresponding DHCP pool which provides IP addresses to clients connecting to this VLAN. You can make this settings - as usual - in the menus **LAN**->**IP Configuration** and **Local Services**->**DHCP Server**, correspondingly; or you make use of the menu offered here. All settings you make here are automatically transferred to the other menus, as well.

You are shown an overview of VLANs that have already been created with their VLAN IDs and their corresponding IP and DHCP configuration. In order to edit an entry, select the icon in the respective line. To create a new entry, select **New**. A new entry can only be created for a VSS with a VLAN ID that does not yet have a VLAN configuration.

9.1.2.1 Edit or Neu

Select the symbol in order to edit an existing entry. Select the **New** button in order to create additional VLANs.

The menu **Wireless LAN Controller**->**Wizard**->**Wireless LAN Controller VLAN Configuration**->**New** consists of the following fields:

Fields in the menu VSS VLAN Network Configuration

Field	Description
VLAN ID	Select an existing VLAN from the pull down menu. Only those

Field	Description
	IDs without a configuration are offered.
IP Address/Netmask	Specify the IP configuration of the new interface. Make sure that the address has not been used before.
DHCP Server	In order to provide clients connecting to this VLAN with an IP configuration, you can either use an external DHCP server, or you can use the integrated one of your device. Possible values: • *External or static*: Select this option if you are already operating a DHCP server in you network, tor if clients connecting to this VLAN have a static IP configuration. Make sure that an external DHCP server can be reached from the VLAN. • *Internal*: Select this option if you intend to use your device as DHCP server for this VLAN.
IP Address Range	Only for **DHCP Server** = *Internal* Specify the first and the last IP address which your device is to distribute inside the VLAN. Make sure that the address range corresponds to the IP address of the interface for this VLAN, and that it does not overlap with other IP address pools. The DHCP configuration automatically assumes your device to be the gateway. The lease time is 120 minutes. If you want to adjust these settings, go to the menu **Local Services**->**DHCP Server**->**DHCP Configuration**.

9.2 Controller Configuration

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

9.2.1 General

The **Wireless LAN Controller**->**Controller Configuration**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Status	Enable the **Status** option to make the basic settings for the wireless LAN controller. The function is disabled by default.
Delete the complete WLAN Controller configuration	Only for **Status** = disabled. You can delete a configuration using the icon.
Regulatory domain	Select the regulation area here. The selection here determines the countries that you can select for the option **Region**. The default value is *ETSI* (European Telecommunications Standards Institute).
Region	Select the country in which the wireless LAN controller is to be operated. Possible values are all the countries configured on the device's wireless module. The range of channels that can be used varies depending on the country setting. The default value is *Germany*.
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 controller and access points. Please note: Make sure that option 138 is active when using an external DHCP server. If you wish to use a bintec elmeg Gateway for example as a DHCP server, click on the **GUI** menu for this device under **Local Services**->**DHCP Server**->**DHCP Pool**->**New**->**Advanced Settings** in the **DHCP Options** field on the **Add** button. Select as **Option** *CAPWAP Controller* and in the **Value** field enter the IP address of the WLAN controller.

Field	Description
	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. Possible values: • *External or static* (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. • *Internal*: Your device, on which the CAPWAP option 138 is active, assigns the IP addresses to the APs.
IP Address Range	Only for **DHCP Server** = *Internal* Enter the start and end IP address of the range. These IP addresses and your device must originate from the same network.
AP location	Select whether the APs that the wireless LAN controller is to manage are located in the LAN or the WAN. Possible values: • *Local (LAN)* (default value) • *Remote (WAN)* The *Remote (WAN)* 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 *Remote (WAN)* maintains its configuration until the connection is reestablished. It then boots up and the controller and the AP then resynchronize.
AP LED mode	Select the lighting scheme of the AP LEDs. Possible values: • *State* (default value): All LEDs show their standard behavior. • *Flashing*: Only the status LED flashes once per second.

Field	Description
	• *Off*: All LEDs are deactivated.

9.2.2 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

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

Fields in the Access Point Filter menu

Field	Description
MAC Address	Enter the MAC address of an access point that is to be configured automatically when it is integrated into the network. By default, **All** is activated so that the entry matches every new access point.
IP Address / Netmask	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.

Fields in the Access Point Settings menu

Field	Description
Location	Specify the location of the AP.
Description	Enter a unique description for the AP.

Fields in the Radio 1 or in the Radio 2

Field	Description
Operating Mode	Select if the access point to which this profile is applied should enable the respective radio module. The function is activated by selecting *Enabled*. The function is enabled by default.
Active Radio Profile	Only for **Operating Mode** = *Enabled*

Field	Description
	Select a radio profile. Possible values: • *2.4 GHz Radio Profile* • *5 GHz Radio Profile*
Assigned Wireless Network (VSS)	Only for **Operating Mode** = *Enabled* Add a new radio profile with **Add**.

9.3 AP configuration

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

9.3.1 Access Points

In the **Wireless LAN Controller**-> **AP configuration**-> **Access Points** menu a list of all APs found with the wizard is displayed.

You will see an entry with a parameter set for each access point (**Location**, **Name**, **IP Address**, **LAN MAC Address**, **Channel**, **Search Channel**, **Status**, **Action**). Choose whether the selected Access Pont is to be managed by the WLAN Controller by clicking the ^ button or the v 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 v button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.

Click on the **START** button under **Channel reallocation** in order to reassign any assigned channels, e.g. when a new access point has been added.

Possible values for Status

Status	Meaning
Discovered	The AP has registered at the wireless LAN controller. The controller has prompted the required parameters from the AP.
Initializing	The WLAN controller and the APs "communicate" via CAPWAP. The configuration is transferred and enabled to the APs.
Managed	The AP is set to "Managed" status. The controller has sent a configuration to the AP and has enabled this. The AP is managed centrally from the controller and cannot be configured via

Status	Meaning
	the **GUI**.
No License Available	The AP does not have an unassigned licence for this AP.
Offline	The AP is either administratively disabled or switched off or has its power supply cut off etc.

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.

The data for wireless module 1 and wireless module 2 are displayed in the **Wireless LAN Controller**-> **AP configuration**-> **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 menu

Field	Description
Device Type	Here you can see various relevant information about this access point, such as: ...the type of access point being managed.
Serial Number	... the serial number of the managed device.
LAN MAC Address	... the MAC address of the LAN interface of the managed device.
Radio Module 1 supported features	Information about the features supported by the access point: • Operation band(s) • Bandwidth • Wireless Mode • Spatial Streams • Data Rate Trimming • WPA 3

Fields in the Access Point Settings menu.

Field	Description
Device	Displays the type of device for the AP.
Location	Displays the locality of the AP. The locations are given numbers if no location has been entered. You can enter another locality.
Name	Displays the name of the AP. You can change the name.
Description	Enter a unique description for the AP.
CAPWAP Encryption	Select whether communication between the controller and access points is to be encrypted. The function is activated by selecting *Enabled*. The function is enabled by default. You can override the encryption in order to view the communication for debugging purposes.

Fields in the Wireless module1 or in the Wireless module 2 menu.

Field	Description
Operation Mode	Displays the mode in which the wireless module is to be operated. You can change the mode. 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 is being set up.
Channel	Displays the channel that is assigned. You can select another channel. The number of channels you can select depends on the country setting. Please consult the data sheet for your device. Access Point mode

Field	Description
	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. Possible values (according to the selected wireless module profile): • For **Active Radio Profile** = *2.4 GHz Radio Profile* Possible values are *1* to *13* and *Auto* (default value). • For **Active Radio Profile** = *5 GHz Radio Profile* Depending on the selected module profile, possible values are *36*, *40*, *44*, *48* and *Auto* (default value)
Used Channel	Only for managed APs. Displays the channel that is currently in use.
Transmit Power	Displays the transmission power. You can select another transmission power. Possible values: • *Max.* (default value): The maximum antenna power is used. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*
Assigned Wireless	Displays the wireless networks that are currently assigned.

Field	Description
Network (VSS)	

9.3.2 Radio Profiles

An overview of all created wireless module profiles is displayed in the **Wireless LAN Controller**-> **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.

The **Wireless LAN Controller**-> **AP configuration**->**Radio Profiles**-> **/ New** menu consists of the following fields:

Fields in the menu Radio Profile Definition

Field	Description
Description	Enter the desired description of the wireless module profile.
Operation Mode	Define the mode in which the wireless module profile is to be operated. Possible values: • *Off* (default value): The wireless module profile is not active. • *Access Point*: Your device is used as an access point in your network.
Operation Band	Select the frequency band of the wireless module profile. Possible values: • *2.4 GHz In/Outdoor* (default value): Your device is operated at 2.4 GHz inside or outside buildings. • *5 GHz Indoor*: Your device is operated at 5 GHz inside buildings. • *5 GHz Outdoor*: Your device is operated at 5 GHz outside

Field	Description
	buildings. • *5 GHz In/Outdoor*: Your device is operated at 5 GHz inside or outside buildings. • *5.8 GHz Outdoor*: 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.

Fields in the menu Performance Settings

Field	Description
Wireless Mode	Select the wireless technology that you want the access point to use. For the *2,4 GHz In/Outdoor* **Operation Band** all modes from *802.11b* up to the current *802.11ax* are available (but not 802.11ac which is used only in 5GHz mode), as well as combinations of these modes. Keep in mind that not all access points and not all clients always support the latest modes. For **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* or *5,8 GHz Outdoor* all modes from *802.11a* to the current *802.11ax* are available (but not 802.11b and g which are not specified for 5-GHz), as well as combinations of these modes. Keep in mind that not all access points and not all clients always support the latest modes.
Bandwidth	Only for **Operation Band** = *5 GHz* and not for **Wireless Mode** *802.11a*. Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: 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. • *80 MHz*: Four channels with 20 MHz bandwidth each are used. Thus a bandwidth of 80 MHz is available.

Field	Description
Number of Spatial Streams	Select how many data streams are to be used in parallel. Possible values: `1` to `4`. The available options depend on the combination of the operation band and wireless mode as well as on the access point model.
Airtime fairness	This function is not available for all devices. The **Airtime fairness** function ensures that the access point's send resources are distributed intelligently to the connected clients. This means that a powerful client (e. g. an 802.11n client) cannot achieve only a poor flow level, because a less powerful client (e. g. an 802.11a client) is treated in the same way when apportioning. The function is enabled with `Enabled`. The function is disabled by default. This function is only applied to unprioritized frames of the WMM Class "Background".
Cyclic Background Scanning	Not all devices support this function. You can enable the **Cyclic Background Scanning** function so that a search is run at regular intervals for neighboring or rogue access points in the network. This search is run without negatively impacting the function as an access point. Enable or disable the function **Cyclic Background Scanning**. The function is enabled with `Enabled`. The function is not activated by default.

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

Fields in the menu Advanced Settings

Field	Description
Channel Plan	Select the desired channel plan. The so-called channel plan allows the automatic selection of channels based on specific choices. This ensures that channels do not overlap, i.e., a gap of at least four channels is maintained between the channels used. This is useful if multiple access

Field	Description
	points with overlapping radio cells are used. Possible values: • *All*: All channels can be chosen during channel selection. • *World Mode* (for **Operation Band** = *2.4 GHz*, default value): Automatic channel selection uses only the non-overlapping channels *1*, *6*, *11*. • *ETSI Mode* (for **Operation Band** = *2.4 GHz*): Automatic channel selection uses only the non-overlapping channels *1*, *5*, *9*, *13*. • *No weather radar channels* (for **Operation Band** = *5 GHz*, default value): The weather radar channels are excluded from channel selection. Possible values: *36*, *40*, *44*, *48*, *52*, *56*, *60*, *64*, *100*, *104*, *108*, *112*, *116*, *132*, *136*, *140*. • *Indoors No DFS/TPC*: These channels can be used inside buildings. DFS (Dynamic Frequency Selection) and TPC (Transmitter Power Control) are not enabled. Possible values: *36*, *40*, *44*, *48*. • *No outdoor channels* (for **Operation Band** = *5 GHz*): This channel plan combines channels 36 to 64, which are specified for indoor applications only. Especially 5GHz WLAN-capable multimedia devices such as smart TVs, which often do not support the 5GHz outdoor channels (from channel 100 upwards), can be optimally integrated into the WLAN network. • *User defined*: Select the desired channels.
User Defined Channel Plan	Only for **Channel Plan** = *User defined* The currently selected channels are displayed here. With **Add** you can add channels. If all available channels are displayed, you cannot add any more entries. You can also delete entries using the icon.

Field	Description
Switch Channel on Jammer	Activate this option if the access point should change the radio channel if the connection is affected by interferences.
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.
Max. Transmission Rate	Select the transmission speed. Possible values: • *Auto* (default value): The transmission speed is determined automatically. • *<Value>*: According to setting for **Operation Band**, **Bandwidth**, **Number of Spatial Streams** and **Wireless Mode** various fixed values in mbps are available.
Beacon Period	Enter the time in milliseconds between the sending of two beacons. This value is transmitted in Beacon and Probe Response Frames. Possible values are *1* to *65535*. The default value is *100*.
DTIM Period	Enter the interval for the Delivery Traffic Indication Message (DTIM). 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. Possible values are *1* to *255*. The default value is *2*.
RTS Threshold	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.

Field	Description
Short Retry Limit	Enter the maximum number of attempts to send a frame with length less than or equal to the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are `1` to `255`. The default value is `7`.
Long Retry Limit	Enter the maximum number of attempts to send a data packet of length greater than the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are `1` to `255`. The default value is `4`.
Fragmentation Threshold	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`.

9.3.3 Wireless Networks (VSS)

An overview of all created wireless networks is displayed in the **Wireless LAN Controller**-> **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.

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

Fields in the menu Service Set Parameters

Field	Description
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)** is to be transmitted. The network name is displayed by selecting *Visible*. It is visible by default.
Intra-cell Repeating	Select whether communication between the WLAN clients is to be permitted within a radio cell. The function is activated by selecting *Enabled*. The function is enabled by default. Users of the guest WLAN should normally have access to the Internet but no access to the company's intranet. To prevent this, the option must be disabled. be.
U-APSD	Select whether the Unscheduled Automatic Power Save Delivery (U-APSD) mode is to be enabled. The function is activated by selecting *Enabled*. The function is enabled by default.
IGMP Snooping	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. The function is activated by selecting *Enabled*. The function is disabled by default.

Fields in the menu Security Settings

Field	Description
Security Mode	Select the security mode (encryption and authentication) for the wireless network. Possible values: • *OWE-Transition* The *OWE-Transition* setting does not require the input of a **Preshared Key** and is suitable for open guest networks. It is suitable for networks that are to be used by WPA3-capable clients, but also by older, non-WPA3-capable clients. Data transmission between access point and client is encrypted for clients supporting **WPA3**. For clients not supporting **WPA3**, data transmission is unencrypted. • *OWE* **Note** OWE only works with clients supporting WPA3 and OWE. The *OWE* setting does not require the input of a **Preshared Key** and is suitable for open guest networks. Nevertheless, data transmission between the access point and the clients is encrypted. • *Inactive* (default value): Neither encryption nor authentication • *WEP 40*: WEP 40 bits • *WEP 104*: WEP 104 bits • *WPA-PSK*: WPA Preshared Key • *WPA Enterprise*: 802.11x
Transmit Key 1-4	Only for **Security Mode** = *WEP 40* or *WEP 104* Select one of the keys configured in **WEP Key** as a standard key. The default value is *Key 1*.
WEP Key 1-4	Only for **Security Mode** = *WEP 40*, *WEP 104* Enter the WEP key.

Field	Description
	Enter a character string with the right number of characters for the selected WEP mode. For *WEP 40* you need a character string with 5 characters, for *WEP 104* with 13 characters.
WPA Mode	For **Security Mode** = *WPA-PSK* and *WPA Enterprise* Possible values: • *WPA*: WLAN clients that support **WPA** can connect. • *WPA2*: WLAN clients that support **WPA2** can connect. • *WPA3*: Only WLAN clients that support **WPA3** can connect. • *WPA and WPA2* : WLAN clients that support **WPA1** or **WPA2** can connect. • *WPA2 and WPA3* (default value): WLAN clients that support **WPA2** or **WPA3** can connect.
WPA Cipher	For **Security Mode** = *WPA-PSK* or *WPA Enterprise* and for **WPA Mode** = *WPA* or *WPA and WPA2* Select the type of encryption you want to apply. Possible values: • *AES* : AES is used. • *TKIP*: TKIP is used. • *AES and TKIP* (default value): AES or TKIP is used.
WPA2 Cipher	For **Security Mode** = *WPA-PSK* or *WPA Enterprise* and for **WPA Mode** = *WPA2* or *WPA and WPA2* Select the type of encryption you want to apply. Possible values: • *AES* : AES is used. • *AES and TKIP* (default value): AES or TKIP is used.
WPA2/3 Cipher	For **Security Mode** = *WPA PSK* or *WPA Enterprise* and for **WPA Mode** = *WPA2 and WPA3* only AES encryption is supported. No further settings are required.
WPA3 Cipher	For **Security Mode** = *WPA PSK* or *WPA Enterprise* and for

Field	Description
	WPA Mode = *WPA3* AES encryption with the following AES variants is supported: • AES • AES-GCMP • AES-256 • AES-GCMP-256.
Preshared Key	Only for **Security Mode** = *WPA-PSK* Enter the WPA password. Enter an ASCII string with 8 - 63 characters. **Note** Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorized access!
Radius Server	Only for **Security Mode** = *WPA Enterprise* 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 RADIUS server.
EAP Preauthentification	Only for **Security Mode** = *WPA Enterprise* Select whether the EAP preauthentification 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. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	Enter the maximum number of clients that can be connected to this wireless network (SSID) 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. Possible values are whole numbers between *1* and *254*. The default value is *32*.
Max. number of clients - soft limit	Not all devices support this function. To avoid a radio module being fully utilized, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the **Max. number of clients - hard limit** is reached. The value of the **Max. number of clients - soft limit** must be the same as or less than that of the **Max. number of clients - hard limit**. The default value is *28*. You can disable this function if you set **Max. number of clients - soft limit** and **Max. number of clients - hard limit** to identical values.
Client Band select	Select whether the 5 GHz band is preferred. Possible values: • *Disabled - optimized for fast roaming*: the 5 GHz band is not preferred, fast roaming is used. • *5 GHz band preferred*: the 5 GHz band is preferred to be used if available.

Field	Description
	Note For the *5 GHz band preferred* setting, configure the same SSID in both client bands.
	• *AP Steering* (Access Point Steering): With Access Point Steering, a WLAN client may not only be directed to another comfort band, but also to another access point. This requires the activation of 802.11k/v.
802.11r (Fast BSS Transition):	802.11r enables an uninterrupted connection even with strongly encrypted WLAN networks when the WLAN client switches from one access point to another.
Radio Resource Management (802.11k) and **Network assisted Roaming (802.11v)**	802.11k/v exchanges information between WLAN client and WLAN access point and uses this information to control the load distribution between several access points more efficiently. These two options are usually activated together, but can also be configured separately. 802.11v controls the exchange of information about the current network topology, while 802.11k controls intelligent client roaming based on the topology data.

Fields in the menu MAC-Filter

Field	Description
Access Control	Select whether only certain clients are to be permitted for this wireless network. The function is activated by selecting *Enabled*. The function is disabled by default.
Allowed Addresses	Use **Add** to make entries and enter the MAC addresses (**MAC Address**) of the clients to be permitted.
Dynamic blacklisting	You can use the **Dynamic blacklisting** function to identify clients that want to gain possibly unauthorized 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

Field	Description
	controller for the VSS concerned, so neither are they able to log into a different radio cell in that VSS. If a client needs to be blocked permanently, this can be done in the **Wireless LAN Controller**->**Monitoring**->**Rogue Clients** menu. The function is activated by selecting *Enabled*. The function is activated by default.
Failed attempts per Time	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. Default values are *10* failed attempts during *60* seconds.
Blacklist blocktime	Enter the time for which an entry in the dynamic blacklist remains valid. Default value is *500* seconds.

Fields in the menu VLAN

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

Fields in the menu Bandwidth limitation for each WLAN client

Field	Description
Rx Shaping	Select a bandwidth limitation in the receive direction. Possible values are • *No limit* (default value) • *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*,

Field	Description
	40 Mbit/s and *50 Mbit/s*.
Tx Shaping	Select a bandwidth limitation in the transmit direction. Possible values are • *No limit* (default value) • *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*.

Fields in the menu Data-rate trimming

Field	Description
2,4 GHz band rate profile	Data Rate Trimming allows you to optimize the performance of your wireless LAN. You can block low transfer rates and enforce the use of higher rates. Clients slowing down other clients through the use of low transfer rates are disconnected from the access point. Select the rate profile to be applied: • *All (Min. 1 MBit/s)* - All clients supporting a transfer rate of 1 MBit/s are allowed to connect to the access point. • *Min. 6 MBit/s (no 802.11b devices)* - see above, for clients with a minimum supported rate of 6 Mbit/s; clients using the obsolete standard 802.11b are not allowed. • *Min. 12 MBit/s (no 802.11b devices)* - see above, for clients with a minimum supported rate of 12 Mbit/s • *Min. 24 MBit/s (no 802.11b devices)* - see above, for clients with a minimum supported rate of 24 Mbit/s
5 GHz band rate profile	Possible values: • *All (Min. 6 MBit/s)* - All clients supporting a transfer rate of 6 MBit/s are allowed to connect to the access point. • *From 12 MBit/s* - see above, for clients with a minimum supported rate of 12 Mbit/s • *From 24 MBit/s* - see above, for clients with a minimum supported rate of 24 Mbit/s

Fields in the menu Low RSSI threshold management

Field	Description
RSSI threshold	The option **RSSI threshold** allows you to define a threshold for the expected strength of a client signal. If the signal strength of a client falls below this value for longer than determined by the **Grace time, the client is disconnected from the access point.** This forces the client to connect to a different access point offering the best possible signal strength. Specify the lower RSSI threshold in dBm. A client falling below this value for longer than allowed by the grace time is disconnected. The default value is `-110` dBm.
Grace time	Specify the time (in seconds) during which the signal strength of a client may fall below the RSSI threshold without the client being disconnected. The default value is `5` seconds.

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 APs, the internal time server of the WLAN Controller should be enabled.

9.4.1 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.
AP managed	Displays the number of managed access points.

Status	Meaning
APs manageable with currently installed licenses	bintec elmeg devices come with a free license for access point management. The number of manageable access points varies from device type to device type.
Maximum number of manageable APs by this device with full licenses	Due to different hardware equipment, bintec elmeg devices can manage a certain number of access points.
WLAN Controller: VSS throughput	Displays the data traffic in receive and transmit direction in bytes per second.
CPU usage [%]	Displays the percentaged CPU load over time.
Memory usage [%]	Displays the percentaged memory consumption over time.
Connected clients/VSS	Displays the number of connected clients per wireless network (VSS) over time.

9.4.2 Access Points

The menu **Wireless LAN Controller**->**Monitoring**-> **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 an summary with additional details about the **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.

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.

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

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**, **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**.

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)

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**, **AP Name**, **VSS**, **MAC Address (VSS)**, **Channel**, **Status**).

9.4.5 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

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 Own Access Points

This menus displays information about controller-managed access points as they "see" by each other. This provides useful information about the network created by your managed access points and helps you with identifying potential WLAN issues.

The menu includes information such as the access point name, the channel it is operating on, its signal strength and when it was last seen by which access point and on which channel.

9.5.3 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.

9.5.4 Rogue Clients

The **Wireless LAN Controller**->**Neighbor Monitoring**->**Rogue Clients** menu displays the clients which have attempted to gain unauthorized access to the network and which are therefore on the blacklist. The blacklist is configured for each VSS in the **Wireless LAN Controller**-> **AP configuration**->**Wireless Networks (VSS)** menu. You can also add a new entry to the static blacklist.

Possible values for Rogue Clients

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

9.5.4.1 New

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

The menu consists of the following fields:

Fields in the New Blacklist Entry menu

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

9.6 Maintenance

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

9.6.1 Firmware Maintenance

In the **Wireless LAN Controller**->**Maintenance**->**Firmware Maintenance** menu, a list of all **Managed Access Points** is displayed.

For each managed AP you will see an entry with the following parameter set: **Update firmware**, **Location**, **Device**, **IP Address**, **LAN MAC Address**, **Firmware Version**, **Status**.

Click the **Select all** button to select all of the entries for a firmware update. Click the **Deselect all** button to disable all entries and to then select individual entries if required (e.g. if there is a large number of entries and only individual APs are to be given software updates).

Possible values for Status

Status	Meaning
Image already exists.	The software image already exists; no update is required.
Error	An error has occurred.
Running	The operation is currently in progress.
Done	The update is complete.

The **Wireless LAN Controller**->**Maintenance**->**Firmware Maintenance** menu consists of the following fields:

Fields in the Firmware Maintenance menu

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • *Update system software*: You can also start an update of the system software. • *Save configuration with state information*: You can save a configuration which contains the AP status information.

Field	Description
Source Location	Select the source for the action. Possible values: • *HTTP server* (default value): The file is stored respectively on a remote server specified in the **URL**. • *Current Software from Update Server*: The file is on the official update server. (Only for **Action**= *Update system software*) • *TFTP server*: The file is stored respectively on a TFTP server specified in the **URL**.
URL	Only for **Source Location** = *HTTP server* or *TFTP server* Enter the URL of the update server from which the system software file is loaded or on which the configuration file is saved.

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.

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

The **Network**->**Routes**->**IPv4 Route Configuration**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Route Type	Select the type of route.

Field	Description
	Possible values: • *Default Route via Interface*: Route via a specific interface which is to be used if no other suitable route is available. • *Default Route via Gateway*: Route via a specific gateway which is to be used if no other suitable route is available. • *Host Route via Interface*: Route to an individual host via a specific interface. • *Host Route via Gateway*: Route to an individual host via a specific gateway. • *Network Route via Interface* (default value): Route to a network via a specific interface. • *Network Route via Gateway*: Route to a network via a specific gateway. Only for interfaces that are operated in DHCP client mode: 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. • *Default Route Template per DHCP*: The information of the gateway to be used is received via DHCP and integrated into the route. • *Host Route Template per DHCP*: The settings received by DHCP are supplemented by routing information about a particular host. • *Network Route Template per DHCP*: The settings received by DHCP are supplemented by routing information about a particular network.

Field	Description
	Note 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.
Interface	Select the interface to be used for this route.
Route Class	Select the type of **Route Class**. Possible values: • *Standard* (default value): Defines a route with the default parameters. • *Extended*: Select whether the route is to be defined with extended parameters. If the function is active, a route is created with extended routing parameters such as source interface and source IP address, as well as protocol, source and destination port, type of service (TOS) and the status of the device interface.

Fields in the menu Route Parameters

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

Field	Description
Gateway IP Address	Only for **Route Type** = *Default Route via Gateway*, *Host Route via Gateway* or *Network Route via Gateway* Enter the IP address of the gateway to which your device is to forward the IP packets.
Metric	Select the priority of the route. The lower the value, the higher the priority of the route. Value range from *0* to *15*. The default value is *1*.

Fields in the menu Extended Route Parameters

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

Field	Description
	• *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023. • *Server*: Entry of server port numbers: 5000 ... 32767. • *Clients 1*: Entry of client port numbers: 1024 ... 4999. • *Clients 2*: Entry of client port numbers: 32768 ... 65535. • *Not privileged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, for a range, the end port in **to Port**.
Destination Port	Only for **Layer 4 Protocol** = *TCP* or *UDP* Enter the destination port. First select the port number range. Possible values: • *Any* (default value): The route is valid for all port numbers. • *Single*: Enables the entry of a port number. • *Range*: Enables the entry of a range of port numbers. • *Privileged*: Entry of privileged port numbers: 0 ... 1023. • *Server*: Entry of server port numbers: 5000 ... 32767. • *Clients 1*: Entry of client port numbers: 1024 ... 4999. • *Clients 2*: Entry of client port numbers: 32768 ... 65535. • *Not privileged*: Entry of unprivileged port numbers: 1024 ... 65535. Enter the appropriate values for the individual port or start port of a range in **Port** and, for a range, the end port in **to Port**.
DSCP / TOS Value	Select the Type of Service (TOS). Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • *DSCP Decimal Value*: Differentiated Services Code Point

Field	Description
	according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F. Enter the relevant value for *DSCP Binary Value*, *DSCP Decimal Value*, *DSCP Hexadecimal Value*, *TOS Binary Value*, *TOS Decimal Value* and *TOS Hexadecimal Value*.
Mode	Select when the interface defined in **Route Parameters**->**Interface** is to be used. Possible values: • *Dialup and wait* (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". • *Authoritative*: The route can always be used. • *Dialup and continue*: 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". • *Never dialup*: The route can be used when the interface is "up". • *Always dialup*: 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".

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.

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

Fields in the Route Parameters menu

Field	Description
Description	Enter a description for the IPv6 route.
Route Active	Select if the route is to be active or inactive.. With *Enabled* the status of the route will be set to active. The function is enabled by default.
Route Type	Select the type of route. Possible values: • *Default Route via Interface* : Route via a specific interface which is used if no other adequate route is available. • *Default Route via Gateway*: Route via a specific gateway which is used if no other adequate route is available. • *Host Route via Interface*: Route to a single host via a specific interface. • *Host Route via Gateway*: Route to a single host via a specific gateway. • *Network Route via Interface*: Route to a network via a specific interface. • *Network Route via Gateway* (default value): Route to a network via a specific gateway.
Destination Interface	Select the IPv6 interface to be used for this route. You can choose from those interfaces available under **LAN**->**IP Configuration**->**Interfaces**->**New** that are IPv6-enabled.

Field	Description
Source Address / Length	Enter the source IPv6 address along with the corresponding prefix length. *::* describes an unspecific address. By default the prefix length *64* is predefined.
Destination Address / Length	Enter the destination IPv6 address along with the corresponding prefix length. *::* describes an unspecific address. By default the prefix length *64* is predefined.
Gateway Address	Enter a the IPv6 address for the next hop.
Metric	Select the priority of the route. The lower the value, the higher the priority of the route. Value range from *0* to *15*. The default value is *1*.

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.

Fields in the menu IPv4 Routing Table

Field	Description
Destination IP Address	Displays the IP address of the destination host or destination network.
Netmask	Displays the netmask of the destination host or destination network.
Gateway	Displays the gateway IP address. Nothing is displayed here

Field	Description
	when routes are received by DHCP.
Interface	Displays the interface used for this route.
Metric	Displays the route's priority. The lower the value, the higher the priority of the route.
Route Type	Displays the route type.
Extended Route	Displays whether a route has been configured with advanced parameters.
Protocol	Displays how the entry has been created , e.g. manually (*Local*) or via one of the available protocols.
Delete	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.

Fields in the IPv6 Routing Table menu

Field	Description
Route	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.
Interface	Displays the interface used for this route.
Metric	Displays the route's priority. The lower the value, the higher the priority of the route.
Protocol	Displays how the entry has been created , e.g. manually (*Local*) 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 activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface. You can therefore prevent the acceptance of packets with false IP addresses - even without using filters.

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
Mode	Select how the interfaces to be activated for Back Route Verify are to be specified. Possible values: • *Enable for all interfaces*: Back Route Verify is activated for all interfaces. • *Enable for specific interfaces* (default value): A list of all interfaces is displayed in which Back Route Verify is only enabled for specific interfaces. • *Disable for all interfaces*: Back route verify is disabled for all interfaces.
No.	Only for **Mode** = *Enable for specific interfaces* Displays the serial number of the list entry.
Interface	Only for **Mode** = *Enable for specific interfaces* Displays the name of the interface.
Back Route Verify	Only for **Mode** = *Enable for specific interfaces* Select whether *Back Route Verify* is to be activated for the interface. The function is enabled with *Enabled*.

Field	Description
	By default, the function is deactivated for all interfaces.

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 129 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.

Fields in the Basic Parameters menu.

Field	Description
General Prefix active	Select if the prefix is to be active or inactive.. With *Enabled* the status of the prefix will be set to active. The function is enabled by default.
Name	Enter a name for the General Prefix.

Field	Description
	A meaningful name helps selecting the General Prefix from a prefix list.
Type	Specify how the address range is to be assigned. Possible values: • *Dynamic* (default value): The general prefix will be set dynamically by DHCP transmission, e.g. from a provider. • *Static*: The prefix is fixed, e. g. by a provider.
From Interface	Only with **Type** = *Dynamic* Select the IPv6 interface from which a General Prefix is to be obtained. You can choose from all interfaces that are availabe under **LAN**->**IP Configuration**->**Interfaces**->**New** and that fullfil the following conditions: • **IPv6** is *Enabled*. • **IPv6 Mode** = *Host* • **DHCP Client** is *Enabled*.
Used Prefix / Length	Only with **Type** = *Static* Enter the prefix to be used. Enter the corresponding length. This prefix must end with ::. The default value is *48* .
Prefix Length	For a dynamically assigned prefix, you only need to enter the prefix length here. You can ask your service provider for the length of the assigned prefix if necessary. The default length here is *56*.

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 194).

Specific instructions for configuring NAT, see the end of the chapter *NAT - Configuration*

example on page 199.

10.3.1 NAT Interfaces

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

For every NAT interface, the *NAT active*, *Loopback active*, *Silent Deny* and *PPTP Passthrough* can be selected.

In addition, *Portforwardings* displays how many port forwarding rules were configured for this interface.

Options in the menu NAT Interfaces

Field	Description
NAT active	Select whether NAT is to be activated for the interface. The function is disabled by default.
Loopback active	The NAT loopback function also enables network address translation for connectors whereby NAT is not activated. This is often used in order to interpret queries from the LAN as if they were coming from the WAN. You can use this to test the server services. The function is disabled by default.
Silent Deny	Select whether IP packets are to be silently denied by NAT. If this function is deactivated, the sender of the denied IP packet is informed by means of an appropriate ICMP or TCP RST message. The function is disabled by default.
PPTP Passthrough	Select whether the setup and operation of several simultaneous, outgoing PPTP connections from hosts in the network are also to be permitted if NAT is activated. The function is disabled by default. If **PPTP Passthrough** is enabled, the device itself cannot be configured as a tunnel endpoint.
Portforwardings	Shows the number of portforwarding rules configured in **Networking**->**NAT**->**NAT Configuration**.

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.

The **Networking**->**NAT**->**NAT Configuration**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the NAT configuration.
Interface	Select the interface for which NAT is to be configured. Possible values: • *Any* (default value): NAT is configured for all interfaces. • *<Interface name>*: Select one of the interfaces from the list.
Type of traffic	Select the type of data traffic for which NAT is to be configured. Possible values: • *incoming (Destination NAT)* (default value): The data traffic that comes from outside. • *outgoing (Source NAT)*: Outgoing data traffic. • *excluding (Without NAT)*: Data traffic excluded from NAT.
NAT method	Only for **Type of traffic** = *outgoing (Source NAT)* 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.

Field	Description
	Possible values: • *full-cone* (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. • *restricted-cone* (UDP only): Like full-cone NAT; as external host, however, only the initial "external" destination host is allowed. • *port-restricted-cone* (UDP only): Like restricted-cone NAT; however, exclusively data from the initial destination port are allowed. • *symmetric* (standard value) any protocol: Outbound, an externally valid source address and an externally valid source port are administratively set. Inbound, only response packets within the existing connection are allowed.

In the **NAT Configuration**->**Specify original traffic** menu, you can configure for which data traffic NAT is to be used.

Fields in the menu Specify original traffic

Field	Description
Service	Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. Select one of the preconfigured services. Possible values: • *User-defined* (default value) • *<service name>*
Action	Only for **Type of traffic** = *excluding (Without NAT)* Select which data packets are to be excluded by NAT. Possible values: • *Exclude* (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/netmask, etc.) are excluded by NAT.

Field	Description
	• *Do not exclude*: All the data packets that do not match the following parameters that are to be configured (protocol, source IP address/network mask, destination IP address/net-mask, etc.) are excluded by NAT.
Protocol	Only for certain services. Not for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *full-cone*, *restricted-cone* or *port-restricted-cone*. In this case UDP is automatically defined. Select a protocol. According to the selected **Service**, different protocols are available. Possible values: • *Any* (default value) • *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP* • *ISO-IP* • *Kryptolan* • *L2TP* • *OSPF* • *PUP*

Field	Description
	• *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP* • *VRRP* • *XNS-IDP*
Source IP Address/ Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* or *excluding (Without NAT)* Enter the source IP address and corresponding netmask of the original data packets, as the case arises.
Original Destination IP Address/Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.
Original Destination Port/Range	Only for **Type of traffic** = *incoming (Destination NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Enter the destination port or the destination port range of the original data packets. The default setting *-All-* means that the port is not specified.
Original Source IP Address/Netmask	Only for **Type of traffic** = *outgoing (Source NAT)* Enter the source IP address and corresponding netmask of the original data packets, as the case arises.
Original Source Port/ Range	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Enter the source port of the original data packets. The default setting *-All-* means that the port remains unspecified. If you select *Specify port* you can specify a single port, if you select *Specify port range* you can specify a continu-

Field	Description
	ous range of ports which will be a applied for filtering the outgoing data traffic
Source Port/Range	Only for **Type of traffic** = *excluding (Without NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Enter the source port or the source port range of the original data packets. The default setting *-All-* means that the port remains unspecified.
Destination IP Address/Netmask	Only for **Type of traffic** = *excluding (Without NAT)* or *outgoing (Source NAT)* and **NAT method** = *symmetric* Enter the destination IP address and corresponding netmask of the original data packets, as the case arises.
Destination Port/Range	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* or **Type of traffic** = *excluding (Without NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Enter the destination port or the destination port range of the original data packets. The default setting *-All-* means that the port remains unspecified.

In the **NAT Configuration**->**Replacement Values** menu you can define, depending on whether you're dealing with inbound or outbound data traffic, new addresses and ports, to which specific addresses and ports from the **NAT Configuration**->**Specify original traffic** menu can be translated.

Fields in the menu Replacement Values

Field	Description
New Destination IP Address/Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* Enter the destination IP address and corresponding netmask to which the original destination IP address is to be translated.
New Destination Port	Only for **Type of traffic** = *incoming (Destination NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Leave the destination port as it appears or enter the destination

Field	Description
	port to which the original destination port is to be translated. Select *Original* to leave the original destination port. If you disable *Original*, an input field appears and you can enter a new destination port. *Original*is active by default.
New Source IP Address/Netmask	Only for **Type of traffic** = *outgoing (Source NAT)* and **NAT method** = *symmetric* Enter the source IP address to which the original source IP address is to be translated, with corresponding netmask, as the case arises.
New Source Port	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric*, **Service** = *user-defined*, **Protocol** = *TCP*, *UDP*, *TCP/UDP* and **Original Source Port/Range**= *-All-* or *Specify port* Leave the source port as it appears or enter a new source port to which the original source port is to be translated. *Original* leaves the original source port. If you disable *Original*, an input field appears in which you can enter a new source port. *Original*is active by default. If you select *Specify port range* for **Original Source Port/Range**, you can choose from the following options: • *Use Original Source Port/Range*: The range specified for **Original Source Port/Range** is not changed, all port numbers are retained. • *Use Source Port/Range starting with*: There is an input field for you to specify the port number with which to start the port range that replaces the original port rannge. The count of ports is retained.

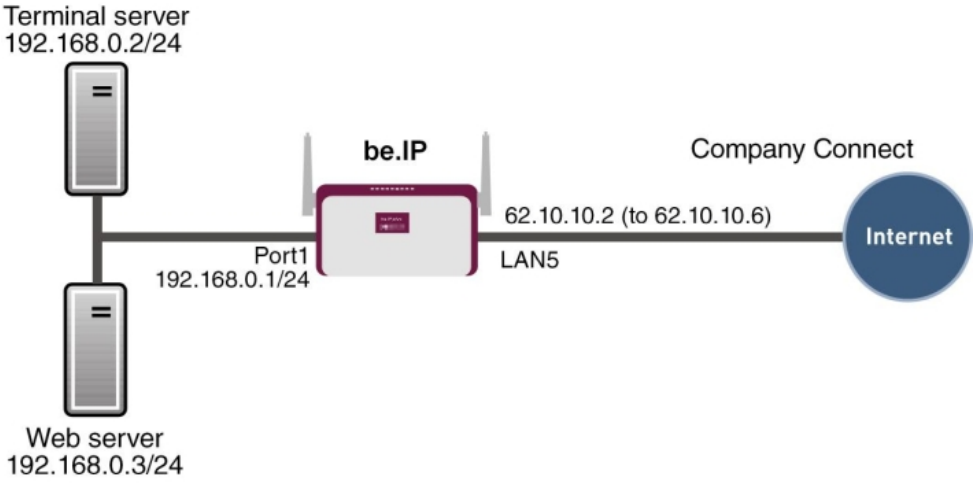
10.3.3 NAT - Configuration example

Requirements

- Basic configuration of the gateway

- A working Internet access. For example, **Company Connect** with 8 IP addresses.
- The Ethernet interface **LAN5** 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 **LAN5**.

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 *LAN_EN5-0*
Silent Deny	**Network->NAT->NAT Interfaces**	Enabled for *LAN_EN5-0*

NAT enable for the GUI

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e.g. *GUI*

Field	Menu	Value
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*
Source IP Address/ Netmask	**Network->NAT->NAT Configuration->New**	*Any*
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**	*Specify port*, *80*
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *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*
Source IP Address/ Netmask	**Network->NAT->NAT Configuration->New**	*Any*
Original Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *62.10.10.3*
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *192.168.0.3*
New Destination Port	**Network->NAT->NAT**	*Original*

Field	Menu	Value
	->**New**	

Terminal Server

Field	Menu	Value
Description	**Network->NAT->NAT Configuration->New**	e.g. *Terminal-Server*
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*
Source IP Address/ Netmask	**Network->NAT->NAT Configuration->New**	*Any*
Original Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *62.10.10.4*
Original Destination Port/Range	**Network->NAT->NAT Configuration->New**	*Specify port*, *3389*
New Destination IP Address/Netmask	**Network->NAT->NAT Configuration->New**	*Host*, e.g. *192.168.0.2*
New Destination Port	**Network->NAT->NAT Configuration->New**	*Original*

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.

Specific instructions for configuring load balancing, see *Load balancing - Configuration example* on page 209.

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.

The menu **Networking**->**Load Balancing**->**Load Balancing Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Group Description	Enter the desired description of the interface group.
Distribution Policy	Select the way the data traffic is to be distributed to the interfaces configured for the group. Possible values: • *Session-Round-Robin* (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.

Field	Description
	• *Load-dependent Bandwidth*: A newly added session is assigned to one of the group interfaces according to the share of the total data rate handled by the interfaces. The current data rate based on the data traffic is decisive in both the send and receive direction.
Consider	Only for **Distribution Policy** = *Load-dependent Bandwidth* Choose the direction in which the current data rate is to be considered. Options: • *Download*: Only the data rate in the receive direction is considered. • *Upload*: Only the data rate in the send direction is considered. By default, the *Download* and *Upload* options are disabled.
Distribution Mode	Select the state the interfaces in the group may have if they are to be included in load balancing. Possible values: • *Always* (default value): Also includes idle interfaces. • *Only use active interfaces*: Only interfaces in the up state are included.

In the **Interface** area, you add interfaces that match the current group context and configure these. You can also delete interfaces.

Use **Add** to create more entries.

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	Enter the percentage of the data traffic to be assigned to an interface. The meaning differs according to the **Distribution Ratio** employed: • For *Session-Round-Robin* is based on the number of distributed sessions. • For *Load-dependent Bandwidth*, the data rate is the decisive factor.

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

Fields in the Advanced Settings menu.

Field	Description
Route Selector	The **Route Selector** parameter is an additional criterion to help define a load balancing group more precisely. Here, routing information is added to the "interface" entry within a load balancing group. The route selector is required in certain scenarios to enable the IP sessions managed by the router to be balanced uniquely for each load balancing group. The following rules apply when using the parameter: • If an interface is only assigned to one load balancing group, it is not necessary to configure the route selector. • If an interface is assigned to multiple load balancing groups, configuration of the route selector is essential. • The route selector must be configured identically for all interface entries within a load balancing group. Select the **Destination IP Address** of the desired route. You can choose between all routes and all extended routes.
Tracking IP Address	You can use the **Tracking IP Address** parameter to have a particular route monitored.

Field	Description
	The load balancing status of the interface and the status of the routes connected to the interface can be influenced using this parameter. This means that routes can be enabled or disabled irrespective of the interface's operation status. The connection is monitored using the gateway's host surveillance function here. Host surveillance entries must be configured in order to use this function. These can be configured in the **Local Services**->**Surveillance**->**Hosts** menu. Here, it is important that only the host surveillance entries with the action **Monitor** are taken into account in the context of load balancing. Links between the load balancing function and the host surveillance function are made through the configuration of the **Tracking IP Address** in the **Load Balancing**->**Load Balancing Groups**->**Advanced Settings** menu. The interface's load balancing status now varies according to the status of the assigned host surveillance entry. Select the IP address for the route to be monitored. You can choose from the IP addresses you have entered in the **Local Services**->**Surveillance**->**Hosts**->**New** menu under **Monitored IP Address** and which are monitored with the aid of the **Action to be executed** field (**Action** = *Monitor*).

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.

The **Networking**->**Load Balancing**->**Special Session Handling**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Admin Status	Select whether the Special Session Handling should be activated. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a name for the entry.
Service	Select one of the preconfigured services, if required. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.

Field	Description
Protocol	Select a protocol, if required. The *Any* option (default value) matches any protocol.
Destination IP Address/Netmask	Enter, if required, the destination IP address and netmask of the data packets. Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host. • *Network*: Enter the network address and the related netmask.
Destination Port/Range	Enter, if required, a destination port number or a range of destination port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Source Interface	If required, select your device's source interface.
Source IP Address/Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host. • *Network*: Enter the network address and the related netmask.
Source Port/Range	Enter, if required, a source port number or a range of source port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.

Field	Description
Special Handling Timer	Enter the time period during which the specified data packets are to be routed via the route that has been defined. The default value is *900* seconds.

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

Fields in the Advanced Settings menu.

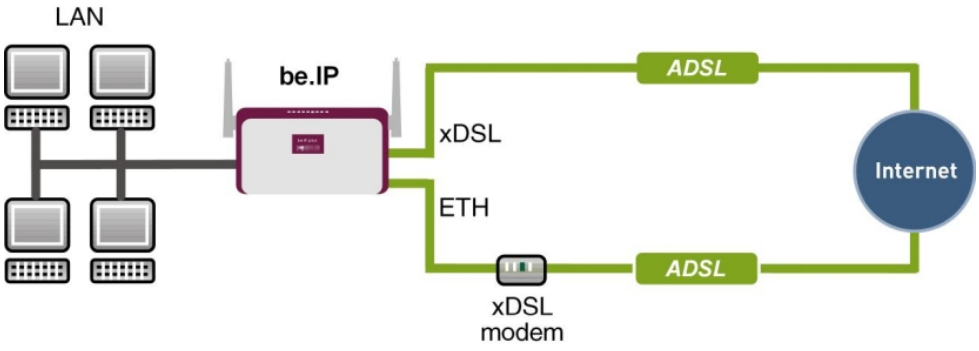
Field	Description
Frozen Parameters	Specify whether, when data packets are subsequently sent, the two parameters **Destination Address** and **Destination Port** must have the same value as the first data packet, i. e. whether the subsequent data packets must be routed via the same **Destination Port** to the same **Destination Address**. The two parameters **Destination Address** and **Destination Port** are enabled by default. If you leave the default setting *Enabled* 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. You can disable one or both parameters if you wish. The **Source IP Address** parameter must always have the same value in data packets sent subsequently as it did in the first data packet. So it cannot be disabled.

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*
Description	**Assistants->Internet Access->Internet Connections->New->Next**	e.g. *ADSL-1*
Type	**Assistants->Internet Access->Internet Connections->New->Next**	*User-defined via PPP over Ethernet (PPPoE)*
Login Name	**Assistants->Internet Access->Internet Connections->New->Next**	e.g. *feste_ip@provider.*

Field	Menu	Value
		de
Password	**Assistants->Internet Access->Internet Connections->New->Next**	e.g. *test12345*

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

Create a load balancing group

Field	Menu	Value
Group Description	**Network->Load Balancing->Load Balancing Groups->New**	e.g. *Internet Access*
Distribution Policy	**Network->Load Balancing->Load Balancing Groups->New**	*Session-Round-Robin*
Distribution Mode	**Network->Load Balancing->Load Balancing Groups->New**	*Always*
Interface	**Network->Load Balancing->Load Balancing Groups->New->Add**	*WAN_ADSL-1*
Distribution Ratio	**Network->Load Balancing->Load Balancing Groups->New->Add**	*50*
Interface	**Network->Load Balancing->Load Bal-**	*WAN_ADSL-2*

Field	Menu	Value
	ancing Groups->New->Add	
Distribution Ratio	**Network->Load Balancing->Load Balancing Groups->New->Add**	*50*

Special Session Handling

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

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.

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the filter.
Service	Select one of the preconfigured services. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.
Protocol	Select a protocol. The *Any* option (default value) matches any protocol.
Type	Only for **Protocol** = *ICMP* Select the type. Possible values: *Any*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. See RFC 792. The default value is *Any*.
Connection State	With **Protocol** = *TCP*, you can define a filter that takes the status of the TCP connections into account. Possible values: • *Established*: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter. • *Any* (default value): All TCP packets match the filter.
Destination IPv4 Address/Netmask	Enter the destination IPv4 address of the data packets and the corresponding netmask.

Field	Description
	Possible values: • *Any* (default value): The destination IP address/netmask are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the corresponding netmask.
Destination IPv6 Address/Length	Enter the destination IPv6 address of the data packets and the prefix length. Possible values: • *Any* (default value): The destination IP address/length are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the prefix length.
Destination Port/Range	Only for **Protocol** = *TCP*, *UDP* or *TCP/UDP* Enter a destination port number or a range of destination port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Source IPv4 Address/ Netmask	Enter the source IPv4 address of the data packets and the corresponding netmask. Possible values: • *Any* (default value): The source IP address/netmask are not specified. • *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the corresponding netmask.
Source IPv6 Address/ Length	Enter the source IPv6 address of the data packets and the prefix length. Possible values:

Field	Description
	• *Any* (default value): The source IP address/length are not specified. • *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the prefix length.
Source Port/Range	Only for **Protocol** = *TCP*, *UDP* or *TCP/UDP* Enter a source port number or a range of source port numbers. Possible values: • *-All-* (default value): The source port is not specified. • *Specify port*: Enter a source port. • *Specify port range*: Enter a source port range.
DSCP/TOS Filter (Layer 3)	Select the Type of Service (TOS). Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	Enter the service class of the IP packets (Class of Service, CoS). Value range *0* to *7*.

Field	Description
	The default value is *0*. The default value is *Ignore*.

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.

The **Networking**->**QoS**->**QoS Classification**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Class map	Choose the class plan you want to create or edit. Possible values: • *New* (default value): You can create a new class plan with this setting. • *<Name of class plan>*: Shows a class plan that has already been created, which you can select and edit. You can add new filters.
Description	Only for **Class map** = *New* Enter the name of the class plan.
Filter	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. To select a filter, at least one filter must be configured in the **Networking**->**QoS**->**QoS Filter** menu.

Field	Description
Direction	Select the direction of the data packets to be classified. Possible values: • *Incoming*: Incoming data packets are assigned to the class (**Class ID**) that is then to be defined. • *Outgoing* (default value): Outgoing data packets are assigned to the class (**Class ID**) that is then to be defined. • *Both*: Incoming and outgoing data packets are assigned to the class (**Class ID**) that is then to be defined.
High Priority Class	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. The function is enabled with *Enabled*. The function is disabled by default.
Class ID	Only for **High Priority Class** not active. Choose a number which assigns the data packets to a class. **Note** The class ID is a label to assign data packets to specific classes. (The class ID does not define the priority.) Possible values are whole numbers between *1* and *254*.
Set DSCP/Traffic Class Filter (Layer 3)	Here you can set or change the DSCP/TOS value of the IP data packets, based on the class (**Class ID**) that has been defined. Possible values: • *Preserve* (default value): The DSCP/TOS value of the IP data packets remains unchanged. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP

Field	Description
	packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
Set COS value (802.1p/Layer 2)	In the header of the Ethernet packets filtered by the selected filter, you can here set/change the service class (Layer 2 priority). Possible values are whole numbers between *0* and *7*. The default value is *Preserve*.
Interfaces	Only for **Class map** = *New* 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.

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.

The **Networking**->**QoS**->**QoS Interfaces/Policies**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface for which QoS is to be configured.
Prioritisation Algorithm	Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface. Possible values: • *Priority Queueing*: QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority. • *Weighted Round Robin*: 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. • *Weighted Fair Queueing*: 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. • *Disabled* (default value): QoS is deactivated on the interface. The existing configuration is not deleted, but can be activated again if required.
Traffic shaping	Activate or deactivate data rate limiting in the send direction. The function is enabled with *Enabled*. The function is disabled by default.
Maximum Upload	Only for **Traffic shaping** = enabled.

Field	Description
Speed	Enter a maximum data rate for the selected interface in the send direction in kbit per second. Possible values are *0* to *1000000*. The default value is *0*, i.e. no limits are set, the selected interface can occupy its maximum bandwidth.
Protocol Header Size below Layer 3	Only for **Traffic shaping** = enabled. Choose the interface type to include the size of the respective overheads of a datagram when calculating the bandwidth. Possible values: • *User defined*: Value in byte. Possible values are *0* to *100*. • *Undefined (Protocol Header Offset=0)* (default value) Can only be selected for Ethernet interfaces • *Ethernet* • *Ethernet and VLAN* • *PPP over Ethernet* • *PPP over Ethernet and VLAN* Can only be selected for IPSec interfaces: • *IPSec over Ethernet* • *IPSec over Ethernet and VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE and VLAN*
Encryption Method	Only if an IPSec Peers is selected as **Interface**, **Traffic shaping** is *Active* and **Protocol Header Size below Layer 3** is not *Undefiniert (Protocol Header Offset=0)*. 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. Possible values:

Field	Description
	• *DES, 3DES, Blowfish, Cast - (cipher block size = 64 Bit)* • AES128, AES192, AES256, Twofish - (cipher block size = 128 Bit)
Real Time Jitter Control	Only for **Traffic shaping** = enabled 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. Real Time Jitter Control is useful for small upload bandwidths (< 800 kbps). Activate or deactivate Real Time Jitter Control. The function is enabled with *Enabled*. The function is disabled by default.
Control Mode	Only for **Real Time Jitter Control** = enabled. Select the mode for optimising voice transmission. Possible values: • *All RTP Streams*: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected. • *Inactive*: Voice data transmission is not optimised. • *Controlled RTP Streams only*: 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. • *Always*: Real Time Jitter Control is always active, even if no real time data is routed.
Queues/Policies	Configure the desired QoS queues. 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

Field	Description
	and for data traffic classified as moving in both directions). Add new entries with **Add**. The **Edit Queue/Policy** menu opens. By creating a QoS policy a DEFAULT entry with the lowest priority 255 is automatically created.

The menu **Edit Queue/Policy** consists of the following fields:

Fields in the Edit Queue/Policy menu.

Field	Description
Description	Enter the name of the queue/policy.
Outbound Interface	Shows the interface for which the QoS queues are being configured.
Prioritisation queue	Select the queue priority type. Possible values: • *Class Based* (default value): Queue for data classified as "normal". • *High Priority*: Queue for data classified as "high priority". • *Default*: Queue for data that has not been classified or data of a class for which no queue has been configured.
Class ID	Only for **Prioritisation queue** = *Class Based* Select the QoS packet class to which this queue is to apply. To do this, at least one class ID must be given in the **Networking->QoS->QoS Classification** menu.
Priority	Only for **Prioritisation queue** = *Class Based* Choose the priority of the queue. Possible values are *1* (high priority) to *254* (low priority). The default value is *1*.
Weight	Only for **Prioritisation Algorithm** = *Weighted Round Robin* or *Weighted Fair Queueing*

Field	Description
	Choose the priority of the queue. Possible values are *1* to *254*. The default value is *1*.
RTT Mode (Realtime Traffic Mode)	Active or deactivate the real time transmission of the data. The function is enabled with *Enabled*. The function is disabled by default. RTT mode should be activated for QoS classes in which real time data has priority. This mode improves latency when forwarding real time datagrams. 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.
Traffic Shaping	Activate or deactivate data rate (=Traffic Shaping) limiting in the send direction. The data rate limit applies to the selected queue. (This is not the limit that can be defined on the interface.) The function is enabled with *Enabled*. The function is disabled by default.
Maximum Upload Speed	Only for **Traffic Shaping** = enabled. Enter a maximum data rate for the queue in kbits. Possible values are *0* to *1000000*. The default value is *0*.
Overbooking allowed	Only for **Traffic Shaping** = enabled. Enable or disable the function. The function controls the bandwidth limit. If **Overbooking allowed** is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface. If **Overbooking allowed** is deactivated, the queue can never

Field	Description
	occupy bandwidth beyond the bandwidth limit that has been set. The function is enabled with *Enabled*. The function is disabled by default.
Burst size	Only for **Traffic Shaping** = enabled. Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached. Possible values are *0* to *64000*. The default value is *0*.

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

Fields in the Advanced Settings menu.

Field	Description
Dropping Algorithm	Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded. Possible values: • *Tail Drop* (default value): The newest packet received is dropped. • *Head Drop*: The oldest packet in the queue is dropped. • *Random Drop*: A randomly selected packet is dropped from the queue.
Congestion Avoidance (RED)	Enable or disable preventative deletion of data packets. Packets which have a data size of between **Min. queue size** and **Max. queue size** are preventively dropped to prevent queue overflow (RED=Random Early Detection). This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses. The function is activated with *Enabled*. The function is disabled by default.

Field	Description
Min. queue size	Enter the lower threshold value for the process **Congestion Avoidance (RED)** in bytes. Possible values are *0* to *262143*. The default value is *0*.
Max. queue size	Enter the upper threshold value for the process **Congestion Avoidance (RED)** in bytes. Possible values are *0* to *262143*. The default value is *16384*.

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.

10.6.1.1 Edit or New

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

The **Networking**->**Access Rules**->**Access Filter**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the filter.
Service	Select one of the preconfigured services. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.
Protocol	Select a protocol. The *Any* option (default value) matches any protocol.
Type	Only if **Protocol** = *ICMP* Possible values: • *Any* • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time exceeded*

Field	Description
	• *Timestamp* • *Timestamp reply* The default value is *Any*. See RFC 792.
Connection State	Only if **Protocol** = *TCP* You can define a filter that takes the status of the TCP connections into account. Possible values: • *Any* (default value): All TCP packets match the filter. • *Established*: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.
Destination IPv4 Address/Netmask	Enter the destination IPv4 address of the data packets and the corresponding netmask. Possible values: • *Any* (default value): The destination IP address/netmask are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the corresponding netmask.
Destination IPv6 Address/Length	Enter the destination IPv6 address of the data packets and the prefix length. Possible values: • *Any* (default value): The destination IP address/length are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the prefix length.
Destination Port/Range	Only if **Protocol** = *TCP*, *UDP* Enter a destination port number or a range of destination port numbers that matches the filter.

Field	Description
	Possible values: • *-All-* (default value): The filter is valid for all port numbers • *Specify port*: Enables the entry of a port number. • *Specify port range*: Enables the entry of a range of port numbers.
Source IPv4 Address/ Netmask	Enter the source IPv4 address of the data packets and the corresponding netmask. Possible values: • *Any* (default value): The source IP address/netmask are not specified. • *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the corresponding netmask.
Source IPv6 Address/ Length	Enter the source IPv6 address of the data packets and the prefix length. Possible values: • *Any* (default value): The source IP address/length are not specified. • *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the prefix length.
Source Port/Range	Only if **Protocol** = *TCP*, *UDP* Enter a source port number or the range of source port numbers. Possible values: • *-All-* (default value): The filter is valid for all port numbers • *Specify port*: Enables the entry of a port number. • *Specify port range*: Enables the entry of a range of port numbers.
DSCP/TOS Filter (Layer 3)	Select the Type of Service (TOS). Possible values:

Field	Description
	• *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	Enter the service class of the IP packets (Class of Service, CoS). Possible values are whole numbers between *0* and *7*. The default value is *Ignore*.

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.

10.6.2.1 Edit or New

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

The **Networking**->**Access Rules**->**Rule Chains**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Rule Chain	Select whether to create a new rule chain or to edit an existing one. Possible values: • *New* (default value): You can create a new rule chain with this setting. • *<Name of the rule chain>*: Select an already existing rule chain, and thus add another rule to it.
Description	Enter the name of the rule chain.
Access Filter	Select an IP filter. If the rule chain is new, select the filter to be set at the first point of the rule chain. If the rule chain already exists, select the filter to be attached to the rule chain.
Action	Define the action to be taken for a filtered data packet. Possible values: • *Allow if filter matches* (default value): Allow packet if it matches the filter. • *Allow if filter does not match*: Allow packet if it does not match the filter. • *Deny if filter matches*: Deny packet if it matches the filter. • *Deny if filter does not match*: Deny packet if it does not match the filter. • *Ignore*: Use next rule.

To set the rules of a rule chain in a different order select the ↑↓ button in the list menu for the entry to be shifted. A dialog box opens, in which you can decide under **Move** whether the entry *below* (default value) or *above* another rule of this rule chain is to be shifted.

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.

10.6.3.1 Edit or New

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

The **Networking**->**Access Rules**->**Interface Assignment**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.
Silent Deny	Define whether the sender is to be informed if an IP packet is denied. • *Enabled* (default value): The sender is not informed. • *Disabled*: The sender receives an ICMP message.
Reporting Method	Define whether a syslog message is to be generated if a packet is denied. Possible values: • *No report*: No syslog message. • *Info* (default value): A syslog message is generated with the protocol number, source IP address and source port number. • *Dump*: A syslog message is generated with the contents of the first 64 bytes of the denied packet.

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**.

The **Networking**->**Drop In**->**Drop In Groups**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Group Description	Enter a unique name for the **Drop In** group.
Mode	Select which mode is to be used to send the MAC addresses of network components. Possible values: • *Transparent* (default value): ARP packets and IP packets belonging to the drop-in network are routed transparently (unchanged). • *Proxy*: ARP packets and IP packets related to the drop-in network are forwarded with the MAC address of the corresponding interface.
Exclude from NAT (DMZ)	Here you can take data traffic from NAT. Use this function to, for example, ensure that certain web servers in a DMZ can be accessed. The function is enabled with *Enabled*. The function is disabled by default.
Network Configuration	Select how an IP address / netmask is assigned to the **Drop In** network. Possible values:

Field	Description
	• *Static* (default value) • *DHCP*
Network Address	Only for **Network Configuration** = *Static* Enter the network address of the **Drop In** network.
Netmask	Only for **Network Configuration** = *Static* Enter the corresponding netmask.
Local IP Address	Only for **Network Configuration** = *Static* Enter the local IP address. This IP address must be identical for all the Ethernet ports in a network.
DHCP Client on Interface	Only for **Network Configuration** = *DHCP* Here you can select an Ethernet interface on your router which is to act as the DHCP client. You need this setting, for example, if your provider's router is being used as the DHCP server. You can choose from the interfaces available to your device; however the interface must be a member of the drop-in group.
ARP Lifetime	Determines the time period for which the ARP entries will be held in the cache. The default value is *3600* seconds.
DNS assignment via DHCP	The gateway can modify DHCP packets which pass through the drop-in group and identify itself as an available DNS server. Possible values: • *Unchanged* (default value) • *Own IP Address*
Interface Selection	Select all the ports which are to be included in the **Drop In** group (in the network). Add new entries with **Add**.

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.

11.1.1.1 Edit

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

The menu **Networking**->**RIP**->**RIP Interfaces**-> consists of the following fields:

Fields in the RIP Parameters for menu.

Field	Description
Send Version	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. Possible values:

Field	Description
	• *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*:Enables sending and receiving RIP packets of both version 1 and 2. • *RIP V2 Multicast*: For sending RIP V2 messages over multicast address 224.0.0.9. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Receive Version	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. Possible values: • *None* (default value): RIP is not enabled. • *RIP V1*: Enables sending and receiving of version 1 RIP packets. • *RIP V2*: Enables sending and receiving of version 2 RIP packets. • *RIP V1/V2*:Enables sending and receiving RIP packets of both version 1 and 2. • *RIP V1 Triggered*: RIP V1 messages are sent, received and processed as per RFC 2091 (triggered RIP). • *RIP V2 Triggered*: RIP V2 messages are sent, received and processed as per RFC 2091 (triggered RIP).
Route Announce	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. Note: This setting does not affect the interface-specific RIP configuration mentioned above. Possible values:

Field	Description
	• *Up or Dormant* (not for LAN interfaces, interfaces in Bridge mode and interfaces for leased lines): Routes are propagated if the interface status is up or ready. • *Up only* (default value): Routes are only propagated if the interface status is up. • *Always*: Routes are always propagated independently of operational status.

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 position.

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.

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.

The menu **Routing Protocols**->**RIP**->**RIP Filter**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Interface	Select the interface to which the rule to be configured applies.
IP Address / Netmask	Enter the IP address and netmask to which the rule is to be applied. This address can be in the LAN or WAN. The rules for incoming and outgoing RIP packets (import or export) for the same IP address must be separately configured. You can enter individual host addresses or network addresses.
Direction	Select whether the filter applies to the export or import of routes. Possible values: • *Import* (default value) • *Export*
Metric Offset for Active Interfaces	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". Possible values are *-16* to *16*. The default value is *0*.
Metric Offset for Inactive Interfaces	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". Possible values are *-16* to *16*. The default value is *0*.

11.1.3 RIP Options

The menu **Routing Protocols**->**RIP**->**RIP Options** consists of the following fields:

Fields in the Global RIP Parameters menu.

Field	Description
RIP UDP Port	The setting option UDP Port, which is used for sending and receiving RIP updates, is only for test purposes. If the setting is changed, this can mean that your device sends and listens at a

Field	Description
	port that no other devices use. The default value *520* should be retained.
Default Route Distribution	Select whether the default route of your device is to be propagated via RIP updates. The function is enabled with *Enabled*. The function is enabled by default.
Poisoned Reverse	Select the procedure for preventing routing loops. With standard RIP, the routes learnt are propagated over all interfaces with RIP SEND activated. With **Poisoned Reverse**, however, your device propagates over the interface via which it learnt the routes, with the metric (Next Hop Count) 16 (=“Network is not reachable“). The function is enabled with *Enabled*. The function is disabled by default.
RFC 2453 Variable Timer	For the timers described in RFC 2453, select whether the same values that you can configure in the **Timer for RIP V2 (RFC 2453)** menu should be used. The function is enabled with *Enabled*. The function is enabled by default. If you deactivate the function, the times defined in RFC are retained for the timeouts.
RFC 2091 Variable Timer	For the timers described in RFC 2091, select whether the same values that you can configure in the **Timer for Triggered RIP (RFC 2091)** menu should be used. The function is enabled with *Enabled*. The function is disabled by default. If the function is not activated, the times defined in RFC are retained for the timeouts.

Fields in the Timer for RIP V2 (RFC 2453) menu.

Field	Description
Update Timer	Only for **RFC 2453 Variable Timer** = *Enabled* An RIP update is sent on expiry of this period of time. The default value is *30* (seconds).
Route Timeout	Only for **RFC 2453 Variable Timer** = *Enabled* After the last update of a route, the route time is active. After timeout, the route is deactivated and the Garbage Collection Timer is started. The default value is *180* (seconds).
Garbage Collection Timer	Only for **RFC 2453 Variable Timer** = *Enabled* The Garbage Collection Timer is started as soon as the route timeout has expired. After this timeout, the invalid route is deleted from the IPROUTETABLE if no update is carried out for the route. The default value is *120* (seconds).

Fields in the Timer for Triggered RIP (RFC 2091) menu.

Field	Description
Hold Down Timer	Only for **RFC 2091 Variable Timer** = *Enabled* The hold down timer is activated as soon as your device receives an unreachable route (metric 16). The route may deleted once this period has elapsed. The default value is 120 (seconds).
Retransmission Timer	Only for **RFC 2091 Variable Timer** = *Enabled* After this timeout, update request or update response packets are sent again until an update flush or update acknowledge packet arrives. The default value is 5 (seconds).

11.2 OSPF

OSPF (Open Shortest Path First) is a dynamic routing protocol that is frequently used in larger networks as an alternative to RIP. It was originally developed to avoid a number of limitations of RIP (when used in larger networks).

The problems (with RIP) avoided by OSPF include:

- Reduced network load: After a short initialization phase, routing information is not sent periodically as with RIP, but only changed routing information.
- Authentication: Gateway authentication can be configured to increase the security when exchanging routing information.
- Routing Traffic Control: Gateways can be combined to form areas to limit the traffic created by exchanging routing information.
- Connection costs: OSPF differs from RIP in that the connection costs are not calculated from the number of next hops, but from the bandwidth of the respective transport medium.
- No limitation of the number of hops: The limitation of the maximum number of 16 hops for RIP does not exist for OSPF.

Although the OSPF protocol is considerably more complex than RIP, the basic concept is the same, i.e. OSPF also determines the best path for forwarding the packets in each case.

OSPF is an Interior Gateway Protocol that is used to distribute routing information within an autonomous system (AS). The Link State Updates are exchanged between the gateways by flooding. Each change of routing information is passed to all gateways in the network. OSPF areas are defined to limit the number of Link State Updates. All gateways of an area have an identical Link State database.

An area is interface-specific. Gateways whose interfaces belong to several areas and connect these to the backbone are called Area Border Routers (ABR). ABRs therefore contain the information of the backbone area and all areas connected. A gateway whose interfaces are all incorporated in one area are called Internal Routers (IR).

There are four types of Link State packets: Router links show the state of the interfaces of a gateway that belong to a certain area. Summary links are generated by the ABR to define how the information on reachability in the network is exchanged between areas. Usually all information is sent to the backbone area, which then passes the information to the other areas. Network links are sent by Designated Routers (DS) within a segment and propagate all gateways that are connected to a certain multi-access segment like Ethernet, Token Ring and FDDI (also NBMA). External links point to networks outside the AS. These networks are incorporated in OSPF using redistribution. In this case, an Autonomous System Border Router (ASBR) incorporates these external routes in the AS.

It is possible to increase security by authenticating the OSPF packets, so that the gateways can participate in Routing Domains using predefined passwords.

It is recommended that several areas are defined in larger networks. If more than one area is configured, one of these areas must possess the area ID 0.0.0.0, which defines the backbone area. This must be the centre point of all areas, i.e. all areas must be physically connected to the backbone area. Occasionally, gateways cannot be physically connected directly to the backbone area and virtual links must be set up.

The purpose of virtual links is to connect areas in which no physical connection to the backbone is possible and to maintain the connection of the backbone in case of a failure of the 0.0.0.0 area.

Summarizing is the term given to the consolidation of the various routes into a single advertisement (summary link). This is usually done by the ABR at the area borders.

Certain areas can be defined as stub areas in OSPF. This prevents external networks, e.g. those propagated from other protocols by redistribution in OSPF, being propagated into the stub area. Externally routing of such areas is propagated with a default route. The configuration of a stub area reduces the database size in the area and reduces the amount of storage space needed on the gateways incorporated in the area.

11.2.1 Areas

OSPF areas must be defined before the gateway interface can be assigned to an area.

A list of all configured OSPF areas is displayed in the **Routing Protocols**->**OSPF**->**Areas** menu.

11.2.1.1 Edit or New

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

The **Routing Protocols**->**OSPF**->**Areas**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Area ID	Enter the ID to identify the OSPF aea. The backbone area is `0.0.0.0`.
Import external routes	Specifies whether the gateway routing information generated from external autonomous systems (not areas) is to be imported.

Field	Description
	The function is enabled with *Enabled*. The function is activated by default.
Import summary routes	Only for **Import external routes** = *Disabled* Define whether summary LSAs (routing information generated by Area Border Gateway) are to be sent to the stub area. Possible values: • *Enabled* (default value): Activates import. • *Disabled*: Deactivates the import.
Create area default route (only ABR)	Only for **Import external routes** = *Disabled* Select whether the Area Border Gateway shall send no LSA's in the stub area, but rather only propagate a default route. The function is enabled with *Enabled*. The function is not activated by default.

Fields in the Route Aggregation menu.

Field	Description
IP Address	Define the OSPF area. • *IP Address*: Here you enter the IP address of the area to be combined. • *Netmask*: Enter the netmask here. • *Advertise*: Subnetworks that are combined into areas either initiate propagation of the given combination (*Yes*, default value), or cause the subnetwork not to be propagated outside the area at all (*No*), i.e. neither the actual subnetworks nor the combined overall subnetwork are propagated. Add new entries with **Add**.

11.2.2 Interfaces

In the **Routing Protocols**->**OSPF**->**Interfaces** menu, a list of all interfaces is displayed.

Caution

If your interfaces are not only to be assigned to Backbone Area 0.0.0.0, you must first define OSPF areas in the **Routing Protocols**->**OSPF**->**Areas** menu.

11.2.2.1 Edit

Select the ✎ symbol to modify the OSPF settings fot the interfaces.

The **Routing Protocols**->**OSPF**->**Interfaces**-> ✎ menu consists of the following fields:

Fields in the OSPF Interface Configuration menu.

Field	Description
Admin Status	The status of an OSPF interface defines whether routes are propagated and/or OSPF protocol packets are sent over the interface. If OSPF is not yet activated, only the Admin Status field is shown (in this case changes are irrelevant). Possible values: • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Passive*: 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. • *Inactive*: OSPF is completely disabled for this interface.
Area ID	Select the ID of the area to which this interface shall be assigned. If your interface is not only to be assigned to Backbone Area 0.0.0.0, you must first define OSPF areas in the **Routing Protocols**->**OSPF**->**Areas** menu.
Metric Determination	Defines how the metric of this interface is calculated. Possible values: • *Auto (Interface Speed)* (default value): The metric is automatically set on the basis of the interface speed.

Field	Description
	• *Fixed*: Enter a specific value in **Metric (direct routes)**.
Metric (direct routes)	Enter the base metric value. The basis of the metric actually used for a route is a base metric value, which is obtained from the bandwidth of the interface: BMV = 100,000,000 / bandwidth in bps For **Metric Determination** *Auto (Interface Speed)* the automatically calculated value is displayed here and cannot be modified. The basic metric value for bandwidths >= 100.000.000 bps is always *1*. So the basic metric value of Gigabit interfaces and 100 Mbit interfaces is identical. To change this, you need to specify a fixed value in **Metric Determination**.
Authentication Type	Select the type of authentication used if OSPF packets are sent over this OSPF interface (or incoming packets checked). Defines how the key in the **Authentication Key** field is used. The default value is *none*. In *Clear Text*, the key is sent as a text string in each packet. In *MD5*, the key is used to create a hash, which is sent with each packet
Authentication Key	Enter a text string to be used in combination with the defined **Authentication Type**.
Export indirect static routes	If this value is set to *No* (default), only direct routes (i.e. routes to networks reached directly over this interface) are propagated over active OSPF interfaces (see **Admin Status**). If the value is set to *Yes*, indirect static routes are also propagated over active interfaces.
Demand Circuit Options	Define whether Demand OSPF procedures (Hello suppression on FULL Neighbors and setting of DoNotAge flags on the propagated LSA) shall be performed (Yes, default value) or not (*No*). This option should be enabled particularly in the case of connections for which the costs are calculated based on time (e. g. ISDN dialup connections, Internet connections with no flat rate).

11.2.3 Global Settings

The **Routing Protocols**->**OSPF**->**Global Settings** menu contains global OSPF parameters. OSPF is activated on the gateway.

The menu consists of the following fields:

Fields in the Global OSPF Settings menu.

Field	Description
OSPF Status	Enable or disable OSPF. The function is disabled by default.
Generate default route for the AS	If this option is activated, the gateway propagates a default route over all active OSPF interfaces. The function is disabled by default.
Propagate routes bound on discard/refuse interface	The logical interfaces REFUSE and IGNORE have the following meaning: REFUSE means (if a route exists on this) that packets from this interface are discarded and an ICMP Unreachable Reply is generated. IGNORE means (if a route exists on this) that packets from this interface are discarded without comment. If the option is activated, routes connected to the two discard/refuse interfaces are saved by OSPF in its database. If the option is deactivated, these routes are ignored. The function is disabled by default.
Dynamic LS Update Compression	Only for **RXL1250** / **RXL12100** Enable or disable the function. The function is disabled by default.

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.

The menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Multicast Routing	Select whether **Multicast Routing** should be used. The function is enabled with *Enabled*. The function is disabled by default.

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.

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

Fields in the IGMP Settings menu.

Field	Description
Interface	Select the interface on which IGMP is to be enabled, i.e. queries are sent and responses are accepted.
Query Interval	Enter the interval in seconds in which IGMP queries are to be sent. Possible values are *0* to *600*. The default value is *125*.
Maximum Response Time	For the sending of queries, enter the time interval in seconds 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. Possible values are *0,0* to *25,0*. The default value is *10,0*.
Robustness	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). Possible values are *2* to *8*. The default value is *2*.
Last Member Query Interval	Define the time after a query for which the router waits for an answer. 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. Possible values are *0,0* to *25,0*. The default value is *1,0*.

Field	Description
IGMP State Limit	Limit the number of reports/queries per second for the selected interface.
Mode	Specify whether the interface defined here only works in host mode or in both host mode and routing mode. Possible values: • `Routing` (default value): The interface is operated in Routing mode. • `Host`: The interface is only operated in host mode.

IGMP Proxy

IGMP Proxy enables you to simulate several locally connected interfaces as a subnet to an adjacent router. Queries coming in to the IGMP Proxy interface are forwarded to the local subnets. Local reports are forwarded on the IPGM Proxy interface.

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

Fields in the Advanced Settings menu.

Field	Description
IGMP Proxy	Select whether your device is to forward the hosts' IGMP messages in the subnet via its defined **Proxy Interface**.
Proxy Interface	Only for **IGMP Proxy** = enabled Select the interface on your device via which queries are to be received and collected.
Fallback Proxy Interface 1	Only for **IGMP Proxy** = enabled Select the fallback interface 1 on your device via which queries are to be received and collected. This interface will be used if the proxy function cannot be carried out on the **Proxy Interface**.
Fallback Proxy Interface 2	Only for **IGMP Proxy** = enabled Select the fallback interface 2 on your device via which queries are to be received and collected. This interface will be used if the proxy function cannot be carried out on the **Fallback Proxy Interface 1**.

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.

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

Fields in the Basic Settings menu.

Field	Description
IGMP Status	Select the IGMP status. Possible values: • *Auto* (default value): Multicast is activated automatically for hosts if the hosts open applications that use multicast. • *Up*: Multicast is always on. • *Down*: Multicast is always off.
Mode	Only for **IGMP Status** = *Up* or *Auto* Select Multicast Mode. Possible values: • *Compatibility Mode* (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. • *Version 3 only*: Only IGMP version 3 is used.
Maximum Groups	Enter the maximum number of groups to be permitted, both internally and in reports. The default value is *64*.
Maximum Sources	Enter the maximum number of sources that are specified in version 3 reports and the maximum number of internally managed sources per group. The default value is *64*.
IGMP State Limit	Enter the maximum permitted total number of incoming queries and messages per second.

Field	Description
	The default value is `0`, i.e. the number of IGMP status messages is not limited.

The section **Advanced Settings** allows you to switch IGMP Snooping on or off. IGMP Snooping ensures that multicast traffic is sent only to those clients that have actually required a specific multicast stream.

The function is enabled by default.

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.

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

Fields in the Basic Parameters menu.

Field	Description
All Multicast Groups	Select whether all multicast groups, i.e. the complete multicast address range 224.0.0.0/4, are to be forwarded from the defined **Source Interface** to the defined **Destination Interface**. To do this, check `Enabled` Disable the option if you only want to forward one defined multicast group to a particular interface. The option is deactivated by default.
Multicast Group Address	Only for **All Multicast Groups** = not active. Enter here the address of the multicast group you want to forward from a defined **Source Interface** to a defined **Destination Interface**.
Source Interface	Select the interface on your device to which the selected multic-

Field	Description
	ast group is sent.
Destination Interface	Select the interface on your device to which the selected multicast group is to be forwarded.

12.4 PIM

Protocol Independent Multicast (PIM) is a multicast-routing process that makes possible dynamic routing from multicast packets. With PIM the distribution of information is regulated via a central point, which is known as the rendezvous point. Data packets are initially routed here before being made available to other recipient routers.

Multicast routing protocols differentiates between sparse mode and dense mode. In dense mode, all packets are forwarded and only packets to groups that have been explicitly cancelled are rejected. In sparse mode, packets are only forward to groups if they have been ordered. Your device uses PIM in sparse mode.

12.4.1 PIM Interfaces

A list of all PIM interfaces is displayed in the **Multicast**->**PIM**->**PIM Interfaces** menu.

12.4.1.1 Edit or New

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

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

Fields in the PIM Interface Settings menu.

Field	Description
Interface	Choose the interface used for PIM, i.e. over which multicast routing is operated.
PIM Mode	Indicates the mode to be used for PIM. Your device uses PIM in sparse mode. The entry cannot be changed.
Use as Stub interface	Determine whether or not the interface is used for PIM data packets. This parameter allows you to use an interface for IGMP, for example, whilst preventing (fake) PIM messages. If this function is deactivated (default value), the PIM data packets for this interface are blocked.

Field	Description
	If the function is active, the interface for the PIM data packets are released.
Designated Router Priority	Define the value of the designated router priority entered in the **Designated Router Priority** option. The higher the value, the greater the probability that the corresponding router will be used as the designated router. The default value is `1`.

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

Fields in the Advanced Settings menu.

Field	Description
Hello Interval	Define the interval (in seconds) at which PIM Hello messages are sent over this interface. The value `0` means that no PIM Hello messages are sent on this interface. Possible values: `0` to `18000` seconds. The default value is `30`.
Triggered Hello Interval	Define the maximum waiting time until a PIM Hello message is sent after a system boot or after a reboot of a neighbour. The value `0` means that PIM Hello messages are always sent straight away. Possible values: `0` to `60` seconds. The default value is `5`.
Hello Hold Time	Define the value of the holdtime field in a PIM Hello message. This indicates how long a PIM route is available. As soon as the **Hello Hold Time** has expired and no other Hello messages have been received, the PIM router will be classed as unavailable. Possible values: `0` to `65535` seconds.

Field	Description
	The default value is *105*.
Join/Prune Interval	Define the frequency at which the PIM Join/Prune messages are sent on the interface. The value *0* means that no periodic PIM Join/Prune messages are sent on this interface. Possible values: *0* to *18000* seconds. The default value is *60*.
Join/Prune Hold Time	Define the value entered in the holdtime field of a PIM Join/Prune message. This is the time for which a recipient must maintain the Join/Prune state. Possible values: *0* to *65535* seconds. The default value is *210*.
Propagation Delay	Define the value entered in the Propagation Delay field. This field is part of the LAN Prune Delay option in the PIM Hello messages, which are sent on this interface. Propagation Delay and Override Interval represent the so-called LAN-Prune-Delay settings. These result in a delay in processing prune messages for upstream routers. If the **Propagation Delay** is too short, the transfer of multicast packets may be cancelled before a downstream router has sent a prune override message. Possible values: *0* to *32* seconds. The default value is *1*.
Override Interval	Define the value that the gateway enters in the Override_Interval field for the LAN Prune Delay option. **Override Interval** defines the maximum time a downstream router can wait until sending a prune override message. Possible values: *0* to *65* seconds.

Field	Description
	The default value is `3`.

12.4.2 PIM Rendezvous Points

In menu **Multicast**->**PIM**->**PIM Rendezvous Points** you determine which Rendezvous Point is responsible for which group.

A list of all PIM Rendezvous Points is displayed.

12.4.2.1 Edit or New

Choose the icon to edit existing entries. To configure PIM Rendezvous Points, select the **New** button.

The **Multicast**->**PIM**->**PIM Rendezvous Points**->**New** menu consists of the following fields:

Fields in the PIM Rendezvous Point Settings menu.

Field	Description
Multicast Group Range	Select the Multicast group for the PIM Rendezvouz point. You can enter `All Groups` (default value), or specify a multicast network segment by selecting `Specific Range`.
Multicast Group Address	Only if **Multicast Group Range** = `Specific Range` Here you enter the IP address of the multicast network segment.
Multicast Group Prefix Length	Only if **Multicast Group Range** = `Specific Range` Here you enter the network mask length of the multicast network segment. 224.0.0.0/4 indicates the entire multicast class D segment. Possible values: `4` (default value) to `32`.
Rendezvous Point IP Address	Enter the IP address or the hostname of the rendezvous points.
Precedence	Enter the value for pimGroupMappingPrecedence to be used for static RP configurations. This allows precise control over which configuration is to be replaced by this static configuration.

Field	Description
	When the function is activated pimStaticRPOverrideDynamic is ignored. The absolute values of this object are only significant on the local router and need not be synchronised with other routers. The function is deactivated with the default value `0`. If the function is not activated by setting a value not 0, this can different consequences for other routers. Hence, avoid using this function if exact control of the behaviour of the static RP is not required.

12.4.3 PIM Options

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

Fields in the Basic Settings menu.

Field	Description
PIM Status	Select whether PIM should be activated. The function is activated by selecting `Enable`. The function is disabled by default.
Keepalive Period	Enter the interval in seconds within which a KeepAlive message must be sent. Possible values: `0` to `65535`. The default value is `210`.
Register Suppression Timer	Enter the time in seconds after which a PIM Designated Router (DR) should no longer send any register-encapsulated data to the Rendezvouz Point (RP) once the Register-Stop-Message has been received. This object is used to employ timers at the DR as well as at the RP. This timespan is named Register_Suppression_Time in the PIM-SM specification. Possible values: `0` to `65535`. The default value is `60`.

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.

In addition, you can create address pools for the dynamic assignment of IP addresses.

To enable your device to set up connections to networks or hosts outside your LAN, you must configure the partners you want to connect to on your device. This applies to outgoing connections (your device dials its WAN partner) and incoming connections (a remote partner dials the number of your device).

If you want to set up Internet access, you must set up a connection to your Internet Service Provider (ISP). For broadband Internet access, your device provides the PPP-over-Ethernet (PPPoE), PPP-over-PPTP and PPP-over-ATM (PPPoA) protocols. You can also configure Internet access over ISDN.

Note

Note your provider's instructions.

Dialin connections over ISDN are used to establish a connection to networks or hosts outside your LANs.

All the entered connections are displayed in a list, which contains the **Description**, the **User Name**, the **Authentication** and the current **Status**.

The **Status** field can have the following values:

Possible values for Status

Field	Description
	connected
	not connected (dialup connection); connection setup possible
	not connected (e.g. because of an error during setup of an outgoing connection, a renewed attempt is only possible after a

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

Default Route

With a default route, all data is automatically forwarded to one connection if no other suitable route is available. Access to the Internet should always be set up as the default route to the Internet Service Provider (ISP). Further information on possible route types can be found under **Networking**->**Routes**.

Activating NAT

With Network Address Translation (NAT), you conceal your whole network to the outside world behind one IP address. You should certainly do this for your connection to the Internet Service Provider (ISP).

Only outgoing sessions are allowed initially if NAT is activated. To allow certain connections from outside to hosts within the LAN, these must be explicitly defined and admitted.

Connection Idle Timeout

The connection idle timeout is determined in order to clear the connection automatically if it is not being used, i.e. if data is no longer being sent, to help you save costs.

Block after Connection Failure

You use this function to set up a waiting time for outgoing connection attempts after which your device's connection attempt is regarded as having failed.

Authentication

When a call is received on ISDN connections, the calling party number is always sent over the ISDN D-channel. This number enables your device to identify the caller (CLID), provided the caller is entered on your device. After identification with CLID, your device can additionally carry out PPP authentication with the connection partner before it accepts the call.

Your device needs the necessary data for this, which you should enter here, for all PPP connections. Establish the type of authentication process that should be performed, then

enter a common password and two codes. You get this information, for example, from your Internet Service Provider (ISP) or the system administrator at your head office. If the data you entered on your device is the same as the caller's data, the call is accepted. The call is rejected if the data is not the same.

Callback

The callback mechanism can be used for every connection over an ISDN or over an AUX interface to obtain additional security regarding the connection partner or to clearly allocate the costs of connections. A connection is not set up until the calling party has been clearly identified by calling back. Your device can answer an incoming call with a callback or request a callback from a connection partner. Identification can be based on the calling party number or PAP/CHAP/MS-CHAP authentication. Identification is made in the former case without call acceptance, as the calling party number is transferred over the ISDN D-channel, and in the latter case with call acceptance.

Channel Bundling

Your device supports dynamic and static channel bundling for dialup connections. Channel bundling can only be used for ISDN connections for a bandwidth increase or as a backup. Only one B-channel is initially opened when a connection is set up.

Dynamic

Dynamic channel bundling means that your device connects other ISDN B-channels to increase the throughput for connections if this is required, e.g. for large data rates. If the amount of data traffic drops, the additional B-channels are closed again.

If devices from other manufacturers are to be used at the far end, ensure that these support dynamic channel bundling for a bandwidth increase or as a backup.

Static

In static channel bundling, you specify right from the start how many B-channels your device is to use for connections, regardless of the transferred data rate.

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 ADSL 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.

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name to uniquely identify the PPPoE partner. The first character in this field must not be a number No special characters or umlauts must be used.
PPPoE Mode	Select whether you want to use a standard Internet connection over PPPoE (*Standard*) or your Internet access is to be set up over several interfaces (*Multilink*). If you choose *Multilink*, 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. For PPPoE Multilink, we recommend using your device's Ethernet switch in Split-Port mode and to use a separate Ethernet interface e.g. *en1-1*, *en1-2* for each PPPoE connection. If you also want to use an external modem for PPPoE Multilink, you must run your device's Ethernet switch in Split-Port mode.
PPPoE Ethernet Interface	Only for **PPPoE Mode** = *Standard* Select the Ethernet interface specified for a standard PPPoE connection. If you want to use an external DSL modem, select the Ethernet port to which the modem is connected. When using the internal DSL modem, select here the EthoA interface configured in **WAN**->**ATM**->**Profiles**->**New**. Select *Automatic* 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 **ATM** menu. This is not required for a VDSL connection.

Field	Description
PPPoE Interfaces for Multilink	Only for **PPPoE Mode** = *Multilink* Select the interfaces you want to use for your Internet connection. Click the **Add** button to create new entries.
User Name	Enter the user name.
Password	Enter the password.
VLAN	Certain Internet service providers require a VLAN-ID. Activate this function to be able to enter a value under **VLAN ID**.
VLAN ID	Only if **VLAN** is enabled. Enter the VLAN-ID that you received from your provider.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. 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
Security Policy	Select the security settings to be used with the interface.

Field	Description
	Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address* (default value): Your device is dynamically assigned an IP address. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.
Local IP Address	Only if **IP Address Mode** = *Static* Enter the static IP address of the connection partner.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or

Field	Description
	network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.

Fields in the IPv6 Settings menu

Field	Description
IPv6	Select whether the selected PPPoE interface should use Internet Protocol version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled* . The function is disabled by default.
Security Policy	Select the security settings to be used with the interface. Possible values: • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. We recommend you use this setting if you want to use IPv6 outside of your LAN. • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
IPv6 Mode	Only for **IPv6** = *Enabled* The selected PPPoE interface is operated in host mode.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Select if Router Advertisements are to be received on the selected interface. Router Advertisements are used, e.g., to create the prefix list.

Field	Description
	The function is activated by selecting *Enabled* . The function is enabled by default.
DHCP Client	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Determine if your device is to act as DHCP client. The function is activated by selecting *Enabled* . The function is enabled by default.
IPv6 Addresses	Only for **IPv6** = *Enabled* You can assign **IPv6 Addresses** to the selected interface.. **Add** allows you to create one or more address entries. A new windows opens that allows you to specify an IPv6 address consisting of a Link Prefix and a host identifier. If your device operates in host mode (**IPv6 Mode** = *Host*, **Accept Router Advertisement** *Enabled* and **DHCP Client** = *Enabled*), its IPv6 addresses are determined through SLAAC. You need not configure an IPv6 address manually, but you can enter addtional addresses if desired. If your device is operating in router mode (**IPv6 Mode** = *Router (Transmit Router Advertisement)*, **Transmit Router Advertisement** = *Enabled* and **DHCP Server** = *Enabled*), you need to configure its IPv6 addresses here.

Use **Add** to create more entries.

Fields in the Link Prefix menu.

Field	Description
Setup Mode	Select in which way the Link Prefix is to be determined. Possible values: • *From General Prefix* (default value): The Link Prefix is derived from a General Prefix. • *Static*: You can enter the link prefix.

Field	Description
General Prefix	Only for **Setup Mode** = *From General Prefix* Select the General Prefix the Link Prefix is to be derived from. You can choose from the General Prefixes available under **Network->IPv6 General Prefixes->General Prefix Configuration->New**.
Auto Subnet Configuration	Only if **Setup Mode** = *From General Prefix* and if a General Prefix has been selected. Select if the subnet is to be created automatically. Automatic subnet creation will use ID *0* for the first subnet, ID *1* for the second, etc. Possible values for the sub net ID are: *0* - *65535*. 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. The function is activated by selecting *Enabled*. The function is enabled by default. If the function is disabled, you can define a subnet by entering a Subnet ID.
Subnet ID	Only if **Auto Subnet Configuration** is not active. 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. Possible values are *0* - *65535*. Upon subnet creation the decimal ID value is converted to a hexadecimal one.
Link Prefix	Only for **Setup Mode** = *Static* You can specify the Link Prefix of an IPv6 address. This prefix must end with *::*. Its predetermined length is *64*.

Fields in the Host Address menu.

Field	Description
Generation Mode	Determine if the Host Identifier of the IPv6 address is to be automatically derived from the MAC address through EUI-64. The function is activated by selecting *Enabled*. The function is enabled by default. EUI-64 triggers the following process: • The hexadecimal 48 bit MAC address is split into 2 x 24 bit. • *FFFE* is inserted into the created gap in order to obtain 64 bit. • The hexadecimal notation of the 64 bit is converted to a binary notation. • Bit no. 7 of the first 8 bit field is set to *1*.
Static Addresses	Independently of the automatic creation described under **Generation Mode**, you can manually specify the Host Identifier of one or more IPv6 addresses with **Add**. Its predefined length is *64*. Start any entry with *::*.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this connection partner. Select the authentication specified by your provider. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.

Field	Description
	• *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.
LCP Alive Check	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. The function is enabled with *Enabled*. The function is enabled by default.

Fiels in the IPv4 Advanced Settings menu

Field	Description
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU)

Field	Description
	in bytes that is allowed for the connection. With default value *Automatic*, the value is specified by link control at connection setup. If you disable *Automatic*, you can enter a value. Possible values are *1* to *8192*. The default value is *0*.

13.1.2 Dual Stack Lite

Dual Stack Lite allows the use of IPv4 connections even if the internet connection at hand is operated via IPv6 only. This is the case if, e.g., you need to continue using IPv4 connections, but your internet service provider assigns IPv6 addresses only due to a shortage of IPv4 addresses.

With DSLite IPv4 packets are "encapsulated" into IPv6 packets. These tunneled IPV4 packets are then sent to the AFTR server (Address Family Transition Router) of your internet service provider where they are "unpacked" and routed into the IPv4 realm of the internet.

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

13.1.2.1 New

Choose the **New** button to set up additional Dual Stack Lite interfaces.

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

Fields in the Basic Parameters menu

Field	Description
Description	Assign a name to your Dual Stack Lite connection.
IPv6 Interface	Select the IPv6 interface that is used for the DS Lite connection. This is normally the interface of your internet connection. IPv4 packets sent via this interface are encapsulated into IPv6 packets.

Field	Description
AFTR	Enter the IPv6 address or domain name of your Address Family Transition Router. The provider of your IPv6 internet connection will provide you with this information.
Default Route	Select whether you want to use this connection as the default route. This setting is useful in order to have the complete IPv4 data traffic that is to be sent over the internet be sent over the IPv6 connection. Otherwise, you need to make the corresponding adjustments to your routing. The function is enabled with *Enabled*. The function is enabled by default.

13.1.3 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.

13.1.3.1 New

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

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the internet connection. The first character in this field must not be a number No special characters or umlauts must be used.
PPTP Ethernet Interface	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. When using the internal DSL modem, select here the EthoA interface configured in **Physical**

Field	Description
	New, e.g. *ethoa50-0*.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle 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
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited.. • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Get IP Address* (default value): Your device is automatically assigned a temporarily valid IP address from the provider. • *Static* : You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.
Local IP Address	Only for **IP Address Mode** = *Static* Assign an IP address from your LAN to the PPT interface, which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this PPTP partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL).

Field	Description
	The function is enabled with *Enabled*. The function is disabled by default.
PPTP Address Mode	Displays the address mode. The value cannot be changed. Possible values: • *Static*: The **Local PPTP IP Address** will be assigned to the selected Ethernet port.
Local PPTP IP Address	Assign the PPTP interface an IP address that is used as the source address. The default value is *10.0.0.140*.
Remote PPTP IP Address	Enter the IP address of the PPTP partner. The default value is *10.0.0.138*.
LCP Alive Check	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. The function is enabled with *Enabled*. The function is enabled by default.

13.1.4 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**.

13.1.4.1 New

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

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

Fields in the Basic Parameters menu.

Field	Description
Description	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.
ATM PVC	Select an ATM profile created in the **ATM**->**Profiles** menu, indicated by the global identifiers VPI and VCI specified by the provider.
User Name	Enter the user name.
Password	Enter the password for the PPPoA connection.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. 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
Security Policy	Select the security settings to be used with the interface.

Field	Description
	Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited.. • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
IP Address Mode	Choose whether your device has a static IP address or is assigned one dynamically. Possible values: • *Get IP Address* (default value): Your device is dynamically assigned an IP address. • *Static*: You enter a static IP address.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.
Local IP Address	Only for **IP Address Mode** = *Static* Enter the static IP address you received from your provider.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or

Field	Description
	network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.

Fields in the IPv6 Settings menu

Field	Description
IPv6	Select whether the selected ATM profile should use Internet Protocol version 6 (IPv6) for data transmission. The function is activated by selecting *Enabled* . The function is disabled by default.
Security Policy	Select the security settings to be used with the ATM profile. Possible values: • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. We recommend you use this setting if you want to use IPv6 outside of your LAN. • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. We recommend you use this setting if you want to use IPv6 on your LAN. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
IPv6 Mode	Only for **IPv6** = *Enabled* The selected PPPoE interface is operated in host mode.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* 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.

Field	Description
	The function is activated by selecting *Enabled* . The function is enabled by default.
DHCP Client	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Determine if your device is to act as DHCP client. The function is activated by selecting *Enabled* . The function is enabled by default.
IPv6 Addresses	Only for **IPv6** = *Enabled* You can assign **IPv6 Addresses** to the selected interface.. **Add** allows you to create one or more address entries. A new windows opens that allows you to specify an IPv6 address consisting of a Link Prefix and a host identifier. If your device operates in host mode (**IPv6 Mode** = *Host*, **Accept Router Advertisement** *Enabled* and **DHCP Client** = *Enabled*), its IPv6 addresses are determined through SLAAC. You need not configure an IPv6 address manually, but you can enter addtional addresses if desired. If your device is operating in router mode (**IPv6 Mode** = *Router (Transmit Router Advertisement)*, **Transmit Router Advertisement** = *Enabled* and **DHCP Server** = *Enabled*), you need to configure its IPv6 addresses here.

Use **Add** to create more entries.

Fields in the Link Prefix menu.

Field	Description
Setup Mode	Select in which way the Link Prefix is to be determined. Possible values: • *From General Prefix* (default value): The Link Prefix is derived from a General Prefix. • *Static*: You can enter the link prefix.

Field	Description
General Prefix	Only for **Setup Mode** = *From General Prefix* Select the General Prefix the Link Prefix is to be derived from. You can choose from the General Prefixes available under **Network->IPv6 General Prefixes->General Prefix Configuration->New**.
Auto Subnet Configuration	Only if **Setup Mode** = *From General Prefix* and if a General Prefix has been selected. Select if the subnet is to be created automatically. Automatic subnet creation will use ID *0* for the first subnet, ID *1* for the second, etc. Possible values for the sub net ID are: *0* - *65535*. 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. The function is activated by selecting *Enabled*. The function is enabled by default. If the function is disabled, you can define a subnet by entering a Subnet ID.
Subnet ID	Only if **Auto Subnet Configuration** is not active. 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. Possible values are *0* - *65535*. Upon subnet creation the decimal ID value is converted to a hexadecimal one.
Link Prefix	Only for **Setup Mode** = *Static* You can specify the Link Prefix of an IPv6 address. This prefix must end with *::*. Its predetermined length is *64*.

Fields in the Host Address menu.

Field	Description
Generation Mode	Determine if the Host Identifier of the IPv6 address is to be automatically derived from the MAC address through EUI-64. The function is activated by selecting *Enabled*. The function is enabled by default. EUI-64 triggers the following process: • The hexadecimal 48 bit MAC address is split into 2 x 24 bit. • *FFFE* is inserted into the created gap in order to obtain 64 bit. • The hexadecimal notation of the 64 bit is converted to a binary notation. • Bit no. 7 of the first 8 bit field is set to *1*.
Static Addresses	Independently of the automatic creation described under **Generation Mode**, you can manually specify the Host Identifier of one or more IPv6 addresses with **Add**. Its predefined length is *64*. Start any entry with *::*.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *60*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Authentication	Select the authentication protocol for this Internet connection. Select the authentication specified by your provider. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted.

Field	Description
	• *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.
LCP Alive Check	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. The function is enabled with *Enabled*. The function is enabled by default.

13.1.5 ISDN

A list of all ISDN interfaces in TE mode (ISDN extern)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

13.1.5.1 New

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

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

Fields in the Basic Parameters menu.

Field	Description
Description	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.
Connection Type	Select which layer 1 protocol your device should use. 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. Possible values: • *ISDN 64 kbps*: For 64-kbps ISDN data connections. • *ISDN 56 kbps*: For 56-kbps ISDN data connections.
User Name	Enter your device code (local PPP user name).
Remote User (for Dial-in only)	Enter the code of the remote terminal (remote PPP user name).
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.

Field	Description
	Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle 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 `20`.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • `Static` (default value): You enter a static IP address. • `Provide IP Address`: Your device dynamically assigns an IP address to the remote terminal. • `Get IP Address`: Your device is dynamically assigned an IP address.
Default Route	Only for **IP Address Mode** = `Static` and `Get IP Address` Select whether the route to this connection partner is to be defined as the default route. The function is enabled with `Enabled`. The function is disabled by default.
Create NAT Policy	Only for **IP Address Mode** = `Static` and `Get IP Address` When you configure an ISDN Internet connection, specify whether Network Address Translation (NAT) is to be activated. The function is enabled with `Enabled`. The function is disabled by default.
Local IP Address	Only if **IP Address Mode** = `Static`

Field	Description
	Assign the IP address from your LAN to the ISDN interface which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.
IP Assignment Pool	Only if **IP Address Mode** = *Provide IP Address* Select IP pools configured in the **WAN**->**Internet + Dialup**->**IP Pools**menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Usage Type	If necessary, select a special interface use. Possible values: • *Standard* (default value): No special type is selected. • *Dialin only*: The interface is used for incoming dialup connections and callbacks initiated externally.

Field	Description
	• *Multi-User (Dialin only)*: The interface is defined as multi-user connection partner, i.e. several clients dial in with the same user name and password.
Authentication	Select the authentication protocol for this PPTP partner. Possible values: • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial then the authentication protocol required by the connection partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
Encryption	Only for **Authentication** = *MS-CHAPv2* 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 **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None* (default value): MPP encryption is not used. • *Enabled*: MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Callback Mode	Select the Callback Mode function. Possible values:

Field	Description

	• *None* (default value): Your device does not call back.
	• *Active*: Select one of the following options:
	  • *No PPP negotiation*: Your device calls the connection partner to request a callback.
	  • *Windows Client Mode*: Your device calls the connection partner to request a callback via CBCP (Callback Control Protocol). Needed for Windows clients.
	• *Passive*: Select one of the following options:
	  • *PPP Negotiation or CLID*: Your device calls back immediately when requested to do so by the connection partner.
	  • *Windows Server Mode*: Your device calls back after a period of time suggested by the Microsoft client (NT: 10 seconds, new systems: 12 seconds. It uses the call number (**Entries**->**Call Number**) with the **Mode** *Outgoing* or *Both* 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.
	  • *Delayed, CLID only*: 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.
	  • *Windows Server Mode, Callback optional*: like *Windows Server Mode* 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 **Cancel**.

Fields in the Bandwith on Demand Options menu.

Field	Description
Channel Bundling	Select whether channel bundling is to be used for ISDN connections with the connection partner, and if so, what type. Your device supports dynamic and static channel bundling for

Field	Description
	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. Possible values: • *None* (default value): No channel bundling, only one B-channel is ever available for connections. • *Static*: Static channel bundling. • *Dynamic*: Dynamic channel bundling.

Fields in the Dial Numbers menu

Field	Description
Entries	Add new entries with **Add**.

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

Field	Description
Mode	Only if **Entries** = *Add* The calling party number of the call is compared with the number entered under **Call Number**. Defines whether **Call Number** should be used for incoming or outgoing calls or for both. Possible values: • *Both* (default value): For incoming and outgoing calls. • *Incoming*: For incoming calls, where your connection partner dials in to your device. • *Outgoing*: For outgoing calls, where you dial your connection partner. The calling party number of the incoming call is compared with the number entered under **Call Number**.
Call Number	Enter the connection partner's numbers.
Number of Used Ports	Select which port is used.

Fields in the IP Options menu.

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent. Possible values: • *Passive* (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. • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether and how ARP requests from your own LAN are to be responded to for the specified connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this connection partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the connection partner is *Up* or *Dormant*. In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the connection partner is *Up* , i.e. a connection already exists to the connection partner.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** and **WINS Server Primary** and **Secondary** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.

13.1.6 AUX

In the **WAN**->**Internet + Dialup**->**AUX** menu, a list of all AUX interfaces is displayed.

You can define various settings for communication between the gateway and modem in this menu. You require a special cable for the console port of your gateway (e.g. AUX Backup cable) to connect an external analogue modem to the AUX port on a bintec elmeg-bintec elmeg gateway.

13.1.6.1 New

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

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the WAN partner. The first character in this field must not be a number No special characters or umlauts must be used.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default. Only activate this option if you have Internet access with a flat-rate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold.

Field	Description
	The default value is *600*.

Fields in the IPv4 Settings menu.

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited.. • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically or whether it should be assigned this dynamically at the remote terminal. Possible values: • *Get IP Address* (default value): Your device is dynamically assigned an IP address. • *Static*: You enter a static IP address. • *Provide IP Address*: Your device dynamically assigns an IP address to the remote terminal.
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is enabled by default.
Create NAT Policy	Specify whether Network Address Translation (NAT) is to be activated. The function is enabled with *Enabled*. The function is enabled by default.

Field	Description
Local IP Address	Only if **IP Address Mode** = *Static* Enter the static IP address of the connection partner.
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.
IP Assignment Pool	Only if **IP Address Mode** = *Provide IP Address* Select IP pools configured in the **WAN**->**Internet + Dialup**->**IP Pools**menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *50*.
Maximum Number of Dialup Retries	Enter the number of unsuccessful attempts to setup a connection before the interface is blocked. Possible values are *0* to *100*. The default value is *5*.
Usage Type	If necessary, select a special interface use. Possible values: • *Standard* (default value): No special type is selected.

Field	Description
	• *Dialin only*: The interface is used for incoming dialup connections and callbacks initiated externally. • *Multi-User (Dialin only)* : The interface is defined as multi-user connection partner, i.e. several clients dial in with the same user name and password.
Authentication	Select the authentication protocol for this PPTP partner. Possible values: • *PAP/CHAP/MS-CHAP*: Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *PAP* (default value): Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the connection partner or sends these to the connection partner. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.
LCP Alive Check	Select whether the availability of the remote terminal is to be

Field	Description
	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. The function is enabled with *Enabled*. The function is enabled by default.

Callback Mode	Select the Callback Mode function.
	
	Possible values:
	
	• *None* (default value): Your device does not call back.
	• *Active*: Select one of the following options:
	  • *No PPP negotiation*: Your device calls the connection partner to request a callback.
	  • *Windows Client Mode*: Your device calls the connection partner to request a callback via CBCP (Callback Control Protocol). Needed for Windows clients.
	• *Passive*: Select one of the following options:
	  • *PPP Negotiation or CLID*: Your device calls back immediately when requested to do so by the connection partner.
	  • *Windows Server Mode*: Your device calls back after a period of time suggested by the Microsoft client (NT: 10 seconds, new systems: 12 seconds. It uses the call number (**Entries**->**Number**) with the **Mode** *Outgoing* or *Both* entered for the connection partner. If no number is entered, the required number can be reported by the caller in a PPP negotiation. This setting should be avoided where possible for security reasons. Currently cannot be avoided for the connection of mobile Microsoft clients via DCN.
	  • *Delayed, CLID only*: 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.
	  • *Windows Server Mode, Callback optional*: like *Windows Server Mode* 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

Field	Description
	been configured for the connection partner. This is done by pressing CANCEL to close the dialog box that appears.

Fields in the Dial Numbers menu.

Field	Description
Entries	Add new entries with **Add**.

Fields in the menu Dial Number Configuration entry: <1> (only appears for Entries = Add

Field	Description
Mode	Only if **Entries** = *Add* Defines whether **Number** should be used for incoming or outgoing calls or for both. Possible values: • *Both* (default value): For incoming and outgoing calls. • *Incoming*: For incoming calls, where your connection partner dials in to your device. • *Outgoing*: For outgoing calls, where you dial your connection partner. The calling party number of the incoming call is compared with the number entered under **Number**.
Call Number	Enter the connection partner's numbers.

Fields in the IP Options menu.

Field	Description
Proxy ARP Mode	Select whether and how ARP requests from your own LAN are to be responded to for the specified connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this connection partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the connection partner is *Up* or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the connection partner is *Up* , i.e.

Field	Description
	a connection already exists to the connection partner.

13.1.7 IP Pools

Note

Note that the menu **IP Pools** is only available if a port in the menu **Physical Interfaces**->**ISDN Ports**-> **ISDN Configuration** is set to external operation (TE mode). A corresponding adapter which is available seperately needs to be connected for external operation.

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.

13.1.7.1 Edit or New

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

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.

Field	Description
	Secondary: Optionally, enter the IP address of an alternative DNS server.

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.

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*).

13.2.1.1 New

Choose the **New** button to set up new ATM profiles.

The menu **WAN**->**ATM**->**Profiles**->**New** consists of the following fields:

Fields in the ATM Profiles Parameter menu.

Field	Description
Provider	Select one of the preconfigured ATM profiles for your provider from the list or manually define the profile using *-- User-defined --*.
Description	Only for **Provider** = *-- User-defined --* Enter the desired description for the connection.
ATM Interface	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.
Type	Only for **Provider** = *-- User-defined --* Select the protocol for the ATM connection. Possible values: • *Ethernet over ATM* (default value): Ethernet over ATM (EthoA) is used for the ATM connection (Permanent Virtual Circuit, PVC). • *Routed Protocols over ATM*: Routed Protocols over ATM (RPoA) is used for the ATM connection (Permanent Virtual Circuit, PVC).

Field	Description
	• *PPP over ATM*: PPP over ATM (PPPoA) is used for the ATM connection (Permanent Virtual Circuit, PVC).
Virtual Path Identifier (VPI)	Only for **Provider** = *-- User-defined --* 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*.
Virtual Channel Identifier (VCI)	Only for **Provider** = *-- User-defined --* Enter the VCI value of the ATM connection. The VCI is the identification 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. Possible values are *32* to *65535*. The default value is 32.
Encapsulation	Only for **Provider** = *-- User-defined --* Select the encapsulation to be used. Note your provider's instructions. Possible values (in accordance with RFC 2684): • *LLC Bridged no FCS* (Default value for Ethernet over ATM : Is only displayed for **Type** = *Ethernet over ATM*. Bridged Ethernet with LLC/SNAP encapsulation without Frame Check Sequence (checksums). • *LLC Bridged FCS*: only displayed for **Type** = *Ethernet over ATM*. Bridged Ethernet with LLC/SNAP encapsulation with Frame Check Sequence (checksums). • *Non ISO* (default value for Routed Protocols over ATM): Is only displayed for **Type** = *Routed Protocols over ATM*. Encapsulation with LLC/SNAP header, suitable for IP routing.

Field	Description
	• *LLC*: only displayed for **Type** = *PPP over ATM*. Encapsulation with LLC header. • *VC Multiplexing* (default value for PPP over ATM): Bridged Ethernet without additional encapsulation (Null Encapsulation) with Frame Check Sequence (checksums).

Fields in menu Ethernet over ATM Settings (appears only for Type = Ethernet over ATM)

Field	Description
Default Ethernet for PPPoE Interfaces	Only for **Type** = *Ethernet over ATM* Select whether this Ethernet-over-ATM interface is to be used for all PPPoE connections The function is enabled with *Enabled*. The function is disabled by default.
Address Mode	Only for **Type** = *Ethernet over ATM* Select how an IP address is to be assigned to the interface. Possible values: • *Static* (default value): The interface is assigned a static IP address in **IP Address / Netmask**. • *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
IP Address/Netmask	Only for **Address Mode** = *Static* Enter the IP addresses (**IP Address**) and the corresponding netmasks (**Netmask**) of the ATM interfaces. Add new entries with **Add**.
MAC Address	Enter a MAC address for the internal router interface of ATM connection, e.g. *00:a0:f9:06:bf:03*. An entry is only required in special cases. For Internet connections, it is sufficient to select the option **Use built-in** (default setting). An address is used which is derived from the MAC address of the *en1-0*.

Field	Description
DHCP MAC Address	Only for **Address Mode** = *DHCP* Enter the MAC address of the internal router interface of ATM connection, e.g. *00:e1:f9:06:bf:03*. If your provider has assigned you an MAC address for DHCP, enter this here. You can also select the **Use built-in** option (default setting) An address is used which is derived from the MAC address of the *en1-0*.
DHCP Hostname	Only for **Address Mode** = *DHCP* If necessary, enter the host name registered with the provider to be used by your device for DHCP requests. 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
IP Address/Netmask	Enter the IP addresses (**IP Address**) and the corresponding netmasks (**Netmask**) of the ATM interface. Add new entries with **Add**.
Prioritize TCP ACK Packets	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 *Enabled*. The function is disabled by default.

Field in menu PPP over ATM Settings (appears only for Type = PPP over ATM)

Field	Description
Client Type	Select whether the PPPoA connection is to be set up permanently or on demand. Possible values: • *On Demand* (default value): The PPPoA is only set up on

Field	Description
	demand, e.g. for Internet access. You'll find additional information on PPP over ATM under *PPPoA* on page 275.

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.

The menu **WAN**->**ATM**->**Service Categories**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Virtual Channel Connection (VCC)	Select the already configured ATM connection (displayed by the combination of VPI and VCI) for which the service category is to be defined.
ATM Service Category	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).

Field	Description
	Possible settings: • *Unspecified Bit Rate (UBR)* (default value): No specific data rate is guaranteed for the connection. The **Peak Cell Rate (PCR)** specifies the limit above which data is discarded. This category is suitable for non-critical applications. • *Constant Bit Rate (CBR)*: (Constant Bit Rate) The connection is assigned a guaranteed data rate determined by the **Peak Cell Rate (PCR)**. This category is suitable for critical (real-time) applications that require a guaranteed data rate. • *Variable Bit Rate V.1 (VBR.1)*: A guaranteed data rate is assigned to the connection - **Sustained Cell Rate (SCR)**. This may be exceeded by the volume configured in **Maximum Burst Size (MBS)**. Any additional ATM traffic is discarded. The **Peak Cell Rate (PCR)** constitutes the maximum possible data rate. This category is suitable for non-critical applications with burst data traffic. • *Variable Bit Rate V.3 (VBR.3)*: A guaranteed data rate is assigned to the connection - **Sustained Cell Rate (SCR)**. This may be exceeded by the volume configured in **Maximum Burst Size (MBS)**. 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 **Peak Cell Rate (PCR)** constitutes the maximum possible data rate. This category is suitable for critical applications with burst data traffic.
Peak Cell Rate (PCR)	Enter a value for the maximum data rate in bits per second. Possible values: *0* to *10000000*. The default value is *0*.
Sustained Cell Rate (SCR)	Only for **ATM Service Category** = *Variable Bit Rate V.1 (VBR.1)* or *Variable Bit Rate V.3 (VBR.3)* Enter a value for the minimum available, guaranteed data rate in bits per second. Possible values: *0* to *10000000*. The default value is *0*.

Field	Description
Maximum Burst Size (MBS)	Only for **ATM Service Category** = *Variable Bit Rate V.1 (VBR.1)* or *Variable Bit Rate V.3 (VBR.3)* Enter a value for the maximum number of bits per second by which the PCR can be exceeded briefly. Possible values: *0* to *100000*. The default value is *0*.

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.

The menu **WAN**->**ATM**->**OAM Controlling**->**New** consists of the following fields:

Fields in the OAM Flow Configuration menu.

Field	Description
OAM Flow Level	Select the OAM flow level to be monitored. Possible values: • *F5*: (virtual channel level) The OAM settings are used for the virtual channel (default value). • *F4* : (virtual path level) The OAM settings are used on the virtual path.
Virtual Channel Connection (VCC)	Only for **OAM Flow Level** = *F5* Select the already configured ATM connection to be monitored (displayed by the combination of VPI and VCI).
Virtual Path Connection (VPC)	Only for **OAM Flow Level** = *F4* Select the already configured virtual path connection to be monitored (displayed by the VPI).

Fields in the Loopback menu.

Field	Description
Loopback End-to-End	Select whether you activate the loopback test for the connection between the endpoints of the VCC or VPC. The function is enabled with *Enabled*. The function is disabled by default.
End-to-End Send Interval	Only if **Loopback End-to-End** is enabled. Enter the time in seconds after which a loopback cell is to be sent. Possible values are *0* to *999*. The default value is 5.
End-to-End Pending Requests	Only if **Loopback End-to-End** is enabled. Enter the number of directly consecutive loopback cells that

Field	Description
	may fail to materialise before the connection is regarded as interrupted ("down"). Possible values are *1* to *99*. The default value is *5*.
Loopback Segment	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. The function is enabled with *Enabled*. The function is disabled by default.
Segment Send Interval	Only if **Loopback Segment** is enabled. Enter the time in seconds after which a loopback cell is sent. Possible values are *0* to *999*. The default value is *5*.
Segment Pending Requests	Only if **Loopback Segment** is enabled. Enter the number of directly consecutive loopback cells that may fail to materialise before the connection is regarded as interrupted ("down"). Possible values are *1* to *99*. The default value is *5*.

Fields in the CC Activation menu.

Field	Description
Continuity Check (CC) End-to-End	Select whether you activate the OAM-CC test for the connection between the endpoints of the VCC or VPC. Possible values: • *Passive* (default value): OAM CC requests are responded to after CC negotiation (CC activation negotiation). • *Active*: OAM CC requests are sent after CC negotiation (CC activation negotiation). • *Both*: OAM CC requests are sent and answered after CC ne-

Field	Description
	gotiation (CC activation negotiation). • *No negotiation*: Depending on the setting in the **Direction** field, OAM CC requests are either sent and/or responded to. There is no CC negotiation. • *Passive*: The function is disabled. Also select whether the test cells of the OAM CC are to be sent or received. Possible values: • *Both* (default value): CC data is both received and generated. • *Sink*: CC data is received. • *Source*: CC data is generated.
Continuity Check (CC) Segment	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. Possible values: • *Passive* (default value): OAM CC requests are responded to after CC negotiation (CC activation negotiation). • *Active*: OAM CC requests are sent after CC negotiation (CC activation negotiation). • *Both*: OAM CC requests are sent and answered after CC negotiation (CC activation negotiation). • *No negotiation*: Depending on the setting in the **Direction** field, OAM CC requests are either sent and/or responded to. There is no CC negotiation. • *None*: The function is disabled. Also select whether the test cells of the OAM CC are to be sent or received. Possible settings: • *Both* (default value): CC data is both received and generated. • *Sink*: CC data is received. • *Source*: CC data is generated.

Field	Description

13.3 Leased Line

A leased line is a permanent (fixed) connection between two communication partners via a telecommunications network. Unlike a switched line, the entire transmission channels is always available. The leased line cannot be set up by the subscriber by dialling and therefore has no call number. The connection must be set up by the network operator.

13.3.1 Interfaces

In the **WAN**->**Leased Line**->**Interfaces** menu, a list of all is displayed. Automatic generation requires the corresponding ISDN interface to be configured.

13.3.1.1 Edit

Choose the button to edit the configuration of the corresponding leased line for a BRI interface.

The **WAN**->**Leased Line**->**Interfaces**->**Autogenerated from BRI (ISDN-S0)**-> menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description for the connection.

Fields in the IP Mode and Routes menu.

Field	Description
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Enter the IP address you received from your network operator.
Route Entries	Define other routing entries for this connection class. Add new entries with **Add**.

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

Fields in the Advanced Settings menu.

Field	Description
LCP Alive Check	Select whether the reachability of the remote terminal is to be checked. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. The function is enabled with *Enabled*. The function is disabled by default.
Compression	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None* (default value): Encryption is not used. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression

Fields in the IP Options menu.

Field	Description
OSPF Mode	Specify whether OSPF protocol packets are sent over the interface. Possible values: • *Passive* (default value): OSPF is not activated for this interface, i.e. no OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • *Active*: OSPF is not activated for this interface, i.e. OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.

Field	Description
Proxy ARP Mode	Select whether and how ARP requests are to be responded to for the specified connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this connection partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the connection partner is *Up* or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the connection partner is *Up* , i.e. a connection already exists to the connection partner.

Choose the button to edit the configuration of the corresponding leased line for a PRI interface.

The **WAN**->**Leased Line**->**Interfaces**->**Autogenerated from PRI (ISDN-S2M)**-> menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description for the connection.

Fields in the IP Mode and Routes menu.

Field	Description
Default Route	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Enter the IP address you received from your network operator.
Route Entries	Define other routing entries for this connection class. Add new entries with **Add**.

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

Fields in the Advanced Settings menu.

Field	Description
LCP Alive Check	Select whether the reachability of the remote terminal is to be checked. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. The function is enabled with *Enabled*. The function is disabled by default.
Compression	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None* (default value): Encryption is not used. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression

Fields in the IP Options menu.

Field	Description
OSPF Mode	Specify whether OSPF protocol packets are sent over the interface. Possible values: • *Passive* (default value): OSPF is not activated for this interface, i.e. no OSPF protocol packets sent over this interface. Networks reachable over this interface are, however, included when calculating the routing information and propagated over active interfaces. • *Active*: OSPF is not activated for this interface, i.e. OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.

Field	Description
Proxy ARP Mode	Select whether and how ARP requests are to be responded to for the specified connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this connection partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the connection partner is *Up* or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the connection partner is *Up*, i.e. a connection already exists to the connection partner.

13.4 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.

13.4.1 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.

13.4.1.1 New

Click the **New** button to optimise voice transmission for other interfaces.

The menu **WAN**->**Real Time Jitter Control**->**Controlled Interfaces**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Interface	Define for which interfaces voice transmission is to be optimised.
Control Mode	Select the mode for the optimisation. Possible values: • *Controlled RTP Streams only* (default value): By means of the data routed via the media gateway, the system detects voice data traffic and optimises the voice transmission. • *All RTP Streams*: All RTP streams are optimised. • *Inactive*: Voice data transmission is not optimised. • *Always*: Voice data transmission is always optimised.
Maximum Upload Speed	Enter the maximum available upstream bandwidth in kbp/s for the selected interface.

Chapter 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 97). IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

Additional 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 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 match 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.

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 524.

14.1.1.1 New

Choose the **New** button to set up more IPSec peers.

The menu **VPN**->**IPSec**->**IPSec Peers**->**New** consists of the following fields:

Fields in the menu Peer Parameters

Field	Description
Administrative Status	Select the status to which you wish to set the peer after saving the peer configuration. Possible values: • *Up* (default value): The peer is available for setting up a tunnel immediately after saving the configuration. • *Down*: The peer is initially not available after the configuration has been saved.
Description	Enter a description of the peer that identifies it. The maximum length of the entry is 255 characters.
Peer Address	Select the **IP Version**. You can choose if IPv4 or IPv6 is to be preferred or if only one IP version is to be permitted. **Note** This selection is only relevant if an IP address is entered as host name. Possible values: • *IPv4 Preferred* • *IPv6 Preferred* • *IPv4 Only* • *IPv6 Only* Enter the public IP address of the peer or a resolvable host name. This entry can be omitted in certain configurations, but in that case your device cannot initiate an IPSec connection.
Peer ID	Select the ID type and enter the peer ID. This entry is not necessary in certain configurations.

Field	Description
	The maximum length of the entry is 255 characters. Possible ID types: • *Fully Qualified Domain Name (FQDN)*: Any string • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *Key ID*: Any string On the peer device, this ID corresponds to the **Local ID Value**.
Internet Key Exchange	Select the version of the Internet Exchange Protocol to be used. Possible values: • *IKEv1* (default value): Internet Key Exchange Protocol Version 1 • *IKEv2*: Internet Kex Exchange Protocol Version 2
Authentication Method	Only for **Internet Key Exchange** = *IKEv2* Select the authentication method. Possible values: • *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **IPSec Peers**. The preshared key is the shared password. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm.
Local ID Type	Only for **Internet Key Exchange** = *IKEv2* Select the local ID type. Possible ID types: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)*

Field	Description
	• *Key ID*: Any string
Local ID	Only for **Internet Key Exchange** = *IKEv2* Enter the ID of your device. For **Authentication Method** = *DSA Signature* or *RSA Signature* the option **Use Subject Name from certificate** is displayed. When you enable the option **Use Subject Name from certificate**, the subject name indicated in the certificate is used.
Preshared Key	Enter the password agreed with the peer. The maximum length of the entry is 50 characters. All characters are possible except for *0x* at the start of the entry.
IP Version of the tunneled Networks	Select if IPv4, IPv6 or both versions are allowed for the VPN tunnel. Possible values: • *IPv4* • *IPv6* • *IPv4 and IPv6*

Fields in the menu IPv4 Interface Routes

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.

Field	Description
IP Address Assignment	Select the configuration mode of the interface. Possible values: • *Static* (default value): Enter a static IP address. • *IKE Config Mode Client*: Select this option if your gateway receives an IP address from the server as IPSec client. • *IKE Config Mode Server*: Select this option if your gateway assigns an IP address as server for connecting clients. This is taken from the selected **IP Assignment Pool**.
Config Mode	Only where **IP Address Assignment** = *IKE Config Mode Server* or *IKE Config Mode Client* Possible values: • *Pull* (default value): The client requests the IP address and the gateway answers the request. • *Push*: The gateway suggests an IP address to the client and the client must either accept or reject this. This value must be identical for both sides of the tunnel.
IP Assignment Pool	Only if **IP Address Assignment** = *IKE Config Mode Server* Select an IP pool configured in the **VPN**->**IPSec**->**IP Pools**menu. If an IP pool has not been configured here yet, the message *Not yet defined* appears in this field.
Default Route	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Client* Select whether the route to this IPSec peer is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Server* Enter the WAN IP address of your IPSec tunnel. This can be the

Field	Description
	same IP address as the address configured on your router as the LAN IP address.
Metric	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Client* and **Default Route** = *Enabled* Select the priority of the route. The lower the value, the higher the priority of the route. Value range from *0* to *15*. The default value is *1*.
Route Entries	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Client* Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask for *Remote IP Address*. • *Metric*: The lower the value, the higher the priority of the route (possible values *0..15*). The default value is *1*.

Fields in the menu Additional IPv4 Traffic Filter

Field	Description
Additional IPv4 Traffic Filter	Only for **Internet Key Exchange** = *IKEv1* Use **Add** to create a new filter.

Fields in the IPv6 Interface Routes menu

Field	Description
Security Policy	Select the security settings to be used with the interface.. Possible values: • *Untrusted*: IP packets are only allowed through if the connection has been initiated from "inside". We recommend you use this setting if you want to use IPv6 outside of your LAN. • *Trusted* (default value): All IP packets are allowed through except for those which are explicitly prohibited.

Field	Description
	We recommend you use this setting if you want to use IPv6 on your LAN. You can configure exceptions for the selected setting in the *Firewall* on page 368 menu.
Local IPv6 Network	Select a network. You can choose from the Link Prefixes avialbale under **LAN**->**IP Configuration**->**Interfaces**->**New**. Enter the Local IPv6 address and the corresponding prefix length. The default prefix length is /64.This prefix must end with ::.
Remote IPv6 Network	Add a new prefix. Enter the address of the other tunnel endpoint. The default prefix **Length** is *64* and the default **Priority** is *1*. The lower the value entered for **Priority**, the higher the priority of the route.

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**.

Fields in the menu Basic Parameters

Field	Description
Description	Enter a description for the filter.
Protocol	Select a protocol. The *Any* option (default value) matches all protocols.
Source IP Address/ Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: • *Any* • *Host*: Enter the IP address of the host. • *Network* (default value): Enter the network address and the related netmask.
Source Port	Only for **Protocol** = *TCP* or *UDP* Enter the source port of the data packets. The default setting *-All-* (= -1) means that the port remains unspecified.
Destination IP Address/Netmask	Enter the destination IP address and corresponding netmask of the data packets.
Destination Port	Only for **Protocol** = *TCP* or *UDP*

Field	Description
	Enter the destination port of the data packets. The default setting *-All-* (= -1) means that the port remains unspecified.

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

Fields in the menu Advanced IPSec Options

Field	Description
Phase-1 Profile	Select a profile for Phase 1. Besides user-defined profiles, predefined profiles are available. Possible values: • *None (use default profile)*: Uses the profile marked as standard in **VPN**->**IPSec**->**Phase-1 Profiles** • *Multi-Proposal*: Uses a special profile which contains the proposals for Phase 1 3DES/MD5, AES/MD5 and Blowfish/MD5 regardless of the proposal selection in menu **VPN**->**IPSec**->**Phase-1 Profiles**. • *<Profilname>*: Uses a profile configured in menu **VPN**->**IPSec**->**Phase-1 Profiles** for Phase 1.
Phase-2 Profile	Select a profile for Phase 2. Besides user-defined profiles, predefined profiles are available. Possible values: • *None (use default profile)*: Uses the profile marked as standard in **VPN**->**IPSec**->**Phase-2 Profiles** • *Multi-Proposal*: Uses a special profile which contains the proposals for Phase 2 3DES/MD5, AES-128/MD5 and Blowfish/MD5 regardless of the proposal selection in menu **VPN**->**IPSec**->**Phase-2 Profiles**. • *<Profilname>*: Uses a profile configured in menu **VPN**->**IPSec**->**Phase-2 Profiles** for Phase 2.
XAUTH Profile	Select a profile created in **VPN**->**IPSec**->**XAUTH Profiles** if you wish to use this IPSec peer XAuth for authentication. If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

Field	Description
Number of Admitted Connections	Choose how many users can connect using this peer profile. Possible values: • *One User* (default value): Only one peer can be connected with the data defined in this profile. • *Multiple Users*: 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. The configuration of the dynamic peer must not have a Peer ID or a Per IP Address. Clients connecting to the gateway, however, must have a **Local ID** configured, since this ID is used to distinguish the IPSec tunnels created by dynamic peers. Find information on how to configure this ID type for your IPSec client in its respective documentation. The resulting peer would not apply to all incoming tunnel requests and needs to be moved to the end of the IPSec peer list. Otherwise, all subsequent peers in the list would inactive.
Start Mode	Select how the peer is to be switched to the active state. Possible values: • *On Demand* (default value): The peer is switched to the active state by a trigger. • *Always up*: The peer is always active.
Backup Peer	Only for peers using IKEv2. If a peer has been configured for the **Start Mode** *Always up*, you can select another, already configured peer as a backup option. If the current peer becomes inactive, e.g. because of an outage of the central VPN dial-in node, the backup peer can initiate a connection to a backup VPN dial-in node. If the primary dial-in node becomes available again, the connection is seamlessly switched back. This solution requires that the routing for the peers has to be configured in a way that a connection to the remote site is actually possible via either of them. Moreover, the routing metric for the backup peer should be lesser than for the primary peer. This ensures that the tunnel is switched back to the primary peer as

Field	Description
	soon as its connection is available again.
Delay until returning to primary peer	If in a fallback case the primary peer is coming up again, it may be desirable to delay the use of the primary peer and thus the reset of the secondary peer. This option defines the intended delay time.

Fields in the menu Advanced IP Options

Field	Description
Public Interface	Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select *Choosen by Routing*, 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 setting under **Public Interface Mode**.
Public Interface Mode	Only when an interface is selected for **Public Interface**. Specify how strictly the setting is handled. Possible values: • *Force*: Only the selected interface is used, independently from the priorities in the current routing table. • *Preferred*: 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.
Public Source IPv4 Address	If you are operating more than one Internet connection in parallel, here you can specify the public IP address that is to be used as the source address for the peer's data traffic. Select whether the **Public Source IPv4 Address** is to be enabled. The function is enabled with *Enabled*. In the input field, enter the public IP address that is to be used as the sender address. The function is disabled by default.
Public Source IPv6 Address	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

Field	Description
	the **Public Source IPv6 Address** is to be enabled. The function is enabled with *Enabled*. In the input field, enter the public IP address that is to be used as the sender address. The function is disabled by default.
IPv4 Back Route Verify	Select whether a check on the back route should be activated for the interface to the connection partner. The function is enabled with *Enabled*. The function is disabled by default.
MobIKE	Only for peers with IKEv2. **MobIKE** In cases of changing public IP addresses, enables only these addresses to be updated in the SAs without the SAs themselves having to be renegotiated. The function is enabled by default. 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.
IPv4 Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this IPSec peer. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the IPSec peer is *Up* (active) or *Dormant* (dormant). In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the IPSec peer is *Up* (active), i.e. a connection already exists to the IPSec peer.

Field	Description
CA Certificates	Only available if certificates are in use on the device. If you enable the **Trust the following CA certificates** option, you can select CA certificates that are accepted for this profile. This option can only be configured if certificates are loaded.

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 be able to use IP address transmission via ISDN, you will need a free additional license.

You can obtain this license from your sales partner or from our support.

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 329. 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
Mode	Select the Callback Mode. Possible values: • *Inactive* (default value): IPSec callback is deactivated. The local device neither reacts to incoming ISDN calls nor initiates ISDN calls to the remote device. • *Passive*: 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. • *Active*: The local device sends an ISDN call to the remote device to cause this to set up an IPSec tunnel. The device

Field	Description
	does not react to incoming ISDN calls. • *Both*: Your device can react to incoming ISDN calls and send ISDN calls to the remote device. The setting up of an IPSec tunnel is executed (after an incoming ISDN call) and initiated (by an outgoing ISDN call).
Incoming Phone Number	Only for **Mode** = *Passive* or *Both* Enter the ISDN number from which the remote device calls the local device (calling party number). Wildcards may also be used.
Outgoing Phone Number	Only for **Mode** = *Active* or *Both* Enter the ISDN number with which the local device calls the remote device calls (called party number). Wildcards may also be used.
Transfer own IP address over ISDN/GSM	Select whether the IP address of your own device is to be transferred over ISDN for IPSec callback. The function is enabled with *Enabled*. The function is disabled by default.
Transfer Mode	Only for **Transfer own IP address over ISDN/GSM** = enabled Select the mode in which your device is to attempt to transfer its IP address to the peer. Possible values: • *Autodetect best mode*: 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.) • *Autodetect only D Channel Modes*: Your device automatically determines the most favourable D channel mode. The use of the B channel is excluded. • *Use specific D Channel Mode*: Your device tries to transfer the IP address in the mode set in the **Mode** field. • *Try specific D Channel Mode, fall back to B Channel*: Your device tries to transfer the IP address in the

Field	Description
	mode set in the **Mode** field. If this does not succeed, the IP address is transferred in the B channel. (This incurs costs.) • *Use only B Channel Mode*: Your device transfers the IP address in the B channel. This incurs costs.
D Channel Mode	Only for **Transfer Mode** = *Use specific D Channel Mode* or *Try specific D Channel Mode, fall back to B Channel* Select the D channel mode in which your device tries to transfer the IP address. Possible values: • *LLC* (default value): The IP address is transferred in the "LLC information elements" of the D channel. • *SUBADDR*: The IP address is transferred in the subaddress "information elements" of the D channel. • *LLC and SUBADDR*: The IP address is transferred in both the "LLC" and "subaddress information elements".

14.1.2 Phase-1 Profiles

A list of all configured tunnel profiles is displayed in the **VPN**->**IPSec**->**Phase-1 Profiles** menu.

In the **Default** column, you can mark the profile to be used as the default profile.

14.1.2.1 New

Choose the **Create new IKEv1 Profile** or **Create new IKEv2 Profile** button to create additional profiles.

The menu **VPN**->**IPSec**->**Phase-1 Profiles**->**Create new IKEv1 Profile** consists of the following fields:

Fields in the Phase-1 (IKE) Parameters / Phase-1 (IKEv2) Parameters menu.

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	In this field, you can select any combination of encryption and

Field	Description
	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. Encryption algorithms (**Encryption**): • *3DES*: 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. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. • *AES* (default value): 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 *AES* , a key length of 128 bits is used. • *AES-128*: 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. • *AES-192*: 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. • *AES-256*: 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. Hash algorithms (**Authentication**): • *MD5*: MD5 (Message Digest #5) is an older hash algorithm. It

Field	Description
	is used with a 96 bit digest length for IPSec. • *SHA1* (default value): 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. • *RipeMD 160*: RipeMD 160 is a 160 bit hash algorithm. It is used as a secure replacement for MD5 and RipeMD. • *Tiger192*: Tiger 192 is a relatively new and very fast algorithm. • *SHA2-256*: 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. • *SHA2-384*: SHA-2 with 384 bit hash length. • *SHA2-512*: SHA-2 with 512 bit hash length. Depending on the hardware of your device some options may not be available. Please note that the quality of the algorithms is subject to relative aspects and may change due to mathematical or cryptographic developments.
DH Group	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". The following groups with their corresponding bit values are available: • *1(768 Bit)* • *2(1024 Bit)* • *5(1536 Bit)* • *14(2048 Bit)* • *15(3072 Bit)* • *16(4096 Bit)* Depending on the hardware of your device some options may not be available.
Lifetime	Create a lifetime for phase 1 keys.

Field	Description
	The following options are available for defining the **Lifetime**: • Input in **Seconds**: Enter the lifetime for phase 1 key in seconds. The value can be a whole number from 0 to 2147483647. The default value is *14400*, which means the key must be renewed once four hours have elapsed. • Input in **kBytes**: Enter the lifetime for phase 1 keys as amount of data processed in kBytes. The value can be a whole number from 0 to 2147483647. The default value is *0*, which means that the number of transmitted kBytes is irrelevant.
Authentication Method	Only for **Phase-1 (IKE) Parameters** Select the authentication method. Possible values: • *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **VPN**->**IPSec**->**IPSec Peers**. The preshared key is the shared password. • *DSA Signature*: Phase 1 key calculations are authenticated using the DSA algorithm. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm. • *RSA Encryption*: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	Only for **Phase-1 (IKE) Parameters** Only for **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* 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.
Mode	Only for **Phase-1 (IKE) Parameters** Select the phase 1 mode.

Field	Description
	Possible values: • *Aggressive* (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. • *Main Mode (ID Protect)*: This mode (also designated Main Mode) requires six messages for a Diffie-Hellman key calculation and thus for configuring a secure channel, over which the IPSec SAs can be negotiated. A condition is that both peers have static IP addresses if preshared keys are used for authentication. Also define whether the selected mode is used exclusively (**Strict**), or the peer can also propose another mode.
Local ID Type	Only for **Phase-1 (IKE) Parameters** Select the local ID type. Possible values: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *Key ID*
Local ID Value	Only for **Phase-1 (IKE) Parameters** Enter the ID of your device. For **Authentication Method** = *DSA Signature* or *RSA Signature* the option **Use Subject Name from certificate** is displayed. When you enable the option **Use Subject Name from certificate**, the subject name indicated in the certificate is used.

Alive Check

During communication between two IPSec peers, one of the peers may become unavailable, e.g. due to routing problems or a reboot. However, this can only be detected when

the end of the lifetime of the security connection is reached. Up until this point the data packets are lost. These are various methods of performing an alive check to prevent this happening. In the **Alive Check** field you can specify whether a method should be used to check the availability of a peer.

Two methods are available: Heartbeats and Dead Peer Detection.

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

Fields in the Advanced Settings menu.

Field	Description
Alive Check	Only for **Phase-1 (IKE) Parameters** Select the method to be used to check the functionality of the IPSec connection. 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. Possible values: • *Autodetect* (default value): Your device detects and uses the mode supported by the remote terminal. • *Inactive*: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Heartbeats (Send only)*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (Send &Expect)*: Your device expects a heartbeat from the peer and sends one itself. • *Dead Peer Detection*: 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. • *Dead Peer Detection (Idle)*: 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 op-

Field	Description
	tion is used to carry out a check at certain intervals depending on forthcoming data transfers.  **Note** As the two methods of accessibility testing use different procedures, it is not recommended to use them in combination in Phase 1 and Phase 2. In Phase 2 only heartbeats are supported, so they should be deactivated if Dead Peer Detection is required in Phase 1. Only for **Phase-1 (IKEv2) Parameters** Enable or disable alive check. The function is enabled by default.
Block Time	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. Possible values are `-1` to `86400` (seconds); `-1` means the value in the default profile is used and `0` means that the peer is never blocked. The default value is `30`. If a peer has been configured in "always up" mode, there is an implicit minimum block time of 15 seconds which is aplied independently from the configured value.
NAT Traversal	NAT Traversal (NAT-T) also enables IPSec tunnels to be opened via one or more devices on which network address translation (NAT) is activated. 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. Only for `IKEv1 profiles`

Field	Description
	Possible values: • *Enabled* (default value): NAT Traversal is enabled. • *Disabled*: NAT Traversal is disabled. • *Force*: The device always behaves as it would if NAT were in use. Only for *IKEv2 profiles* The function is enabled with *Enabled*. The function is enabled by default.
CA Certificates	Only for **Phase-1 (IKE) Parameters** Only for **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* If you enable the **Trust the following CA certificates** option, you can select up to three CA certificates that are accepted for this profile. This option can only be configured if certificates are loaded.

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.

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.

The menu **VPN**->**IPSec**->**Phase-2 Profiles**->**New** consists of the following fields:

Fields in the Phase-2 (IPSEC) Parameters menu.

Field	Description
Description	Enter a description that uniquely identifies the profile.

Field	Description
	The maximum length of the entry is 255 characters.
Proposals	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. Encryption algorithms (**Encryption**): • *3DES*: 3DES is an extension of the DES algorithm with an effective key length of 112 bits, which is rated as secure. It is the slowest algorithm currently supported. • *-- ALL --*: All options can be used. • *AES* (default value): 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 *AES* , a key length of 128 bits is used. • *AES-128*: 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. • *AES-192*: 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. • *AES-256*: 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. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits.

Field	Description
	Hash algorithms (**Authentication**): • *MD5*: MD5 (Message Digest #5) is an older hash algorithm. It is used with a 96 bit digest length for IPSec. • *-- ALL --*: All options can be used. • *SHA1* (default value): 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. • *SHA2-256*: 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. • *SHA2-384*: SHA-2 with 384 bit hash length. • *SHA2-512*: SHA-2 with 512 bit hash length. Note that RipeMD 160 and Tiger 192 are not available for message hashing in phase 2. Depending on the hardware of your device some options may not be available.
Use PFS Group	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 (*Enabled*), the options are the same as for the configuration of **DH Group** in the **VPN**->**IPSec**->**Phase-1 Profiles** 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. The following groups with their corresponding bit values are available: • *1(768 Bit)* • *2(1024 Bit)* • *5(1536 Bit)* • *14(2048 Bit)* • *15(3072 Bit)* • *16(4096 Bit)* Depending on the hardware of your device some options may not be available.

Field	Description
Lifetime	Define how the lifetime is defined that will expire before phase 2 SAs need to be renewed. 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. The following options are available for defining the **Lifetime**: • Input in **Seconds**: Enter the lifetime for phase 2 key in seconds. The value can be a whole number from *0* to *2147483647*. The default value is *7200*. • Input in **kBytes**: Enter the lifetime for phase 2 keys as amount of data processed in kBytes. The value can be a whole number from *0* to *2147483647*. The default value is *0*. **Rekey after**: Specify the percentage in the course of the lifetime at which the phase 2 keys are to be regenerated. The percentage entered is applied to both the lifetime in seconds and the lifetime in kBytes. The default value is *80* %.

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

Fields in the Advanced Settings menu.

Field	Description
IP Compression	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. The function is enabled with *Enabled*. The function is disabled by default.
Alive Check	Select whether and how IPSec heartbeats are used. A bintec elmeg IPSec heartbeat is implemented to determine

Field	Description
	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. Possible values: • *Autodetect* (default value): Automatic detection of whether the remote terminal is a bintec elmeg device. If it is, *Heartbeats (Send &Expect)* (for a remote terminal with bintec elmeg) or *Inactive* (for a remote terminal without bintec elmeg) is set. • *Inactive*: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Heartbeats (Send only)*: Your device expects no heartbeat from the peer, but sends one itself. • *Heartbeats (Send &Expect)*: Your device expects a heartbeat from the peer and sends one itself.  **Note** In Phase 1 and Phase 2, your device supports different methods of accessibility testing: In Phase 1, dead peer detection and heartbeats, in Phase 2 only heartbeats. Since the two methods of accessibility testing use different procedures, it is not recommended to combine them in Phase 1 and Phase 2. Heartbeats should therefore be deactivated in Phase 2 if Dead Peer Detection is required in Phase 1.
Propagate PMTU	Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. The function is enabled with *Enabled*. The function is enabled by default.

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. Multiple users can dial-in either one after another or simultaneously via a so-called multi peer. 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, for example, one peer for each branch. A password is assigned to each peer, i.e. each branch. Besides this authentication method per branch, XAuth offers an additional method for logging in individually and independently from a user's location via a private password. A specific user can then use the IPSec tunnel across various peers. This is useful, for example, if an employee works alternately in different branches and if he needs to have individual access to the tunnel.

All users are assigned the same password in a so-called multi peer, i.e. a group password. Here, XAuth offers an individual authentication method to the user, too. If in a branch, for example, multiple users have access to a tunnel via a multi peer, it may have an adventage for users with different tasks that each of them uses a private password.

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.

The **VPN**->**IPSec**->**XAUTH Profiles**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for this XAuth profile. You can create up to 10 XAuth profiles with **Role** = *Server* and **Mode** = *Local* or **Role** = *Client* settings (see below).
Role	Select the role of the gateway for XAuth authentication. Possible values: • *Server* (default value): The gateway requires a proof of authorisation. • *Client*: The gateway provides proof of authorisation.
Mode	Only for **Role** = *Server* Select how authentication is carried out. Possible values: • *RADIUS* (default value): Authentication is carried out via a Radius server. It is configured in the **System Management**->**Remote Authentication**->**RADIUS** menu and selected in the **RADIUS Server Group ID** field. • *Local*: Authentication is carried out via a local list.
Name	Only for **Role** = *Client* Enter the authentication name of the client.
Password	Only for **Role** = *Client* Enter the authentication password.
RADIUS Server Group ID	Only for **Role** = *Server* Select the desired list in **System Management**->**Remote Authentication**->**RADIUS** configured RADIUS group.
Users	Only for **Role** = *Server* and **Mode** = *Local* 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 (**Name**) and the

Field	Description
	authentication password (**Password**). Add new members with **Add**. There is no limitation for users per XAuth profile.

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.

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

14.1.6 Options

The menu **VPN**->**IPSec**->**Options** consists of the following fields:

Fields in the Global Options menu.

Field	Description
Enable IPSec	Select whether you want to activate IPSec. The function is enabled with *Enabled*.

Field	Description
	The function is active as soon as an IPSec Peer is configured.
Delete complete IPSec configuration	If you click the icon, delete the complete IPSec configuration of your device. This cancels all settings made during the IPSec configuration. Once the configuration is deleted, you can start with a completely new IPSec configuration. You can only delete the configuration if **Enable IPSec** = not activated.
IPSec Debug Level	Select the priority of the syslog messages of the IPSec subsystem to be recorded internally. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* • *Debug* (default value, lowest priority) 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".

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other bintec elmeg devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

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

Fields in the Advanced Settings menu.

Field	Description
IPSec over TCP	Determine whether IPSec over TCP is to be used. 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. The function is enabled with *Enabled*. The function is disabled by default.
Send Initial Contact Message	Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist. The function is enabled with *Enabled*. The function is enabled by default.
Sync SAs with ISP interface state	Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from *Up* to *Down*, *Dormant* or *Blocked*. The function is enabled with *Enabled*. The function is disabled by default.
Use Zero Cookies	Select whether zeroed ISAKMP Cookies are to be sent. 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 *Enabled*.
Zero Cookie Size	Only for **Use Zero Cookies** = enabled. Enter the length in bytes of the zeroed SPI used in IKE proposals. The default value is *32*.
Dynamic RADIUS Authentication	Select whether RADIUS authentication is to be activated via IPSec. The function is enabled with *Enabled*.

Field	Description
	The function is disabled by default.

Fields in the PKI Handling Options menu.

Field	Description
Ignore Certificate Request Payloads	Select whether certificate requests received from the remote end during IKE (phase 1) are to be ignored. The function is enabled with *Enabled*. The function is disabled by default.
Send Certificate Request Payloads	Select whether certificate requests are to be sent during IKE (phase 1). The function is enabled with *Enabled*. The function is enabled by default.
Send Certificate Chains	Select whether complete certificate chains are to be sent during IKE (phase 1). The function is enabled with *Enabled*. 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).
Send CRLs	Select whether CRLs are to be sent during IKE (phase 1). The function is enabled with *Enabled*. The function is disabled by default.
Send Key Hash Payloads	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 *Enabled* to suppress 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.

The menu **VPN**->**L2TP**->**Tunnel Profiles**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the current profile. The device automatically names the profiles *L2TP* and numbers them, but the value can be changed.
Local Hostname	Enter the host name for LNS or LAC. • *LAC*: 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. • *LNS*: Is the same as the value for **Remote Hostname** of the

Field	Description
	incoming tunnel setup message from the LAC.
Remote Hostname	Enter the host name of the LNS or LAC. • *LAC*: Defines the value for **Local Hostname** of the LNS (contained in the SCCRQs received from the LNS and the SCCRPs received from the LAC). A **Local Hostname** configured in the LAC must match **Remote Hostname** configured for the intended profile in the LNS and vice versa. • *LNS*: Defines the **Local Hostname** of the LAC. If the **Remote Hostname** field remains empty on the LNS, the related profile qualifies as the standard entry and is used for all incoming calls for which a profile with a matching remote hostname cannot be found.
Password	Enter the password to be used for tunnel authentication. Authentication between LAC and LNS takes place in both directions, i.e. the LNS checks the **Local Hostname** and the **Password**contained in the SCCRQ of the LAC and compares them with those specified in the relevant profile. The LAC does the same with the fields of the SCCRP of the LNS. If this field remains empty, authentication data in the tunnel setup messages are not sent and are ignored.

Fields in the LAC Mode Parameters menu.

Field	Description
Remote IP Address	Enter the fixed IP address of the LNS used as the destination address for connections based on this profile. The destination must be a device that can behave like an LNS.
UDP Source Port	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. By default, the **Fixed** option is disabled, which means that ports are dynamically assigned to the connections that use this profile. If you want to enter a fixed port, enable the *Fixed* option. Select this option if you encounter problems with the firewall or NAT.

Field	Description
	The available values are `0` to `65535`.
UDP Destination Port	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. Possible values are `0` to `65535`. The default value is `1701` (RFC 2661).

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

Fields in the Advanced Settings menu.

Field	Description
Local IP Address	Enter the IP address to be used as the source address for all L2TP connections based on this profile. 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.
Hello Intervall	Enter the interval (in seconds) between the sending of two L2TP HELLO messages. These messages are used to keep the tunnel open. The available values are `0` to `255`, the default value is `30`. The value `0` means that no L2TP HELLO messages are sent.
Minimum Time between Retries	Enter the minimum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The wait time is dynamically extended until it reaches the **Maximum Time between Retries**. The available values are `1` to `255`, the default value is `1`.
Maximum Time between Retries	Enter the maximum time (in seconds) that your device waits before resending a L2TP control packet for which it received no response. The available values are `8` to `255`, the default value is `16`.
Maximum Retries	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*.
Data Packets Sequence Numbers	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 *Enabled*. 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.

The menu **VPN**->**L2TP**->**Users**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a name for uniquely identifying the L2TP partner. 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.
Connection Type	Select whether the L2TP partner is to take on the role of the L2TP network server (LNS) or the functions of a L2TP access concentrator client (LAC client). Possible values: • *LNS* (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. • *LAC*: 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.

Field	Description
Tunnel Profile	Only for **Connection Type** = *LAC* Select a profile created in the **Tunnel Profile** menu for the connection to this L2TP partner.
User Name	Enter the code of your device.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** is disabled Enter the idle time in seconds for static short hold. The static short hold setting determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the short hold. The default value is *300*.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Static* (default value): You enter a static IP address. • *Provide IP Address*: Only for **Connection Type** = *LNS*. Your device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Only for **Connection Type** = *LAC*. Your device is dynamically assigned an IP address.
Default Route	Only for **IP Address Mode** = *Get IP Address* and *Static*

Field	Description
	Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Create NAT Policy	Only for **IP Address Mode** = *Get IP Address* and *Static* Specify whether Network Address Translation (NAT) is to be activated for this connection. The function is enabled with *Enabled*. The function is disabled by default.
IP Assignment Pool (IPCP)	Only for **IP Address Mode** = *Provide IP Address* Select an IP pool configured in the **WAN**->**Internet + Dialup**->**IP Pools** menu.
Local IP Address	Only for **IP Address Mode** = *Static* Enter the WAN IP address of your device.
Route Entries	Only for **IP Address Mode** = *Static* Enter **Remote IP Address** and **Netmask** of the LANs for L2TP partners and the corresponding **Metric**. Add new entries with **Add**.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Authentication	Select the authentication protocol for this L2TP partner.

Field	Description
	Possible values: • *PAP/CHAP/MS-CHAP* (default value): Primarily run CHAP, on denial, the authentication protocol required by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *PAP*: Only run PAP (PPP Password Authentication Protocol); the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *MS-CHAPv2*: Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
Encryption	If necessary, select the type of encryption that should be used for data traffic to the L2TP partner. This is only possible if STAC or MS-STAC compression is not activated for the connection. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None*: MPP encryption is not used. • *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
LCP Alive Check	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. The function is enabled with *Enabled*. The function is enabled by default.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially

Field	Description
	applied for asymmetrical bandwidths (ADSL). The function is enabled with *Enabled*. The function is disabled by default.

Fields in the IP Options menu.

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are sent. Possible values: • *Passive* (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. • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific L2TP partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this L2TP partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the L2TP partner is *Up* (active) or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the L2TP partner is *Up* (active), i.e. a connection already exists to the L2TP partner.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** und **Secondary DNS Server** and **WINS Server Primary** and **Secondary** from the L2TP partner or sends these to the L2TP partner.

Field	Description
	The function is enabled with *Enabled*. The function is enabled by default.

14.2.3 Options

The menu **VPN**->**L2TP**->**Options** consists of the following fields:

Fields in the Global Options menu.

Field	Description
UDP Destination Port	Enter the port to be monitored by the LNS on incoming L2TP tunnel connections. Available values are all whole numbers from *1* to *65535*, the default value is *1701*, as specified in RFC 2661.
UDP Source Port Selection	Select whether the LNS should only use the monitored port (**UDP Destination Port**) as the local source port for the L2TP connection. The function is enabled with *Fixed*. The function is disabled by default.

14.3 PPTP

The Point-to-Point Tunnelling Protocol (=PPTP) can be used to set up an encrypted PPTP tunnel to provide security for data traffic over an existing IP connection.

First a connection to an ISP (=Internet Service Provider) is set up at both sites. Once these connections are available, a tunnel is set up to the PPTP partner over the Internet using PPTP.

The PPTP subsystem sets up a control connection between the endpoints of the tunnel. This is used to send control data to set up, keep alive and terminate the connection between the two PPTP tunnel end-points. As soon as this control connection is set up, the PPTP transfers the traffic data packed in GRE packets (GRE = Generic Routing Encapsulation).

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.

The **VPN**->**PPTP**->**PPTP Tunnels**->**New** menu consists of the following fields:

Fields in the PPTP Partner Parameters menu.

Field	Description
Description	Enter a unique name for the tunnel. The first character in this field must not be a number No special characters or umlauts must be used.
PPTP Mode	Enter the role to be assigned to the PPTP interface. Possible values: • *PNS* (default value): this assigns the PPTP interface the role of PPTP server. • *Windows Client Mode*: This assigns the PPTP interface the role of PPTP client.
User Name	Enter the user name.
Password	Enter the password.
Always on	Select whether the interface should always be activated. The function is enabled with *Enabled*. The function is disabled by default.
Connection Idle Timeout	Only if **Always on** 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*.

Field	Description
	Example: *10* for FTP transmission, *20* for LAN-to-LAN transmission, *90* for Internet connections.
Remote PPTP IP Address	Only for **PPTP Mode** = *PNS* Enter the IP address of the PPTP partner.
Remote PPTP IP AddressHost Name	Only for **PPTP Mode** = *Windows Client Mode* Enter the IP address of the PPTP partner.

Fields in the IP Mode and Routes menu.

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Static* (default value): You enter a static IP address. • *Provide IP Address*: Only for **PPTP Mode** = *PNS*: Your device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Only for **PPTP Mode** = *Windows Client Mode*: Your device is dynamically assigned an IP address.
Default Route	Only if **IP Address Mode** = *Static* Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Create NAT Policy	Only if **IP Address Mode** = *Static* When you configure an PPTP connection, specify whether Network Address Translation (NAT) is to be enabled. The function is enabled with *Enabled*. The function is disabled by default.

Field	Description
Local IP Address	Only for **IP Address Mode** = *Static* Assign the IP address from your LAN to the PPTP interface which is to be used as your device's internal source address.
Route Entries	Only if **IP Address Mode** = *Static* Define routing entries for this connection partner. • *Remote IP Address*: IP address of the destination host or LAN. • *Netmask*: Netmask for **Remote IP Address** • *Metric*: The lower the value, the higher the priority of the route (possible values *0...15*). The default value is *1*.
IP Assignment Pool (IPCP)	Only if **PPTP Mode** = *PNS*, **IP Address Mode** = *Provide IP Address* Select a IP pool configured in the **VPN**->**PPTP**->**IP Pools** menu.

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

Fields in the Advanced Settings menu.

Field	Description
Block after connection failure for	Enter the wait time in seconds before the device should try again after an attempt to set up a connection has failed. The default value is *300*.
Usage Type	If necessary, select a special interface use. Possible values: • *Standard* (default value): No special type is selected. • *Multi-User (Dialin only)*: The interface is defined as multi-user connection partner, i.e. several clients dial in with the same user name and password.
Authentication	Select the authentication protocol for this PPTP partner. Possible values: • *PAP*: Only run PAP (PPP Password Authentication Protocol);

Field	Description
	the password is transferred unencrypted. • *CHAP*: Only run CHAP (PPP Challenge Handshake Authentication Protocol as per RFC 1994); password is transferred encrypted. • *PAP/CHAP*: Primarily run CHAP, otherwise PAP. • *MS-CHAPv1*: Only run MS-CHAP version 1 (PPP Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP*: Give priority to CHAP, if refused use the authentication protocol requested by the PPTP partner. (MSCHAP version 1 or 2 possible.) • *MS-CHAPv2* (default value): Run MS-CHAP version 2 only. • *None*: Some providers use no authentication. In this case, select this option.
Encryption	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If **Encryption** is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None*: MPP encryption is not used. • *Enabled* (default value): MPP encryption V2 with 128 bit is used to RFC 3078. • *Windows compatible*: MPP encryption V2 with 128 bit is used as compatible with Microsoft and Cisco.
Compression	If necessary, select the type of encryption that should be used for data traffic to the connection partner. If encryption is set, the remote terminal must also support it, otherwise a connection cannot be set up. Possible values: • *None* (default value): Encryption is not used. • *STAC* • *MS-STAC* • *MPPC*: Microsoft Point-to-Point Compression
LCP Alive Check	Select whether the availability of the remote terminal is to be

Field	Description
	checked by sending LCP echo requests or replies. This is recommended for leased lines, PPTP and L2TP connections. The function is enabled with *Enabled*. The function is enabled by default.

Fields in the IP Options menu.

Field	Description
OSPF Mode	Select whether and how routes are propagated via the interface and/or OSPF protocol packets are to be sent. Possible values: • *Passive* (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. • *Active*: OSPF is activated for this interface, i.e. routes are propagated or OSPF protocol packets sent over this interface. • *Inactive*: OSPF is disabled for this interface.
Proxy ARP Mode	Select whether your device is to answer APR requests from your LAN on behalf of the specific PPTP partner. Possible values: • *Inactive* (default value): Disables Proxy-ARP (Address Resolution Protocol) for this PPTP partner. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the PPTP partner is *Up* (active) or *Dormant*. In the case of *Idle*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device answers an APR request only if the status of the connection to the PPTP partner is *Active*, i.e. if a connection to the PPTP partner has already been established.
DNS Negotiation	Select whether your device receives IP addresses for **Primary DNS Server** and **Secondary DNS Server** from the PPTP part-

Field	Description
	ner or sends these to the PPTP partner. The function is enabled with *Enabled*. The function is enabled by default.

Fields in the PPTP Callback menu.

Field	Description
Callback	Enables a PPTP tunnel through the Internet to be set up with a PPTP partner, even if the partner is currently inaccessible. As a rule, the PPTP partner will be requested by means of an ISDN call to go online and set up a PPTP connection. The function is enabled with *Enabled*. The function is disabled by default. 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.
Incoming ISDN Number	Only if **Callback** is enabled. Enter the ISDN number from which the remote device calls the local device (calling party number).
Outgoing ISDN Number	Only if **Callback** is enabled. Enter the ISDN number with which the local device calls the remote device calls (called party number).

Fields in the Dial Port Selection (only if callback = activated)

Field	Description
Selected Ports	Enter the ISDN port over which callback is carried out. Possible values: • *All Ports*: The callback is routed over an available ISDN port. • *Specify port*: In **Specific Ports** You can select the required ISDN port.
Specific Ports	Only for **Selected Ports** = *Specify port*, you can select additional ports with **Add**.

14.3.2 Options

In this menu, you can make general settings of the global PPTP profile.

The **VPN**->**PPTP**->**Options**menu consists of the following fields:

Fields in the Global Options menu.

Field	Description
GRE Window Adaption	Select whether the GRE Window Adaptation is to be enabled. 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. The function is enabled with *Enabled*. The function is enabled by default.
GRE Window Size	Enter the maximum number of GRE packets that can be sent without confirmation. Windows XP uses a higher initial reception window in the GRE, which is why the maximum send window size must be adjusted here by the **GRE Window Size** value. Possible values are *0* to *256*. The default value is *0*.
Max. incoming control connections per remote IP Address	Enter the maximum number of control connections.

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.

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

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.

The **VPN**->**GRE**->**GRE Tunnels**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE partner. If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.
Remote GRE IP Address	Enter the target IP address of the GRE packets to the GRE partner.
Default Route	If you enable the **Default Route**, all data is automatically routed to one connection. The function is disabled by default.
Local IP Address	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.
Route Entries	Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.

Field	Description
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners. Possible values are *1* to *8192*. The default value is *1500*.
Use key	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). The identification is enabled with *Enabled* The function is disabled by default.
Key Value	Only if **Use key** is enabled. Enter the GRE connection key. Possible values are *0* to *2147483647*. The default value is *0*.

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).

Specific instructions for the configuration of Stateful Inspection Firewall (SIF), see the end of the chapter *Configuration* on page 382.

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.

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

Note

Informationen on the selection of Trusted Interfaces can be found here: *IPv4 Filter Rules* on page 370.

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

The menu **Firewall**->**Policies**+**IPv4 Filter Rules**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Source	Select one of the preconfigured aliases for the source of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**Groups**), addresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available. The value *Any* means that neither the source interface nor the source address is checked.
Destination	Select one of the preconfigured aliases for the destination of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**Groups**), addresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**). The value *Any* means that neither the destination interface nor the destination address is checked.
Service	Select one of the preconfigured services to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* • *Internet* • *Netmeeting* Additional services are created in **Firewall**->**Services**->**Service List**.

Field	Description
	In addition, the service groups configured in **Firewall**->**Services**->**Groups** can be selected.
Action	Select the action to be applied to a filtered packet. Possible values: • *Access* (default value): The packets are forwarded on the basis of the entries. • *Deny*: The packets are rejected. • *Reject*: The packets are rejected. An error message is issued to the sender of the packet.

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.

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.

The menu **Firewall**->**Policies**->**IPv6 Filter Rules**->**New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Source	Select one of the preconfigured aliases for the source of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**IPv6 Groups**), adresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available for selection for IPv6.
Destination	Select one of the preconfigured aliases for the destination of the packet. In the list, all WAN/LAN interfaces, interface groups (see **Firewall**->**Interfaces**->**IPv6 Groups**), addresss (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available for selection for IPv6.
Service	Select one of the preconfigured services to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* Additional services are created in **Firewall**->**Services**->**Service List**.

Field	Description
	In addition, the service groups configured in **Firewall**->**Services**->**Groups** can be selected.
Action	Select the action to be applied to a filtered packet. Possible values: • *Access* (default value): The packets are forwarded on the basis of the entries.. • *Deny* : The packets are rejected. • *Reject* : The packets are rejected. An error message is issued to the sender of the packet.

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.

The menu **Firewall**->**Policies**->**Options** consists of the following fields:

Fields in the Global Firewall Options menu

Field	Description
IPv4 Firewall Status	Enable or disable the IPv4 firewall function. The function is enabled with *Enabled* The function is enabled by default.
Logged Actions	Select the firewall syslog level. The messages are output together with messages from other subsystems. Possible values: • *All* (default value): All firewall activities are displayed. • *Deny*: Only reject and deny events are shown, see "Action". • *Accept*: Only accept events are shown.

Field	Description
	• *None*: Syslog messages are not generated.
IPv4 Full Filtering	With TCP sessions, the SIF first verifies if a session has been established completely and correctly. Incomplete sessions will be blocked. The filtering itself is carried out in a second step. The default setting **IPv4 Full Filtering** has been designed to meet this "standard" case. If - in a two-way communication - one traffic direction is sent through the router, but the counter direction takes a different route, the session is interpreted as "incomplete" by the SIF, and the data traffic of this connection will be blocked by the router. In order to allow the data traffic of such "incomplete" sessions in the special case of identical source and destination interface you have to disable **IPv4 Full Filtering**. SIF rules for this data traffic will be ignored.
STUN Handler	Enable this option if you intend to allow network devices (esp. SIP clients) to use STUN in order to identify the network address translation mode and the public IP address. The firewall creates temporary rules that allow RTP data traffic for SIP phone calls.
Port STUN server	Only for **STUN Handler**= Enabled Enter the number of the port to be used for the connection to the STUN server. The default value is 3478. A 5 digit sequence isd possible.

Fields in the Session Timer menu.

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP Inactivity	Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*.

Field	Description
	The default value is *3600*.
PPTP Inactivity	Enter the inactivity time after which a PPTP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *86400*.
Other Inactivity	Enter the inactivity time after which a session of another type is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *30*.

Fields in the Factory Reset Firewall

Field	Description
Factory Reset Firewall	Click **Reset** 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.

The menu **Firewall**->**Interfaces**->**IPv4 Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the IPv4 interface group.

Field	Description
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Selection** 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 menu **Firewall**->**Interfaces**->**IPv6 Groups**->**New** consists of the following fields

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the IPv6 interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Selection** 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.

The menu **Firewall**->**Addresses**->**Address List**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address.
IPv4	Allows configuration of IPv4 address lists. The function is enabled with *Enabled*. The function is enabled by default.
Address Type	Only for **IPv4** = *Enabled* Select the type of address you want to specify. Possible values: • *Address / Subnet* (default value): Enter an IP address with subnet mask. • *Address Range*: Enter an IP address range with a start and end address.
Address / Subnet	Only for **IPv4** = *Enabled* and **Address Type** = *Address / Subnet* Enter the IP address of the host or a network address and the related netmask. The default value is *0.0.0.0*.
IPv6	Allows configuration of IPv6 address lists. The function is enabled with *Enabled*. The function is disabled by default.
Address / Prefix	Only for **IPv6** = *Enabled* 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.

The menu **Firewall**->**Addresses**->**Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the address group.
IP Version	Select the IP version used. Possible values: • *IPv4* • *IPv6* *IPv4* is selected by default.
Selection	Select the members of the group from the available **Addresses**. To do this, activate the Fields in the **Selection** column.

15.4 Services

15.4.1 Service List

In the **Firewall**->**Services**->**Service List** menu, a list of all available services is displayed. Choose the icon to edit existing entries. You can delete existing entries with the icon .

Note

Service is also removed from NAT service list! Recreation possible only by factory reset.

15.4.1.1 New

Choose the **New** button to set up additional services.

The menu **Firewall**->**Services**->**Service List**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter an alias for the service you want to configure.
Protocol	Select the protocol on which the service is to be based. The most important protocols are available for selection.
Destination Port Range	Only for **Protocol** = *TCP*, *UDP/TCP* or *UDP* In the first field, enter the destination port via which the service is to run. 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. Possible values are *1* to *65535*.
Source Port Range	Only for **Protocol** = *TCP*, *UDP/TCP* or *UDP* In the first field, enter the source port to be checked, if applicable. 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. Possible values are *1* to *65535*.
Type	Only for **Protocol** = *ICMP* The **Type** field shows the class of ICMP messages, the **Code** field specifies the type of message in greater detail. Possible values: • *Any* (default value) • *Echo Reply* • *Destination unreachable* • *Source Quench*

Field	Description
	• *Redirect* • *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	Selection options for the ICMP codes are only available for **Type** = *Destination unreachable* Possible values: • *Any* (default value) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable* • *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

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.

The menu **Firewall**->**Services**->**Groups**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the desired description of the service group.
Members	Select the members of the group from the available service aliases. To do this, activate the Fields in the **Selection** column.

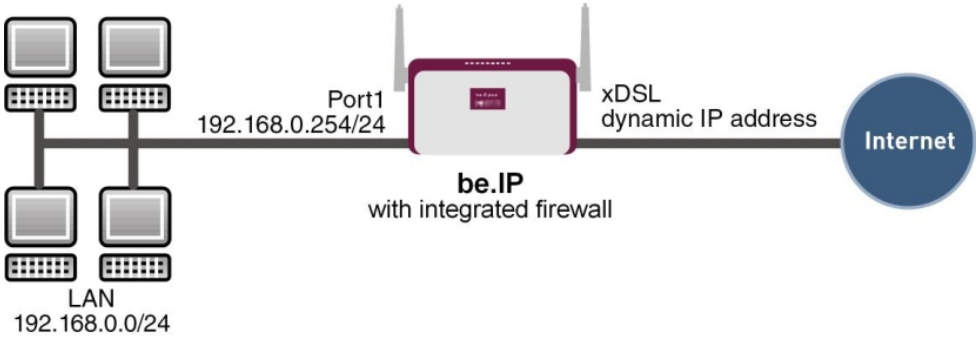
15.5 Configuration

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 established 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. *Administrator*
Address Type	**Firewall ->Addresses-> Address List ->New**	*Address / Subnet*
Address / Subnet	**Firewall-> Addresses ->Address List-> New**	e.g. *192.168.0.2* with *255.255.255.255*
Description	**Firewall-> Addresses ->Address List ->New**	e.g. *Director*
Address Type	**Firewall-> Addresses ->Address List-> New**	*Address / Subnet*
Address / Subnet	**Firewall ->Addresses-> Address List ->New**	e.g. *192.168.0.3* with *255.255.255.255*
Description	**Firewall-> Addresses ->Address List-> New**	e.g. *be.IP*
Address Type	**Firewall-> Addresses ->Address List ->New**	*Address / Subnet*
Address / Subnet	**Firewall-> Addresses ->Address List-> New**	e.g. *192.168.0.254* with *255.255.255.255*
Description	**Firewall ->Addresses-> Address List ->New**	e.g. *Network Internal*

Field	Menu	Value
Address Type	**Firewall-> Addresses ->Address List-> New**	*Address / Subnet*
Address / Subnet	**Firewall-> Addresses ->Address List ->New**	e.g. *192.168.0.0* with *255.255.255.0*

Address groups

Field	Menu	Value
Description	**Gro** **Firewall->Addresses->ups->New**	e.g. *be.IP*
IP Version	**Gro** **Firewall->Addresses->ups->New**	*IPv4*
Selection	**Gro** **Firewall->Addresses->ups->New**	e.g. *Administrator* and *Director*

Service Sets

Field	Menu	Value
Description	**Group** **Ne** **Firewall->Services->s->w**	e.g. *Internet Ports*
Members	**Group** **Ne** **Firewall->Services->s->w**	e.g. *http*, *http (SSL)* and *ftp*
Description	**Group** **Ne** **Firewall->Services->s->w**	e.g. *Administration Ports*
Members	**Group** **Ne** **Firewall->Services->s->w**	e.g. *http* and *telnet*

Filter rules 1: Manage Gateway (System administrator)

Field	Menu	Value
Source Location	**Firewall ->Policies ->IPv4 Filter Rules-> New**	*be.IP*
Destination	**Firewall-> Policies ->IPv4 Filter Rules-> New**	*be.IP*

Field	Menu	Value
Service	**Firewall ->Policies ->IPv4 Filter Rules-> New**	*Administration Ports*
Action	**Firewall-> Policies ->IPv4 Filter Rules-> New**	*Access*

Filter rules 2: Use gateway as DNS proxy

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*LOCAL*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*ANY*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*dns*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Access*
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*Netzwerk_Intern*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*be.IP*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*dns*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Access*

Filter rules 3: Deny access from outside to the Gateway

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*ANY*
Destination	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*be.IP*
Service	**Firewall ->Policie s->IPv4 Filter Rules-> New**	*any*
Action	**Firewall-> Policies-> IPv4 Filter Rules-> New**	*Deny*

Filter rules 4: Allow access to all services on the Internet (Director)

Field	Menu	Value
Source Location	**Firewall ->Policie s->IPv4**	*Director*

Field	Menu	Value
	Filter Rules-> **New**	
Destination	**Firewall**-> **Policies**-> **IPv4** **Filter Rules**-> **New**	*ANY*
Service	**Firewall** ->**Policie s**->**IPv4** **Filter Rules**-> **New**	*any*
Action	**Firewall**-> **Policies**-> **IPv4** **Filter Rules**-> **New**	*Access*

Filter rules 5: Allow access to the Internet (Staff)

Field	Menu	Value
Source Location	**Firewall** ->**Policie s**->**IPv4** **Filter Rules**-> **New**	*Network_Internal*
Destination	**Firewall**-> **Policies**-> **IPv4** **Filter Rules**-> **New**	*ANY*
Service	**Firewall** ->**Policie s**->**IPv4** **Filter Rules**-> **New**	*Internet Ports*
Action	**Firewall**-> **Policies**-> **IPv4** **Filter Rules**-> **New**	*Access*

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.

The Session Initiation Protocol (SIP) is used to establish, clear and control a communication session.

16.1 Application Level Gateway

To enable IP telephones to connect by SIP to a VoIP Provider your device has an Application Level Gateway (ALG), i.e. an appropriate proxy that implements the necessary NAPT and firewall releases.

Note

The Application Level Gateway must always be used if NAT is enabled on the interface that makes the connection to the Internet.

16.1.1 SIP Proxies

Here you can view a list of application level gateway entries that have already been configured. These entries enable the ALG. Each entry defines a particular TCP or UDP destination port that is to be supervised by the ALG. In the ex works state, there are two entries configured for the SIP Ports TCP 5060 and UDP 5060 in accordance with the IANA definition.

16.1.1.1 Edit or New

Choose the icon to edit existing entries. Choose the **New** button to create application level gateway entries. The **VoIP**->**Application Level Gateway**->**SIP Proxies**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the application level gateway.
Administrative Status	Select whether the SIP proxy should be enabled or disabled. The function is activated by selecting *Enabled*. The function is enabled by default.
Protocol	Select the protocol to be used. Possible values: *UDP* (default value) or *TCP* Enter the port to be supervised by the proxy as **Destination Port**. or each destination port to which VoIP clients from the LAN can connect, you must configure a proxy. The ports can be provider-specific.
Session Timeout	Enter the time in seconds for which a session stays up if no data packets are sent or received. This value must be greater than the SIP Expire Time of the connected SIP client (SIP telephone, terminal adapter etc.) The default value is *1800*.
Low Latency Transmission	Specify whether a mechanism should be used to minimise the transit time of VoIP data packets between two subscribers. This guarantees good voice quality with high line load. Note that low latency transmission only has to be enabled for calls that are not established via the connections configured in **VoIP**->**Media Gateway**. The function is activated by selecting *Enabled*. The function is disabled by default.

16.1.2 SIP Endpoints

Shows the sessions that are currently being managed by ALG.

This includes static entries to make internal SIP servers/proxies (e.g. internal Asterisk serv-

er) accessible from the WAN (Internet) by NAPT. In addition, internal SIP clients without registration can be made accessible using a static entry. All active SIP sessions that have been initiated from internal SIP terminals are recognised dynamically and listed here. These are only displayed for monitoring and administration and cannot be edited.

Note

All automatically created entries that are not used for longer than 24 hours are automatically deleted from the table.

16.1.2.1 Edit or New

Choose the **New** button to add static entries for SIP terminals in the LAN that are to be accessible by terminals from the WAN across the NAPT barrier. Choose the icon to edit existing static entries.

Note

Entries created dynamically for active sessions cannot be edited. These entries can only be removed resulting in the immediate termination of the corresponding SIP connection.

The **VoIP**->**Application Level Gateway**->**SIP Endpoints**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Type of Endpoint	Select the role for the SIP endpoint in the LAN. Possible values: • *Client* (default value): The internal SIP endpoint is a SIP client (e.g. telephone). • *Server*: The internal SIP endpoint is a SIP server into which the SIP endpoint can login externally.
Protocol	Select the protocol to be used for data transmission. Possible values: • *UDP* (default value)

Field	Description
	• *TCP* If a protocol has been automatically recognised, it should not be changed.
Internal IP Address	Specify the IP address for the internal SIP endpoint in the LAN.
Remote Port	Only for **Type of Endpoint** = *Client* Enter the port of the removed SIP terminal (in the WAN).
Internal Port	Only for **Type of Endpoint** = *Server* Enter the port for the internal SIP endpoint in the LAN.
External Port	Specify the port on the WAN site of the gateway that is used for access through the NAPT barriers to a SIP endpoint in the LAN. For clients, the external port is recognised automatically and should not be changed.

16.2 Settings

16.2.1 Extensions

Here you can configure the numbers of the terminal devices (=Extensions) connected to the media gateway, i.e. the numbers of the SIP terminals and the numbers of the ISDN terminals, depending on the available interfaces.

A list of all existing subscribers is displayed in the **VoIP**->**Settings**->**Extensions** menu.

16.2.1.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to create new extensions.

The **VoIP**->**Settings**->**Extensions**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the extension.

Field	Description
Extension / User Name	ISDN terminals: Enter the subscriber number the extension. SIP terminals: Enter the user name. A maximum of 40 characters can be entered.
Interface Type	Select the interface type to be used. The selection depends on the interfaces available. Possible values: • *SIP*: A SIP terminal device is used for the call. • *ISDN*: An ISDN terminal device is used for the call. Can only be selected if ISDN interfaces configured with Euro ISDN point-to-multipoint (NT mode) are available. • *Analogue*: An analogue terminal device is used for the call. Can only be selected if analogue interfaces are available.
Select ISDN interface	Only for **Interface Type** = *ISDN* Select an ISDN interface. The ISDN interfaces you can select depends on the device used.
Select analogue interface	Only for **Interface Type** = *Analogue* Select an analogue interface. Possible values: • fxs5-1 • fxs5-2 • fxs5-3 (default value) • fxs5-4
Registration	Only for **Interface Type** = *SIP* Specify whether the registration mechanism is to be used by SIP REGISTER. Normally, every SIP client (user) sends its current position to a REGISTRAR server by means of a REGISTER message. This information about the user and his current address is held by the REGISTRAR server and queried by other proxies to find the user.

Field	Description
	The function is enabled with *Enabled*. The function is enabled by default. Apart from this standard procedure, the relevant data can also be sent to a particular IP address that is already known to the correspondent. Registration and authentication are not then needed and the **Registration** function is disabled. An example of this method is Microsoft Exchange SIP.
Expire Time	Only if **Registration** is enabled. Enter the time in seconds after which the current registration becomes invalid and a new registration request is therefore sent. For clients, the external port is recognised automatically and should not be changed. Possible values are *0* to *3600*. The default value is *60*.
SIP Endpoint IP Address	Only if **Registration** is disabled. For configurations with no registration (e.g. connection to a Microsoft Exchange Communication Server) the connection can be set up as a static host. This requires you to specify the static IP address of the terminal.
Authentication ID	Only for **Interface Type** = *SIP* Enter a name that is to be used for authentication. A maximum of 20 characters can be entered. The name given here must also be entered on the SIP telephone. If you do not enter a name, the name in the **Extension / User Name** field is used.
Password	Only for **Interface Type** = *SIP* Enter a password here. A maximum of 20 characters can be entered.

Field	Description
	The password given here must also be entered on the SIP telephone.
Protocol	Select the protocol to be used for data transmission. Possible values: *UDP* (default value), *TCP* or *TLS*. If a protocol has been automatically recognised, it should not be changed.
Port	Enter the number of the UDP, TCP port or TLS ports to be used for the connection to the server or proxy. Possible values are *0* to *65535*. The default value is *5060*.

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

Fields in the Codec Settings menu

Field	Description
Codec Proposal Sequence	Choose the order in which the codecs are offered for use by the media gateway. If the first codec cannot be used, the second is tried and so on. Possible values: • *Default* (default value): the codec in the first position in the menu will be used if possible. • *Quality*: The codecs are sorted by quality. If possible, the codec with the best quality is used. • *Lowest*: The codecs are sorted by required bandwidth. If possible, the codec with the lowest bandwidth requirement is used. • *Highest*: The codecs are sorted by required bandwidth. If possible, the codec with the highest bandwidth requirement is used.

Fields in the Sort Order menu

Field	Description
Sort Order	Select the codecs to be proposed for the connection. The co-

Field	Description
	decs chosen here are proposed in a certain order, depending on the setting in the **Codec Proposal Sequence** field. Possible values: • *G.711 uLaw*: ISDN codec according to US law • *G.711 aLaw*: ISDN codec according to EU law • *G.722*: G.722 passes audio signals in the range of 50-7000 Hz and samples them at the rate of 16,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,5. • *G.729*: Compressed from 31 to 8 kbps; good voice quality • *G.726-40*: Compressed from 63 to 40 kbps • *G.726-32*: Compressed from 55 to 32 kbps • *G.726-24*: Compressed from 47 to 24 kbps • *G.726-16*: Compressed from 39 to 16 kbps • *RFC 2833*: First the system attempts to use RFC 2833. If the remote terminal does not use this standard, SIP Info is used. • *SRTP*: SRTP is an encrypted variant of the Real-Time Transport Protocol (RTP). • *Data (RFC 4040)*: Enable the transport of 64 kbit/s channel data in RTP packets. • *SIP Info*: SIP Info is used for the transmision of DTMF events. • *T.38 Fax*: Allows the transmission of fax messages over data networks. By default *G.711 uLaw*, *G.711 aLaw* and *G.729* are enabled. The codecs actually used are the intersect of the codecs defined here and those signalled by the provider. For outgoing calls, any remaining codecs are dropped from the list that would require more than the available bandwidth.

Fields in the Voice Quality Settings menu.

Field	Description
Echo Cancellation	Select whether echo cancellation should be used. Echo cancellation is a technique to suppress echo feedback in

Field	Description
	voice communication on full duplex lines. The function is enabled with *Enabled*. The function is enabled by default.
Comfort Noise Generation (CNG)	Specify whether Comfort Noise Generation should be used. For digital voice transmission, this function introduces a low level of background noise to avoid the impression that, during pauses at the other end, the connection is lost. The function is enabled with *Enabled*. The function is enabled by default.
Packet Size	Specify how many milliseconds of voice an RTP data packet should contain. Possible values are *5* to *500*. The default value is *20*.

16.2.2 SIP Accounts

If your want your device to connect to other SIP servers (e.g. servers of Internet SIP Service providers), you can configure the necessary entries here. In this case, the media gateway acts as a SIP client.

Furthermore, you can configure the entries for SIP trunking scenarios here. In this case, the media gateway acts as a SIP server for other SIP servers. An example for this is the connection of a SIP PBX (e.g. Asterisk) to the media gateway.

This means that not only all SIP provider accounts are configured here but also direct dial-in PBXs connected with the media gateway.

Note

In no case should you use this menu to configure SIP extensions, i.e. for SIP clients or PSTN clients such as SIP telephones, terminal adapters or ISDN telephones

SIP extensions can be configured in the **VoIP**->**Extensions**menu.

The **VoIP**->**Settings**->**SIP Accounts** menu displays a list of all existing SIP accounts (SIP Client Mode and SIP Server Mode).

16.2.2.1 Edit or New

Select the **New** button to create new SIP accounts. Choose the icon to edit existing entries. In this menu SIP accounts are configured in SIP client mode as well as in SIP server mode.

The **VoIP**->**Settings**->**SIP Accounts**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the SIP account.
Administrative Status	Select whether the SIP account should be enabled or disabled. The function is enabled with *Enabled*. The function is enabled by default.
Trunk Mode	Select whether and in which trunk mode the SIP account should be operated. Trunk mode (DDI, Direct Dial In) allows an incoming call to be assigned correctly to a terminal (DDI). For an outgoing call, the caller can be indicated to the called party. The setting that you can use depends on the provider. Possible values: • *Off* (default value): Trunk mode is not used. The SIP account has only one number. • *Client*: The media gateway is operated as DDI client. It is assigned a DDI. • *Server*: The media gateway is operated as a DDI server so that DDI clients can connect. • *Gateway*: The media gateway is operated as DDI client, but used as a trunk. This setting is used to connect a software-based IP PBX from Swyx.
Registrar	Only for **Trunk Mode** = *Off*, *Client* and *Gateway*Enter the

Field	Description
	IP address or domain name (FQDN) of the SIP registrar. The maximum number of characters is 40. Entries with spaces are not allowed.
SIP Endpoint IP Address	Only for **Trunk Mode** = *Server* and **Registration type** = *No registartion* Enter the IP address or domain name (FQDN) of the SIP proxy server.
Outbound Proxy	Only for **Trunk Mode** = *Off*, *Client* or *Gateway* Enter the name or IP address of the SIP outbound proxy server. A maximum of 32 characters can be entered. Here you must make an entry only if, for all SIP sessions, the communication is not to be direct but via a further proxy. In SIP client mode: Enter a name or IP address only if this is explicitly specified by the provider.
Domain / Realm	Enter a new domain name or a new IP address for the SIP proxy server. If you do not make an entry, the entry in the **Registrar** field is used. In SIP client mode: Enter a name or IP address only if this is explicitly specified by the provider.
Protocol	Select the protocol to be used for data transport. Possible values: *UDP* (default value) or *TCP* Enter the **Port** via which the data is to be transported. The default value is *5060*. In SIP client mode: The ports can be provider-specific.
User Name	In SIP client mode: Enter the username for authentication if your VoIP provider has assigned one for you. In SIP server mode: You must define the user name.

Field	Description
	A maximum of 40 characters can be entered.
Authentication ID	Enter a name that is to be used for authentication with the outbound proxy. If you do not enter a name, the name in the **User Name** field is used. In SIP client mode: Enter a name only if this is explicitly specified by the provider.
Password	In SIP client mode: The VoIP provider gives you a PIN or password for authentication. You must enter this value here. In SIP server mode: Define a PIN or a password. A maximum of 40 characters can be entered.
Location	Set the location of the VoIP subscriber. Possible values: • *Not defined (Registration for Private Networks Only)* (default value): The VoIP subscriber is only registered if located within the private network. • *LAN*: The VoIP subscriber is only registered if located in the LAN.
Registration type	Specify how registration and authentication at a provider are to be handled, or if they can omitted completely. In the latter case, the relevant data are sent to a particular IP address that is already known to the correspondent. Registration and authentication are not then needed and the Registration function is disabled. An example of this method is Microsoft Exchange SIP. If a registration is required, it can be carried out in either of two ways: • *Single*: With this option, a single MSN is registered with the SIP provider. • *Bulk (BNC)*: With this option, a SIP Trunk (DDI) is registered with the SIP provider, i.e. several numbers are registered under a single address. • *No registration*: There is not registration.

Field	Description
Expire Time	Only if **Registration type** = *Single* or *Bulk (BNC)* Enter the time in seconds after which the current registration becomes invalid and a new registration request is therefore sent. Possible values are *0* to *38400*. The default value is *600*. In answer to a REGISTER request, a server can set another Expire Time which overwrites the setting here.
Called Address	Determines from which parameter of the called address the number is extracted. Possible values: • *Standard* (default value): Extracts the number from the first part of the address. If this fails, the number is extracted from the second part of the address. • *Request URI*: In some applications (especially in DDI connections) the target address of a SIP call needs to be extracted from the Request URI. By activating this option the address is preferably read from this field of the invite.
Check Source IP	As a response to a DNS SRV request, your SIP provider transmits the addresses of valid registration servers. If you activate this option, each SIP invite has its source IP checked against these valid addresses. If it does not originate from one of them, the invite is ignored. The option is not active per default.
TLS certificate check	Only for DDI / SIP trunk connections. If a connection is encrypted using TLS (Transport Layer Security) a validity check on the server certificate of the remote station is performed. The option is not active per default.
Send RTP Dummy	This option is required if the media gateway is connected to a NAT device that provides internet access towards the SIP provider.

Fields in the Trunk Settings menu.

Field	Description
SIP Header Field: FROM Display	Not for **Trunk Mode** = *Off* The sender ID is placed in the "Display" field of the SIP header. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: FROM User	Not for **Trunk Mode** = *Off* The sender ID is sent in the "User" field of the SIP header. Possible values: • *Username* (default value): The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: P-Preferred	Not for **Trunk Mode** = *Off* The so-called "p-preferred-identity" field is added to the SIP header and contains the sender ID. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: P-Asserted	Not for **Trunk Mode** = *Off* The so-called "p-asserted-identity" field is added to the SIP

Field	Description
	header and contains the sender ID. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
Subscribe Number	Only for **Trunk Mode** = *Client* or *Server* You can set a number that is added as a prefix for outgoing calls to the sender's number and is removed from the destination number for incoming calls. This corresponds to the trunk (exchange) number of an exchange.
Billing Number	Enter the phone number from which the call is established.

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

Fields in the Codec Settings menu

Field	Description
Codec Proposal Sequence	Choose the order in which the codecs are offered for use by the media gateway. If the first codec cannot be used, the second is tried and so on. Possible values: • *Default* (default value): the codec in the first position in the menu will be used if possible. • *Quality*: The codecs are sorted by quality. If possible, the codec with the best quality is used. • *Low Bandwidth*: The codecs are sorted by required bandwidth. If possible, the codec with the lowest bandwidth requirement is used. • *High Bandwidth*: The codecs are sorted by required bandwidth. If possible, the codec with the highest bandwidth requirement is used.

Fields in the Codecs menu

Field	Description
Codecs	Select the codecs to be proposed for the connection. The codecs chosen here are proposed in a certain order, depending on the setting in the **Codec Proposal Sequence** field. Possible values: • *G.711 uLaw*: ISDN codec according to US law • *G.711 aLaw*: ISDN codec according to EU law • *G.722*: G.722 passes audio signals in the range of 50-7000 Hz and samples them at the rate of 16,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,5. • *G.729*: Compressed from 31 to 8 kbps; good voice quality • *G.726-40*: Compressed from 63 to 40 kbps • *G.726-32*: Compressed from 55 to 32 kbps • *G.726-24*: Compressed from 47 to 24 kbps • *G.726-16*: Compressed from 39 to 16 kbps By default *G.711 uLaw*, *G.711 aLaw* and *G.729* are enabled. The codecs actually used are the intersect of the codecs defined here and those signalled by the provider. For outgoing calls, any remaining codecs are dropped from the list that would require more than the available bandwidth.

Fields in the Options menu

Field	Description
Options	Select the option to be used for the connection. Possible values: • *RFC 2833*: First the system attempts to use RFC 2833 for the transmission of DTMF events. If the remote terminal does not use this standard, SIP Info is used. • *SRTP*: SRTP is an encrypted variant of the Real-Time Transport Protocol (RTP). • *Data (RFC 4040)*: Enable the transport of 64 kbit/s channel data in RTP packets.

Field	Description
	• *SIP Info*: SIP Infor is used for the transmission of DTMF events. • *T.38 Fax*: Allows the transmission of fax messages over data networks. • *SIP 302*Select whether calls are to be redirected externally with the SIP provider. The call is forwarded using SIP status code 302. The function is activated by selecting *Enabled*. The function is disabled by default. • *MediaSec*:MediaSec negotiates the protection of RTP data with the SIP servers. For seamless support, automatic negotiation of the transport protocol is mandatory. Fixed transport protocol settings (UDP and TCP) may cause problems during registration. Additionally, the use of SRTP must be allowed. Your VoIP provider must support MediaSec.

Fields in the Voice Quality Settings menu.

Field	Description
Echo Cancellation	Select whether echo cancellation should be used. Echo cancellation is a technique to suppress echo feedback in voice communication on full duplex lines. The function is enabled with *Enabled*. The function is enabled by default.
Comfort Noise Generation (CNG)	Specify whether Comfort Noise Generation should be used. For digital voice transmission, this function introduces a low level of background noise to avoid the impression that, during pauses at the other end, the connection is lost. The function is enabled with *Enabled*. The function is enabled by default.
Packet Size	Specify how many milliseconds of voice an RTP data packet should contain.

Field	Description
	Possible values are *5* to *500*. The default value is *20*.

16.2.3 Locations

In the **VoIP**->**Settings**->**Locations** menu you configure the locations of the VoIP subscribers who have been configured on your system, and define the bandwidth management for the VoIP traffic.

Individual locations can be set up for using the bandwidth management. A location is identified from its fixed IP address or DynDNS address or from the interface to which the device is connected. The available VoIP bandwidth (up- and downstream) can be set up for each location.

Only for compact systems: A predefined entry with the parameters **Description** = *LAN*, **Parent Location** = *None*, **Type** = *Interfaces*, **Interfaces** = *LAN_EN1-0* is displayed.

Fields in the Registration behavior for VoIP subscribers without assigned location menu.

Field	Description
Default Behavior	Specify how the system is to proceed when registering VoIP subscribers for whom no location has been defined. Possible values: • *Registration for Private Networks Only* (default value): The VoIP subscriber is only registered if located within the private network. • *Not allowed*: The VoIP subscriber is never registered. • *Unrestricted Registration*: The VoIP subscriber is always registered.

16.2.3.1 Edit or New

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

The menu **VoIP**->**Settings**->**Locations**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter the description of the entry.
Parent Location	You can cascade the SIP locations as you wish. Define here which SIP location that has been defined constitutes the high-level node for the SIP location to be configured here.
Type	Select whether the location is to be defined through IP addresses/DNS names or interfaces. Possible values: • *Addresses* (default value): The SIP location is defined via IP addresses or DNS names. • *Interfaces*: The SIP location is defined via the available interfaces.
Addresses	Only for **Type** = *Addresses* Enter the IP addresses of the devices at the SIP locations. Click **Add** to configure new addresses. Enter the IP address or DNS name that you want under **IP Address/DNS Name**. Also enter the required **Netmask**.
Interfaces	Only for **Type** = *Interfaces* Indicate the interfaces to which the devices of a SIP location are connected. Click **Add** to select a new interface. Under **Interface**, select the interface you want.
Upstream Bandwidth Limitation	Determine whether the upstream bandwidth is to be restricted. The bandwidth is reduced with *Enabled*. The function is disabled by default.
Maximum Upstream Bandwidth	Enter the maximum data rate in the send direction in kBits per second.

Field	Description
Downstream Bandwidth Limitation	Determine whether the downstream bandwidth is to be restricted. The bandwidth is reduced with *Enabled*. The function is disabled by default.
Maximum Downstream Bandwidth	Enter the maximum data rate in the receive direction in kBits per second.

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

Fields in the Advanced Settings menu.

Field	Description
DSCP Settings for rtp Traffic	Select the Type of Service (TOS) for RTP data. Possible values: • *DSCP Binary Value* (default value): Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). The preconfigured value is *101110*. • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.

16.2.4 ISDN Trunks

Your device must have at least two ISDN connections in point-to-point mode (BRI or PRI), which are configured as TE (party line) or NT for a configuration in the **ISDN Trunks** menu.

In this menu, the ISDN party lines (bundles) are defined.

16.2.4.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to create a new party line.

The **VoIP**->**Settings**->**ISDN Trunks** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the party line. The maximum number of characters is 40.
ISDN Mode	Select the mode in which the party line is to be operated. Possible values: • *Extern* (default value): Point-to-Point TE connection (telecom party line) • *Trunk*: Point-to-Point NT connection (for connection of a PABX).
Members	Select the desired ISDN interfaces to be included with this party line. You can choose among the ISDN connections in point-to-point mode (BRI or PRI), which are configured as TE (party line) or NT.

16.2.5 Options

In the **VoIP**->**Settings**->**Options** menu you can perform global settings for the Media Gateway.

The menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Media Gateway Status	Select whether the media gateway function should be enabled. This option has to be enabled if you intend to establish VoIP

Field	Description
	connections from terminals directly connected to your device. If this option is disabled, so is the complete VoIP functions of the Media Gateway. This is desirable if you intend to connect an existing IP PABX to your device. All SIP accounts that are intended to establish connections then have to be configured in that IP PABX. We recommend using the **VoIP PBX in the LAN** assistant in order to configure your device for this application. The function is enabled with *Enabled*. The function is disabled by default.
Session Border Controller Mode	Specify how the media gateway should behave in conjunction with a session border controller mode. Possible values: • *Auto* (default value): for all extensions that exactly agree with an existing SIP account, the call routing is handled by the session border controller, i.e. all SIP messages configured for the corresponding SIP account are forwarded to the session border controller. For all other extensions, the call routing is handled by the media gateway in accordance with the entries configured under **Call Routing**. Note that the call routing is handled by the media gateway if the provider is not available (backup). • *Off*: Call routing is handled exclusively by the media gateway in accordance with the entries configured under **Call Routing** and the local extensions. For calls that are to be routed via a particular provider (SIP account), you must configure a corresponding call routing entry. Internal calls (from internal extension to internal extension) that are only to be routed internally do not require an additional call routing entry. • *<SIP Trunk>*: Select a SIP trunk account configured under **VoIP**->**Settings**->**SIP Accounts**. In this case, the call routing for all extensions is handled by the session border controller, all SIP messages are forwarded to the session border controller. Note that the call routing is handled by the media gateway if the provider is not available (backup). Please note: Entries in **Call Routing** have priority ahead of the session border controller configuration!
Call Routing for local	Determine if routing entries are to be preferred over extensions.

Field	Description
Extensions	*Enabled* activates this function. The function is enabled per default.
Media Stream Termination	Choose how RTP sessions are controlled by the system. If the function is enabled, RTP sessions are terminated on the media gateway, i.e. all RTP streams are controlled by the media gateway and routed via the media gateway. The participating terminal devices (e.g. SIP telephones) are not connected directly with one another. Note that, for VoIP to VoIP connections, there is no code translation for different VoIP terminal codecs. The codecs of media gateway and VoIP terminals must therefore agree. If the function is disabled, RTP sessions are not terminated on the media gateway, i.e. all RTP streams are routed by the media gateway without termination. The RTP data packets can be routed in complex networks and thus also via other gateways. The function is enabled with *Enabled*. The function is enabled by default.
Default Drop Extension	You can specify an extension to which incoming calls are forwarded if they cannot be assigned to an extension or connected PABX.
Dial Latency	Enter the maximum delay time before the system assumes the call number entered is complete and starts the SIP dialling process (sends the SIP INVITE message). This timeout is reset each time that a button is pressed. Possible values are *0* to *15*. The default value is *5*. If you terminate the number entered with #, dialling is immediate.

Fields in the Advanced Settings menu.

Field	Description
ISDN Call Signalling	If you have connected a PABX to one of the internal ISDN connections, you can specify how to treat subscriber numbers of a DDI here. For some PABXs the type of number has to be identified, and the **International Prefix / Country Code** and/or the **National Prefix / Area Code** have to be removed from the subscriber number in order to correctly identify the subscriber. You can do this by selecting *Specific: international, national or subsriber number*. Possible values: • *Standard: always as unknown number*: The type of number is not detected. • *Specific: international, national or subscriber number*: The type of number is detected. If required, the **International Prefix / Country Code** and/or the **National Prefix / Area Code** are removed from the subscriber number
Speed Dialing	Define short sequences of numbers that can be dialled instead of the entire number. Click **Add** to configure new speeddial numbers. Enter the desired speeddial number for the user, e.g. *123* under **Shortcut**. Under **Replacement** enter the subscriber number to be dialled in place of the speed dial number, e.g. *09119673*. In the example above, if a user types in **123*, the device dials *09119673*. If the user wishes to call extension *111*, he types in **123111*. The device dials *09119673111*. A period at the end of the number indicates a complete number. This is dialled immediately the period is recognised.

If you want to use a speeddial number from this list, you must dial * followed by the speeddial number.

16.3 Media Gateway

A media gateway serves as a translation instance between different telecommunications networks, e.g between the plain old phone network and the next generation networks (IP networks).

With the bintec elmegbintec elmeg Media Gateway, a company equipped with an automatic PBX on a wired telephone network can be connected to a SIP Trunking Service Provider on the Internet in order to use IP telephony.

The bintec elmegbintec elmeg Media Gateway supports the binding of several SIP Provider Accounts. With this gateway, you can set up extensions, create an extension number plan and configure exchange functions and optimise voice data transmission for low bandwidth of the upload connection.

Note

Your device must be equipped with a DSP module to be able to use the media gateway functions.

Please consult the data sheet of your device to find out whether the DSP module is an integral component of your device or if you can mount a DSP module. Information on mounting the DSP module is provided in the installation instructions included with the module.

16.3.1 Call Routing

Here you can define the conditions for the routing of calls. Define a list with rules or rule chains that are used to manipulate the indicated destination numbers.

A list of all existing entries is displayed in the **VoIP**->**Media Gateway**->**Call Routing** menu.

16.3.1.1 Edit or New

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

The **VoIP**->**Media Gateway**->**Call Routing**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the entry.
Administrative Status	Select whether the entry should be activated. The function is enabled with *Enable*. The function is enabled by default.
Type	Specify how calls are to be routed. Possible values: • *Accept Rule*: For calls forwarded by the media gateway to a PBX or an ISDN TE connector or a SIP DDI client. For this, the following can be used: PRI interfaces in NT mode, BRI interfaces in NT mode, SIP accounts in trunk mode (server mode). • *Deny*: For calls that are not to be routed (to be blocked).
Calling Line	You can restrict the application of the entry to the line on which the call comes in. The selection depends on the interfaces available and on the SIP accounts that have been created. Possible values: • *pri<Interface Index>*: restricts the routing entry to the selected PRI interface. • *bri<Interface Index>*: restricts the routing entry to the selected BRI interface. • *<SIP Account>*: restricts the routing entry to the selected SIP account. • *Any*: No restriction of the entry.
Calling Address	You can restrict the application of the entry to a particular caller. To do this, you must specify the subscriber number exactly (no wildcards).
Called Address	Enter the called address to which the rule is to be applied. To do this, enter an address numerically (e.g. a subscriber number) or alphanumerically (e.g. for a trunk) that is to be compared

Field	Description
	with a dialled address. The following wildcards can be used: • * means that at the end of a character string any number of characters may follow, • ? is a placeholder for an arbitrary character. If the configured address agrees with the signalled address, the entry is used.

In the **Routing Rules** menu you can define rules to determine how the subscriber number is manipulated before it is used for dialling.

Use **Add** to create more entries.

Fields in the Routing Rules menu (For Type = Accept Rule only)

Field	Description
Priority	Enter a whole number starting with 1 in ascending order to define the order of filter rules. The rules are worked through in the order given in the list. If a line or SIP account is not available, the next rule is automatically used.
Administrative Status	Select whether the rule should be activated. The rule is enabled with *Enable*. The rule is active by default.
Line	Choose the ISDN line (PRI, BRI) or SIP account used for the outgoing call.
Called Address Translation	Enter how the subscriber number is manipulated before it is used for dialling. Notation: <a:b>; i.e. a is replaced by b. Every rule must be ended with a semicolon. A number of rules can be chained together using semicolons as separators, e.g. <a:b>;<c:d>;<e:f>. After confirmation of entry, the rule chain is automatically sorted by the "best match" method.

Field	Description
	Numerical and alphanumerical values are permissible. ? is a placeholder for an arbitrary character. **Example 16.1. Example of a rule** • Rule: <:+49911>; • number dialled: 96731234 • manipulated number: +4991196731234

16.3.2 CLID Translation

Here you define the processing of the calling party number for incoming calls.

You can, for example, add a prefix to a received call number in order to route corresponding outgoing calls via a particular SIP account.

In the **VoIP**->**Media Gateway**->**CLID Translation** menu, a list of all existing entries is shown on which the received number is edited.

16.3.2.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to create entries for CLID translation.

The **VoIP**->**Media Gateway**->**CLID Translation**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the entry.
Calling Line	Select the ISDN line or SIP account from which the call comes. The selection depends on the interfaces available and on the SIP accounts that have been created. Possible values: • *pri<Interface Index>*: Restricts the entry to the selected PRI interface.

Field	Description
	• *bri<Interface Index>*: Restricts the entry to the selected BRI interface. • *<SIP Account>*: Restricts the entry to the selected SIP account. • *Any*: No restriction of the entry.
Called Line	Here you have the option of entering the destination line of the call. Possible values: • *pri<Interface Index>*: Restricts the entry to the selected PRI interface. • *bri<Interface Index>*: Restricts the entry to the selected BRI interface. • *<SIP Account>*: Restricts the entry to the selected SIP account. • *Any*: No restriction of the entry. Enter either **Called Line** or **Called Address**. If a value other than *Any* is selected, **Called Address** should not be used. If **Called Line** = *Any* and **Called Address** is not used, all calls for **Called Line** are processed.
Called Address	Here you have the option of entering the destination address of the call. Enter either **Called Line** or **Called Address**. If **Called Address** is used, then **Called Line** = *Any* can be set .
Calling Address Translation	Enter the transformation rule applied to the call numbers. Notation: <a:b>; i.e. a is replaced by b. Every rule must be ended with a semicolon. A number of rules can be chained together using semicolons as separators, e.g. <a:b>;<c:d>;<e:f>;. After confirmation of entry, the rule chain is automatically sorted by the "best match" method. ? is a placeholder for an arbitrary digit.

Field	Description
	Example 16.2. Example of a rule • Rule: <:+49911>; • number dialled: 96731234 • manipulated number: +4991196731234

16.3.3 Call Translation

You can create a list for the translation of subscriber numbers, i.e. this list associates internal and external numbers.

Note

Which number (called party number or calling party number) is translated depends on the direction (incoming or outgoing) of the call in question. For incoming calls it is the called party number, for outgoing calls the calling party number that is translated.

For example, the internal number 340 can be shown externally as 09119673900 or a call from outside for the number 09119673200 can be routed internally to the number 340.

In the **VoIP**->**Media Gateway**->**Call Translation** menu, a list of existing transformations is displayed.

16.3.3.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to create entries for call translation.

The **VoIP**->**Media Gateway**->**Call Translation**-> ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the call translation.
Direction	Select the direction for the entry. Possible values:

Field	Description
	• *Both* (default value): For incoming and outgoing calls (bidirectional). • *Incoming*: For incoming calls. • *Outgoing*: For outgoing calls.
Associated Line	Select the ISDN line or SIP account via which the calls are to be routed. Possible values: • *pri<Interface Index>*: Restricts the call to the selected PRI interface. • *bri<Interface Index>*: Restricts the call to the selected BRI interface. • *<SIP Account>*: restricts the call to the selected SIP account.
Local Address	Enter the internal number (e.g. extension or PABX number). For incoming calls, the signalled Called Party Number (corresponds in the menu to the **External Address**) is translated to **Local Address**. For outgoing calls, the signalled Calling Party Number (corresponds in the menu to the **Local Address** field) is translated to **External Address**. Numerical and alphanumerical characters are permissible. *?* is a placeholder for an arbitrary digit. See **Local Address** and **External Address** must contain the same number of wildcards.
External Address	Enter the external number (e.g. ISDN MSN or SIP account subscriber number). For incoming calls, the signalled Called Party Number (corresponds in the menu to the **External Address**) is translated to **Local Address**. For outgoing calls, the signalled Calling Party Number (corresponds in the menu to the **Local Address** field) is translated to **External Address**. The **External Address** is not shown if the field **Associated Line** = *<SIP Account>* is set. In this case, the **User Name** of the selected SIP Account is used as **External Address**..

16.3.4 Special Numbers

At a DDI connection, the called number of an outgoing call is automatically converted to the international E.164 format. This conversion is undesirable for certain numbers. Exceptions from the conversion can be configured here.

16.3.4.1 Edit or New

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

The **Call Routing**->**Outgoing Services**->**Special Numbers**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Special Number	Specify the number that is to be excepted from E.164 conversion.

16.4 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.

16.4.1 RTSP Proxy

In the **VoIP**->**RTSP**->**RTSP Proxy** menu, you configure the use of the RealTime Streaming protocol.

The menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
RTSP Proxy	Select whether you want to permit RTSP sessions. The function is activated by selecting *Enabled*. The function is disabled by default.
RTSP Port	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).
- Start network devices that are switched off via an integrated network card (Wake-On-LAN)
- 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 name servers attached to an interface 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

The menu **Local Services**->**DNS**->**Global Settings** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Domain Name	Enter the standard domain name of your device.
WINS Server **Primary** **Secondary**	Enter the IP address of the first and, if necessary, alternative global Windows Internet Name Server (=WINS) or NetBIOS Name Server (=NBNS).

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

Fields in the Advanced Settings menu

Field	Description
Positive Cache	Select whether the positive dynamic cache is to be activated, i.e. successfully resolved names and IP addresses are to be stored in the cache. The function is activated by selecting *Enabled*. The function is enabled by default.
Negative Cache	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. The function is activated by selecting *Enabled*. The function is enabled by default.
Cache Size	Enter the maximum total number of static and dynamic entries. Once this value is reached, the dynamic entry not requested for the longest period of time is deleted when a new entry is added. **Cache Size** is reduced by the user, dynamic entries are deleted if necessary. Statistical entries are not deleted. **Cache Size** cannot be set to lower than the current number of static entries. Possible values: *0*.. *1000*.

Field	Description
	The default value is *100*.
Maximum TTL for Positive Cache Entries	Enter the value to which the TTL is to be set for a positive dynamic DNS entry in the cache if its TTL is *0* or its TTL exceeds the value for **Maximum TTL for Positive Cache Entries**. The default value is *86400*.
Maximum TTL for Negative Cache Entries	Enter the value set to which the TTL is to be set in the case of a negative dynamic entry in the cache. The default value is *86400*.
Fallback interface to get DNS server	Select the interface to which a connection is set up for name server negotiation if other name resolution attempts were not successful. The default value is *Automatic*, i.e. a one-time connection is set up to the first suitable connection partner configured in the system.

Fields in the IP address to use for DNS/WINS server assignment menu

Field	Description
As DHCP Server	Select which name server addresses are sent to the DHCP client if your device is used as DHCP server. Possible values: • *None*: No name server address is sent. • *Own IP Address* (default value): The address of your device is transferred as the name server address. • *DNS Setting*: The addresses of the global name servers entered on your device are sent.
As IPCP Server	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. Possible values: • *None*: No name server address is sent. • *Own IP Address*: The address of your device is transferred

Field	Description
	as the name server address. • *DNS Setting* (default value): The addresses of the global name servers entered on your device are sent.

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.

The **Local Services**->**DNS**->**DNS Servers**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Admin Status	Select whether the DNS server should be enabled. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a description for DNS server.
Priority	Assign a priority to the DNS server. You can assign more than one pair of DNS servers (**Primary DNS Server** and **Secondary DNS Server**) to an interface (i. e. for example, to an Ethernet port or a PPPoE WAN partner) or to multiple interfaces. The pair with the highest priority is used if the interface is "up". Possible values from *0* (highest priority) to *9* (lowest priority).

Field	Description
	The default value is `5`.
Interface Mode	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. Possible values: • `Static` • `Dynamic` (default value)
Interface	Select the interface to which the DNS server pair is to be assigned. The selected interface is relevant for outgoing DNS requests. This interface is used for DNS requests directed at the router or generated by the router itself. For **Interface Mode** = `Static` A DNS server is configured for all interfaces with the `Any` setting.
IP Version	Select the IP version used. Possible values: • `IPv4` • `IPv6` `IPv4` is selected by default.
Primary IPv4 DNS Server	Only if **Interface Mode** = `Static` Enter the IPv4 address of the first name server for Internet address name resolution.
Secondary IPv4 DNS Server	Only if **Interface Mode** = `Static` Optionally, enter the IPv4 address of an alternative name server.
Primary IPv6 DNS	Only if **Interface Mode** = `Static`

Field	Description
Server	Enter the IPv6 address of the first name server for Internet address name resolution.
Secondary IPv6 DNS Server	Only if **Interface Mode** = *Static* Optionally, enter the IPv6 address of an alternative name server.

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.

The menu **Local Services**->**DNS**->**Static Hosts**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Default Domain	Here, the domain is displayed that you have specified in the menu **DNS**->**Global Settings** as Domain Name.
DNS Hostname	Enter the host name to which the **IP Address** defined in this menu is to be assigned if a positive response is sent upon a DNS request. If a negative response is sent upon a DNS request, no address is specified. The entry can also start with the wildcard *, e.g. *.bintec-elmeg.com. If you specify a simple name (e.g. *router*), it is expanded by the Default Domain to form a complete DNS name (Fully Qualified Domain Name, FQDN). If you enter a name with the structure of a FQDN (i.e. character sequences separated by "."), the entry is interpreted as a FQDN and is not expanded. The closing "." which is mandatory for a complete FQDN is automatically appended if required. Entries with spaces are not allowed.
Response	In this entry, select the type of response to DNS requests.

Field	Description
	Possible values: • *Negative*: A DNS request for **DNS Hostname** gets a negative response. • *Positive* (default value): A DNS request for **DNS Hostname** is answered with the related **IP Address**. • *None*: A DNS request is ignored; no answer is given.
IPv4 Address	Only if **Response** = *Positive* Enter the IPv4 address assigned to **DNS Hostname**.
IPv6 Address	Only if **Response** = *Positive* Enter the IPv6 address assigned to **DNS Hostname**.

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 menu **Local Services**->**DNS**->**Domain Forwarding**->**New** consists of the following fields:

Fields in the Forwarding Parameters menu.

Field	Description
Forward	Select whether requests for a host or domain are to be forwarded. Possible values: • *Host* (default value) • *Domain*
Host	Only for **Forward** = *Host* Enter the name of the host for which requests are to be forwarded.

Field	Description
	If you enter a name without a ".", the entry is supplemented with the name supplied by the value specified in **Local Services**->**DNS**->**Global Settings** for **Domain Name** as soon as you confirm with **OK**.
Domain	Only for **Forward** = *Domain* Enter the name of the domain for which requests are to be forwarded. The entry can start with the wildcard "*", e.g. "*.bintec-elmeg.com". If you enter a name without a leading wildcard "*" a leading wildcard "*" is supplemented as soon as you confirm with **OK**.
Forward to	Select if matching DNS requests are to be forwarded to the DNS server of an **Interface** or to a manually specified **DNS Server**. Possible values: • *Interface* (default value): Requests are forwarded to the DNS server assigned to either an automatically selected or to a user-selected interface. • *DNS Server*: Requests are forwarded to the specified **DNS Server**.
Destination Interface	Only for **Forward to** = *Interface* Select the interface that has the DNS server assinged which is to receive the DNS requests.
Source Interface	Here you can select the DNS request source interface for domain forwarding. This option is available for forwarding to an interface as well as to specific DNS servers. It allows you to send DNS requests from different network segments to different DNS servers. For example, you can forwards the requests from your guest network to a webfilter DNS and deny access to undesired content.
Primary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the primary DNS server.

Field	Description
Secondary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* 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.

17.1.6 Cache

In the **Local Services**->**DNS**->**Cache** menu, a list of all available cache entries is displayed.

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

In the **Local Services**->**DNS**->**Statistics** menu, the following statistical values are displayed:

Fields in the DNS Statistics menu.

Field	Description
Received DNS Packets	Shows the number of received DNS packets addressed direct to your device, including the response packets for forwarded requests.
Invalid DNS Packets	Shows the number of invalid DNS packets received and addressed direct to your device.
DNS Requests	Shows the number of valid DNS requests received and addressed direct to your device.
Cache Hits	Shows the number of requests that were answered with static or dynamic entries from the cache.
Forwarded Requests	Shows the number of requests forwarded to other name servers.

Field	Description
Cache Hitrate (%)	Indicates the number of **Cache Hits** pro DNS request in percentage.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

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 menu consists of the following fields:

Fields in the HTTPS Parameters menu.

Field	Description
HTTPS TCP Port	Enter the port via which the HTTPS connection is to be established. Possible values are *0* to *65535*. The default value is *443*.
Local Certificate	Select a certificate that you want to use for the HTTPS connection. Possible values: • *Internal* (default value): Select this option if you want to use the certificate built into the device. • *<Certificate name>*: Under **System Management**->**Certificates**->**Certificate List** select entered certificate.

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.

The menu **Local Services**->**DynDNS Client**->**DynDNS Update**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host Name	Enter the complete host name exactly as registered with the DynDNS provider.

Field	Description
Interface	Select the WAN interface the IP address of which is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.
Provider	Select the DynDNS provider with which the specified data are registered. A choice of DynDNS providers is already available. and the protocols they use are supported. Other DynDNS providers can be configured in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu. The default value is *DynDNS*.
Enable update	Select whether the DynDNS entry configured here is to be activated and the current IP address of the selected interface is to be sent to the provider . The function is activated by selecting *Enabled*. The function is disabled by default.
HTTPS/SSL	This option is only available if the selected DynDNS provider supports SSL. If required, you can create a new provider supporting this option in the menu **Local Services**->**DynDNS Client**->**DynDNS Provider**. Enable this option in order to create an SSL-encrypted connection between your device and your DynDNS provider. Choosing *Enabled* activates the option. It is not enabled per default.
Certificate checking	Enable this fucntion in order verify the SSL certificate of the sever.
IP Version	This option is only available if your selected DynDNS provider provides server addresses for both IP versions. Select the IP version of the address you intend to update with your DynDNS

Field	Description
	provider. Possible values: IPv4 IPv6. In order to update the IPv4 as well as the Pv6 address of an interface, create two entries with otherwise identical settings. Inquire with your service provider if they support multiple updates!

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

Fields in the Advanced Settings menu.

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether forwarding of all subdomains of the **Host Name** is to be enabled for the current IP address of the **Interface** (advanced name resolution). The function is activated by selecting *Enabled*. 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.

The menu **Local Services**->**DynDNS Client**->**DynDNS Provider**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is *80*.
Protocol	Select one of the protocols implemented. Information on which protocol to use can be found in your provider's documentation. Possible values: • *DynDNS* (default value) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit* • *dyndnss* • *dyndns2*
Update Interval	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. The default value is *300* seconds.

Field	Description
IPv6 server	Specify the host name or IPv6 address of the DynDNS provider if you intend to update an IPv6 address.
Supports SSL	Enable support of SSL for securing data traffic between your device and the DnyDNS provider. The option is disabled per default.
Homepage	Here you can specify a web address that will take you to the page of the provider.

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.

For specific instructions how to use your device as a DHCP server, DHCP client or DHCP relay agent, see the ent of the chapter *DHCP - Configuration example* on page 442.

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.

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

17.4.2 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.

The **Local Services**->**DHCP Server**->**DHCP Configuration**->**New** menu consists of the

following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface over which the addresses defined in **IP Pool Name** are to be assigned to DHCP clients. When a DHCP request is received over this **Interface**, one of the addresses from the address pool is assigned.
IP Pool Name	Select an IP pool name configured in the **Local Services**->**DHCP Server**->**IP Pool Configuration** menu.
Pool Usage	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. In the second case, it is possible to use an IP address pool for the remote network. Possible values: • *Local* (default value): The DHCP pool is only used for DHCP requests from a network directly connected to an Ethernet interface. • *Relay*: The DHCP pool is only used for DHCP requests forwarded from remote networks. • *Local/Relay*: The DHCP pool can be used for both kinds of requests.
Description	Enter any description to uniquely identify the DHCP pool.

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

Fields in the menu Advanced Settings

Field	Description
Gateway	Select which IP address is to be transferred to the DHCP client as gateway. Possible values: • *Use router as gateway* (default value): Here, the IP address defined for the **Interface** is transferred.

Field	Description
	• *No gateway*: No IP address is sent. • *Specify*: Enter the corresponding IP address.
Lease Time	Enter the length of time (in minutes) for which an address from the pool is to be assigned to a host. After the **Lease Time** expires, the address can be reassigned by the server. The default value is *120*.
DHCP Options	Specify which additional data is forwarded to the DHCP client. Possible values for **Option**: • *Time Server* (default value): Enter the IP address of the time server to be sent to the client. • *DNS Server*: Enter the IP address of the DNS server to be sent to the client. • *DNS Domain Name*: Enter the DNS domain to be sent to the client. • *WINS/NBNS Server*: Enter the IP address of the WINS/NBNS server to be sent to the client. • *WINS/NBT Node Type*: Select the type of the WINS/NBT node to be sent to the client. • *TFTP Server*: Enter the IP address of the TFTP server to be sent to the client. • *CAPWAP Controller*: Enter the IP address of the CAPWAP controller to be sent to the client. • *URL (provisioning server)*: This option enables you to send a client any URL. Use this option to send querying **IP1x0** telephones the URL of the provisioning server if the telephones are to be provisioned automatically. The URL then needs to take the form *http://<IP address of the provisioning server>/eg_prov*. Multiple entries are possible. Add additional entries with the **Add** button.

Vendor Specific Information (DHCP Option 43)

The options for a **Vendor String** or a vendor-specific group of DHCP options (**Vendor Group**) enable you to transmit any manufacturer-specific information or configuration parameters to DHCP clients. You can also define entire groups of DHCP options to be transmitted.

Note

For some products settings have already been predefined in this section. These are required for the seamless integration of telephones or LTE access routers and should not be changed or deleted.

Choose the icon to edit an existing entry or one of the **Add** buttons to add an 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 for vendor strings

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server. Possible values: • *Other* (default value) • *-bintec-*
APN	Only für **Select vendor** = *-bintec-* Enter the Access Point Namen (APN) of the SIM card.
PIN	Only für **Select vendor** = *-bintec-* Enter the PIN of the SIM card.
Vendor Description	Only für **Select vendor** = *Other* Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Vendor ID	Only für **Select vendor** = *Other* To identify the device, enter the manufacturer ID.

Field	Description
Vendor Option String	Only für **Select vendor** = *Other* Enter the manufacturer specific configuration parameters.

Fields in the Basic Parameters menu for vendor groups

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server. Possible values: • *Siemens* (default value) • *Other*
Provisioning Server	Only für **Select vendor** = *Siemens* Enter which manufacturer value shall be transmitted. For the setting **Select vendor** = *Siemens*, the default value *sdlp* is displayed. You can complete the IP address of the desired server.
Vendor Description	Only für **Select vendor** = *Other* Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Vendor ID	Only für **Select vendor** = *Other* To identify the device, enter the manufacturer ID.
Custom DHCP Options	Only für **Select vendor** = *Other* Use **Add** to add more entries. You can add custom DHCP options.

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**->**IP Pool Configuration**, and in the **Local Services**->**DHCP Server**->**DHCP Configuration** menu a valid IP Pool is assigned to the DHCP server.

17.4.3.1 New

Choose the **New** button to set up new IP/MAC bindings.

The menu **Local Services**->**DHCP Server**->**IP/MAC Binding**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter the name of the host to which the **MAC Address** the **IP Address** is to be bound. A character string of up to 256 characters is possible.
IP Address	Enter the IP address to be assigned to the MAC address specified in **MAC Address** is to be assigned.
MAC Address	Enter the MAC address to which the IP address specified in **IP Address** is to be assigned.

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.

The menu **Local Services**->**DHCP Server**->**DHCP Relay Settings** consists of the following fields:

Fields in the Basic Parameters menu.

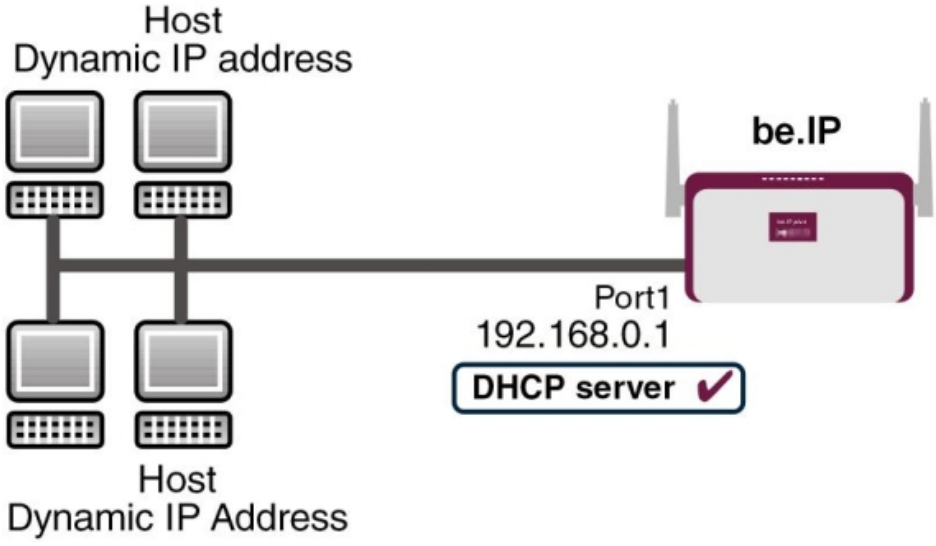
Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded. The default value is `0.0.0.0`.
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server. The default value is `0.0.0.0`.

17.4.5 DHCP - Configuration example

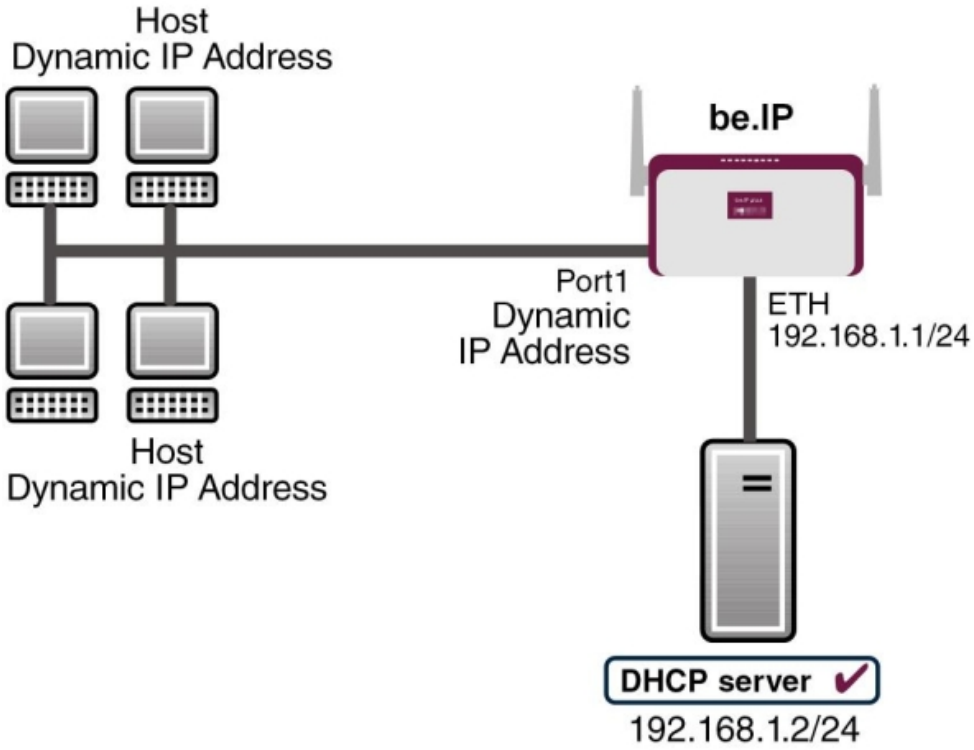
Requirements

- An optional DHCP server

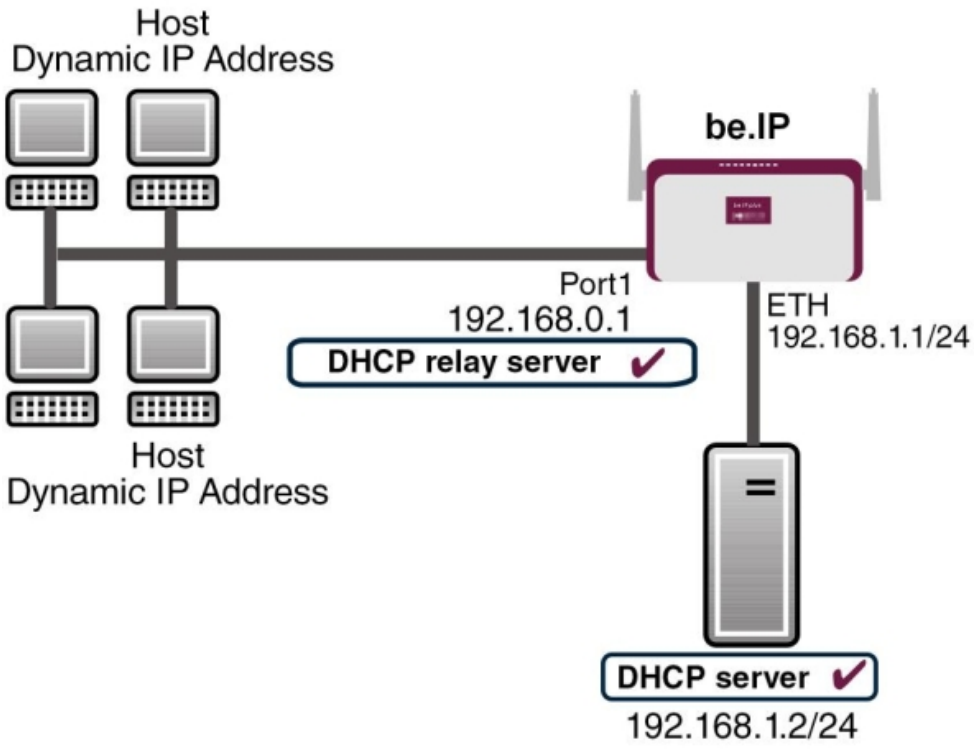
Example scenaria



Example scenario as DHCP Server



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. *IP-Pool-1*
IP Address Range	**Local Services->DHCP Server->IP Pool Configuration->New**	e.g. *192.168.0.2* and *192.168.0.10*
Interface	**Local Services->DHCP Server->DHCP Configuration->New**	e.g. *en1-0*
IP Pool Name	**Local Services->DHCP Server->DHCP Configuration->New**	*IP-Pool-1*
Pool Usage	**Local Services->DHCP Server->DHCP Configuration->New**	*Local*

Field	Menu	Value
Gateway	**Local Services->DHCP Server->DHCP Configuration->New->Advanced Settings**	*Use Router as Gateway*
Lease Time	**Local Services->DHCP Server->DHCP Configuration->New->Advanced Settings**	e.g. *120*
IP address to use for DNS/WINS server assignment	**Local Services->DNS->Global Settings->Advanced Settings**	e.g. *Own IP address*

DHCP Client

Field	Menu	Value
Address Mode	**LAN->IP Configuration->Interfaces-> <en1-4>->**	*DHCP*
DHCP MAC Address (optional)	**LAN->IP Configuration->Interfaces-> <en1-4> ->** **->Advanced Settings**	MAC address for a specific DHCP server

DHCP Relay Server

Field	Menu	Value
Primary DHCP Server	**Local Services->DHCP Server->DHCP Relay Settings**	e.g. *192.168.1.2*
Secondary DHCP Server (optional)	**Local Services->DHCP Server->DHCP Relay Settings**	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 an 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 **Add** and configure the Link Prefix. Confirm your configuration with **Accept**. The configuration of the recommended settings s 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.

The menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Name	Enter a name for the Option Set.
Interface	Select the IPv6 interface the Option Set is assigned to. You can choose from interfaces with the following configuration: • IPv6 is enabled. • The option **DHCP Server** is enabled. In the ex works state, IPv6 is disabled for all interfaces. If the intended 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 **LAN->IP Configuration->Interfaces**.
Address assignment	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. Use **Add** to assign one or more IPv6 Link Prefixes to the IPv6 Option Set. **Note** Note that only such IPv6 Link Prefixes are available for selection that are assigned to the selected interface.

Fields in the menu Server Options

Field	Description
DNS domains search list	Use **Add** 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
DNS Server	Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server"). Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field **DNS Propagation** in the menu **LAN**->**IP Configuration**->**Interfaces**->  ->**Advanced Settings** if **IPv6** = *Enabled* .) You can also manually specify DNS servers and have them propagated to the clients. To do this disable the option **Use RA or Global Fallback DNS Server** and create the desired DNS server entries using **Add**.
SNTP Server	Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Use **Add** 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).

The menu consist of the following fields:

Fields in the menu Basic Parameters

Field	Description
DNS domains search list	Use **Add** 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

Field	Description
	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
Server preference	The DHCPv6 advertisements sent by the DHCPv6 server to the clients may contain the DHCPv6 option 7 "Preference". Possible values are *0...255*. 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. A value of *0* means "not specified" (lowest priority), *255* denotes the highest priority.

Fields in the menu Advanced Server Fallback Options

Field	Description
DNS Server	Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server"). Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field **DNS Propagation** in the menu **LAN**->**IP Configuration**->**Interfaces**->  ->**Advanced Settings** if **IPv6** = *Enabled* .) You can also manually specify DNS servers and have them propagated to the clients. To do this disable the option **Use RA or Global Fallback DNS Server** and create the desired DNS server entries using **Add**.
SNTP Server	Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Use **Add** to create the desired time server entries.

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.

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.

The menu consists of the following fields.

Fields in the menu Basic Parameters

Field	Description
DUID	Clients use the **DUID field** (DHCP Unique Identifier) in order to identify themselves and request an IP address from the DHCPv6 server. If you create an entry using **New** you can specify the **DUID** as a 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).
Accept Client FQDN	If **Accept Client FQDN** is enabled, the client is entered into the cache of the Domain Name Server with the parameter FQDN (Fully Qualified Domain Name).
Administrative FQDNs	With **Add**, you can specify an FQDN (Fully Qualified Domain Name) - even for automatically created entries.
Static Interface Identifier	The field **Static Interface Identifier** 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 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.

17.6.1 User

A list of all configured CAPI users is displayed in the **Local Services**->**CAPI Server**->**User** menu.

17.6.1.1 New

Choose the **New** button to set up new CAPI users.

The menu **Local Services**->**CAPI Server**->**User**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
User Name	Enter the user name for which access to the CAPI service is to be allowed or denied.
Password	Enter the password which the user **User Name** shall use for identification to gain access to the CAPI service.

Field	Description
Access	Select whether access to the CAPI service is to be permitted or denied for the user. The function is activated by selecting *Enabled*. The function is enabled by default.

17.6.2 Options

The menu **Local Services**->**CAPI Server**->**Options** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Enable server	Select whether your device is to be enabled as a CAPI server. The function is activated by selecting *Enabled*. The function is enabled by default.
Faxheader	Select whether the fax header should be printed at the top of outgoing faxes. The function is activated by selecting *Enabled*. The function is disabled by default.
CAPI Server TCP Port	The field can only be edited if **Enable server** is enabled. Enter the TCP port number for remote CAPI connections. The default value is *2662*.

17.7 Scheduling

Your device has an event scheduler which enables certain standard actions (activation or deactivation of interfaces, for example) to be carried out. In addition, every existing MIB variable can be configured with any value.

You configure the desired **Actions** and define the triggers controlling the date and other conditions of the **Actions**. A trigger may be a single event or a sequence of events collected in an **Event List**. For a single event, create an **Event List** containing only one element.

It is possible to trigger operations on a time-controlled basis. What's more, the status or accessibility of interfaces, or their data traffic can lead to performance of the configured operations, as also the validity of licenses. Here again, it is possible to configure every MIB variable with any value as initiator.

Activate the **Schedule Interval** option under **Options** to put the event scheduler into operation. The system uses this time interval to check if at least one event has occurrred. This triggers the configured action.

Specific instructions for configuring Time-controlled Tasks (Scheduling), see the end of the chapter *Configuration example - Time-controlled Tasks (Scheduling)* on page 470.

Caution

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of bintec elmeg gateways. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

Note

To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

17.7.1 Trigger

All configured event lists are displayed in the **Local Services**->**Scheduling**->**Trigger** menu. Each event list contains at least one event intended to trigger a configured action.

17.7.1.1 New

Choose the **New** button to create additional event lists.

The menu **Local Services**->**Scheduling**->**Trigger**->**New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Event List	You can create a new event list with `New` (default value). You give this list a name with **Description**. You use the remaining parameters to create the first event in the list.

Field	Description
	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. 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.
4Description	Only for **Event List** *New* Enter your chosen designation for the **Event List**.
Event Type	Select the type of initiator. Possible values: • *Time* (default value): The operations configured and assigned in **Actions** are initiated at specific points in time. • *MIB/SNMP*: The operations configured and assigned in **Actions** are initiated when the defined MIB variables assumes the assigned values. • *Interface Status*: Operations configured and assigned in **Actions** are initiated, when the defined interfaces take on a specified status. • *Interface Traffic*: Operations configured and assigned in **Actions** are initiated when the data traffic on the specified interfaces falls below or exceeds the defined value. • *Ping Test*: Operations configured and assigned in **Actions** are initiated when the specified IP address is / is not accessible. • *Certificate Lifetime*: Operations configured and assigned in **Actions** are initiated when the defined period of validity is reached. • *Function Button*: The option *Function Button* 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 *Active*, pushing it for more than three seconds sets it to *Inactive*. Actions depending on the state of the button are then carried out after the next cyclical query determined by the **Schedule Interval**. In this way, e.g., a WLAN interface can be activated when the button is pushed

Field	Description
	for a second. Pushing the button for more than three seconds deactivates the interface again.
Monitored Variable	Only for **Event Type** *MIB/SNMP* Select the MIB variable whose defined value is to be configured as initiator. First, select the **System** in which the MIB variable is saved, then the **MIB Table** and finally the **MIB Variable** itself. Only the MIB tables and MIB variables present in the respective area are displayed.
Compare Condition	Only for **Event Type** *MIB/SNMP* Select whether the MIB variable *Greater* (default value), *Equal*, *Less*, *Not Equal* must have the value given in *Compare Value* or must lie within *Range* to initiate the operation.
Compare Value	Only for **Event Type** *MIB/SNMP* Enter the value of the MIB variable.
Index Variables	Only for **Event Type** *MIB/SNMP* If required, select MIB variables to uniquely identify a specific data set in a **MIB Table**, e.g. *ConnIfIndex*. The combination of **Index Variable** (normally an index variable labelled by a *) and **Index Value** creates the unique identification of a specific table entry. Create additional **Index Variables** with **Add**.
Monitored Interface	Only for **Event Type** *Interface Status* and *Interface Traffic* Select the interface whose defined status or data traffic shall initiate an event.
Interface Status	Only for **Event Type** *Interface Status* Select the status that the interface must have in order to initiate the intended operation. Possible values: • *Up* (default value): The function is enabled.

Field	Description
	• *Down*: The interface is disabled.
Traffic Direction	Only for **Event Type** *Interface Traffic* Select the direction of the data traffic whose values should be monitored as initiating an operation. Possible values: • *RX* (default value): Incoming data traffic is monitored. • *TX*: Outgoing data traffic is monitored.
Interface Traffic Condition	Only for **Event Type** *Interface Traffic* Select whether the value for data traffic must be *Greater* (default value) or *Less* the value specified in *Transferred Traffic* in order to initiate the operation.
Transferred Traffic	Only for **Event Type** *Interface Traffic* Enter the desired value in **kBytes** for the data traffic to serve as comparison. The default value is *0*.
Destination IP Address	Only for **Event Type** *Ping Test* Enter the IP address whose accessibility is to be checked.
Source IP Address	Only for **Event Type** *Ping Test* Enter an IP address to be used as sender address for the ping test. Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Status	Only for **Event Type** *Ping Test* Select whether **Destination IP Address** *Reacheable* must be (default value) or *Unreacheable* in order to initiate the opera-

Field	Description
	tion.
Interval	Only for **Event Type** *Ping Test* Enter the time in **Seconds** after which a ping must be resent. The default value is *60* seconds.
Trials	Only for **Event Type** *Ping Test* Enter the number of ping tests to be performed. The default value is *3*.
Monitored Certificate	Only for **Event Type** *Certificate Lifetime* Select the certificate whose validity should be checked.
Remaining Validity	Only for **Event Type** *Certificate Lifetime* Indicate the remaining validity of the certificate in percentage.
Function Button Status	Only for **Event Type** *Function Button*. When creating the trigger the dropdown selection **Function Button Status** allows you to choose which status of the function button activates or deactivates the trigger. If you set the status to *On*, the trigger becomes active if the status of the function button is *Active*, and inactive, if the state of the function button is *Inactive*. If your set it to *Off*, the trigger becomes active if the state of the function button is *Inactive*, and inactive if the state of the function button is *Active*. The current state is checked cyclically at the configured schedule interval.

Fields in the Select time interval menu

Field	Description
Time Condition	Only for **Event Type** = *Time* First select the type of time entry in **Condition Type**. Possible values: • *Weekday* : Select a weekday in **Condition Settings**. • *Periods* (default value): In **Condition Settings**, select a par-

Field	Description
	ticular period. • *Day of Month*: Select a specific day of the month in **Condition Settings**. Possible values for **Condition Settings** in **Condition Type** = *Weekday*: *Monday* (default value) ... *Sunday*. Possible values for **Condition Settings** in **Condition Type** = *Periods*: • *Daily* : The initiator becomes active daily (default value). • *Monday - Friday* : The initiator becomes active daily from Monday to Friday. • *Monday - Saturday* : The initiator becomes active daily from Monday to Saturday. • *Saturday - Sunday* : The initiator becomes active on Saturdays and Sundays. Possible values for **Condition Settings** in **Condition Type** = *Day of Month*: *1* ... *31*.
Start Time	Enter the time from which the initiator is to be activated. Activation is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Enter the time from which the initiator is to be deactivated. Deactivation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set a **Stop Time** = **Start Time**, the initiator is activated, and deactivated after 10 seconds.

17.7.2 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**.

17.7.2.1 New

Choose the **New** button to configure additional operations.

The menu **Local Services**->**Scheduling**->**Actions**->**New** consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter your chosen designation for the action.
Command Type	Select the desired action. Possible values: • *Reboot* (default value): Your device is rebooted. • *MIB/SNMP*: The desired value is entered for a MIB variable. • *Interface Status*: The status of an interface is modified. • *Wlan Status*: Only for devices with a wireless LAN. The status of a WLAN-SSID is modified. • *Software Update*: A software update is initiated. • *Configuration Management*: A configuration file is loaded onto your device or backed up by your device. • *Ping Test*: Accessibility of an IP address is checked. • *Certificate Management*: A certificate is to be renewed, deleted or entered. • *5 GHz WLAN Bandscan*: Only for devices with a wireless LAN. A scan of the 5 GHz frequency band is performed. • *5.8 GHz WLAN Bandscan*: Only for devices with a wireless LAN. A scan of the 5.8 GHz frequency range is performed. • *WLC: New Neighbor Scan*: Only for devices with a WLAN controller. A Neighbor Scan is initiated by the WLAN network controlled by the WLAN controller. • *WLC: VSS State*: Only for devices with a WLAN controller. The status of a wireless network is modified. • *WLAN: Operation Mode*: The operating mode of a WLAN radio module is modified.
Event List	Select the event list you want which has been created in **Local Services**->**Scheduling**->**Trigger**.

Field	Description
Event List Condition	For the selected chains of events, select how many of the configured events must occur for the operation to be initiated. Possible values: • *All* (default value): The operation is initiated if all events occur. • *One*: The operation is initiated if a single event occurs. • *None*: The operation is triggered if no event occurs. • *One not*: The operation is triggered if one of the events does not occur.
Reboot device after	Only if **Command Type** = *Reboot* Enter the timespan in seconds that must elapse after occurrence of the event until the device is restarted. The default value is *60* seconds.
MIB/SNMP Variable to add/edit	Only if **Command Type** = *MIB/SNMP* Select the MIB table in which the MIB variable whose value shall be changed is saved. First, select the **System**, then the **MIB Table**. Only the MIB tables present in the respective area are displayed.
Command Mode	Only if **Command Type** = *MIB/SNMP* Select how the MIB entry is to be manipulated. Possible settings: • *Change existing entry* (default value): An existing entry shall be modified. • *Create new MIB entry*: A new entry shall be created.
Index Variables	Only if **Command Type** = *MIB/SNMP* Where required, select MIB variables to uniquely identify a specific data set in **MIB Table**, e.g. *ConnIfIndex*. The unique identification of a particular table entry is derived from the combination of **Index Variable** (usually an index variable which is flagged with *) and **Index Value**.

Field	Description
	Use **Index Variables** to create more entries with **Add**.
Trigger Status	Only if **Command Type** = *MIB/SNMP* Select what status the event must have in order to modify the MIB variable as defined. Possible values: • *Active* (default value): The value of the MIB variable is modified if the initiator is active. • *Inactive*: The value of the MIB variable is modified if the initiator is inactive. • *Both*: The value of the MIB variable is differentially modified if the initiator status changes.
MIB Variables	Only if **Command Type** = *MIB/SNMP* Select the MIB variable whose value is to be configured as dependent upon initiator status. If the initiator is active (**Trigger Status** *Active*), the MIB variable is described with the value entered in **Active Value**. If the initiator is inactive (**Trigger Status** *Inactive*), the MIB variable is described with the value entered in **Inactive Value**. If the MIB variable is to be modified, depending on whether the initiator is active or inactive (**Trigger Status** *Both*), it is described with an active initiator with the value entered in **Active Value** and with an inactive initiator with the value in **Inactive Value**. Use **Add** to create more entries.
Interface	Only if **Command Type** = *Interface Status* Select the interface whose status should be changed.
Set interface status	Only if **Command Type** = *Interface Status* Select the status to be set for the interface. Possible values:

Field	Description
	• *Up* (default value) • *Down* • *Reset*
Local WLAN SSID	Only if **Command Type** = *Wlan Status* Select the desired wireless network whose status shall be changed.
Set status	Only if **Command Type** = *Wlan Status* or *WLC: VSS State* Select the status for the wireless network. Possible values: • *Activate* (default value) • *Deactivate*
Source Location	Only if **Command Type** = *Software Update* Select the source for the software update. Possible values: • *Current Software from Update Server* (default value): The latest software will be downloaded from the update server. • *HTTP Server*: The latest software will be downloaded from an HTTP server that you define in *Server URL*. • *HTTPS Server*: The latest software will be downloaded from an HTTPS server that you define in *Server URL*. • *TFTP Server*: The latest software will be downloaded from an TFTP server that you define in *Server URL*.
Server URL	Where **Command Type** = *Software Update* if **Source Location** not *Current Software from Update Server* Enter the URL of the server from which the desired software version is to be retrieved. Where **Command Type** = *Configuration Management* with **Action** = *Import configuration* or *Export configuration*

Field	Description
	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.
File Name	For **Command Type** = *Software Update* Enter the file name of the software version. Where **Command Type** = *Certificate Management* with **Action** = *Import certificate* Enter the file name of the certificate file.
Action	For **Command Type** = *Configuration Management* Select which operation is to be performed on a configuration file. Possible values: • *Import configuration* (default value) • *Export configuration* • *Rename configuration* • *Delete configuration* • *Copy configuration* For **Command Type** = *Certificate Management* Select which operation you wish to perform on a certificate file. Possible values: • *Import certificate* (default value) • *Delete certificate* • *SCEP*
Protocol	Only for **Command Type** = *Certificate Management* and *Configuration Management* if **Action** = *Import configuration* Select the protocol for the data transfer. Possible values:

Field	Description
	• *HTTP* (default value) • *HTTPS* • *TFTP*
CSV File Format	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Select whether the file is to be sent in the CSV format. The CSV format can easily be read and modified. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The function is enabled by default.
Remote File Name	Only if **Command Type** = *Configuration Management* For **Action** = *Import configuration* Enter the name of the file under which it is saved on the server from which it is to be retrieved. For **Action** = *Export configuration* Enter the file name under which it should be saved on the server.
Local File Name	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration*, *Rename configuration* or *Copy configuration* At import, renaming or copying enter a name for the configuration file under which to save it locally on the device.
File Name in Flash	Where **Command Type** = *Configuration Management* and **Action** = *Export configuration* Select the file to be exported. Where **Command Type** = *Configuration Management* and **Action** = *Rename configuration* Select the file to be renamed.

Field	Description
	Where **Command Type** = *Configuration Management* and **Action** = *Delete configuration* Select the file to be deleted. Where **Command Type** = *Configuration Management* and **Action** = *Copy configuration* Select the file to be copied.
Configuration contains certificates/keys	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Select whether the certificates and keys contained in the configuration are to be imported or exported. The function is disabled by default.
Encrypt configuration	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* or *Export configuration* Define whether the data of the selected **Action** are to be encrypted.. The function is disabled by default.
Reboot after execution	Only if **Command Type** = *Configuration Management* Select whether your device should restart after the intended **Action**. The function is disabled by default.
Version Check	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration* 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. The function is disabled by default.
Destination IP Address	Only if **Command Type** = *Ping Test*

Field	Description
	Enter the IP address whose accessibility is to be checked.
Source IP Address	Only if **Command Type** = *Ping Test* Enter an IP address to be used as sender address for the ping test. Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Interval	Only if **Command Type** = *Ping Test* Enter the time in **Seconds** after which a ping must be resent. The default value is *1* second.
Count	Only if **Command Type** = *Ping Test* Enter the number of ping tests to be performed. The default value is *3*.
Server Address	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter the URL of the server from which a certificate file is to be retrieved.
Local Certificate Description	Where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter a description for the certificate under which to save it on the device. Where **Command Type** = *Certificate Management* and **Action** = *Delete certificate* Select the certificate to be deleted.
Password for protected Certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate*

Field	Description
	Select whether to use a secure certificate requiring a password and enter it into the entry field. The function is disabled by default.
Overwrite similar certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to overwrite a certificate already present on the your device with the new one. The function is disabled by default.
Write certificate in configuration	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to integrate the certificate in a configuration file; and if so, select the desired configuration file. The function is disabled by default.
Certificate Request Description	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a description under which the SCEP certificate on your device is to be saved.
URL SCEP Server URL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter the URL of the SCEP server, e.g. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Your CA administrator can provide you with the necessary data.
Subject Name	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a subject name with attributes. Example: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA Name	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP*

Field	Description
	Enter the name of the CA certificate of the certification authority (CA) from which you wish to request your certificate, e.g. *cawindows*. Your CA administrator can provide you with the necessary data.
Password	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* To obtain certificates, you may need a password from the certification authority. Enter the password you received from the certification authority here.
Key Size	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Select the length of the key to be created. Possible values are *1024* (default value), *2048* and *4096*.
Autosave Mode	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* 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. The function is enabled by default.
Use CRL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* 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. Possible values: • *Auto* (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. • *Yes*: CRLs are always checked.

Field	Description
	• *No*: No checking of CRLs.
Select radio	Only where **Command Type** = *5 GHz WLAN Bandscan*, *5.8 GHz WLAN Bandscan* or *WLAN: Operation Mode* Select the WLAN module on which to perform the frequency band scan.
WLC SSID	Only where **Command Type** = *WLC: VSS State* Select the wireless network administered over the WLAN controller whose status should be changed.
Operation Mode (Active)	Only where **Command Type** = *WLAN: Operation Mode* Select the required operating mode for the selected radio module if it currently has the status *Active*. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.
Operation Mode (Inactive)	Only where **Command Type** = *WLAN: Operation Mode* Select the required operating mode for the selected radio module if it currently has the status *Down*. You may select from any of the operating modes that your device supports. So the choice may vary from device to device.

17.7.3 Options

You configure the schedule interval in the **Local Services**->**Scheduling**->**Options** menu.

The menu consists of the following fields:

Fields in the Scheduling Options menu

Field	Description
Schedule Interval	Select whether the schedule interval is to be enabled. Enter the interval in seconds after which the system checks whether events have occured. Possible values are *0* to *65535*.

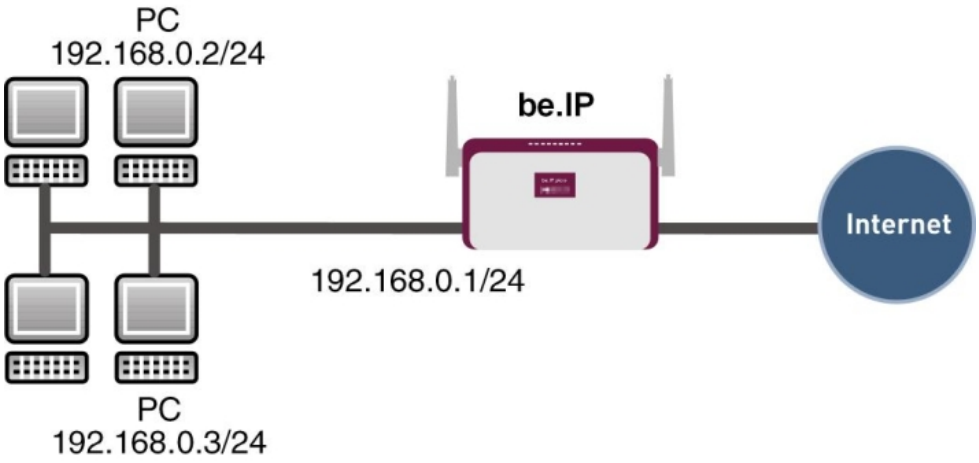
Field	Description
	The value *300* is recommended (5 minute accuracy).

17.7.4 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**	*New*
Description	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	e.g. *Trigger Reboot*
Event Type	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*Time*
Time Condition	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Condition Type = *Periods*, Condition Settings = *Daily*
Start Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *02* Minute *00*
Description	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *Reboot the devicet*
Command Type	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Reboot*
Event List	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Trigger Reboot*
Event List Condition	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*All*
Reboot device after	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *60* Seconds
Schedule Interval	**Local Services** -> **Scheduling** -> **Options**	*Enabled*, *55* sec

Suspending the WLAN interface

Field	Menu	Value
Event List	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*New*
Description	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	e.g. *Trigger switch off WLAN interface*
Event Type	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*Time*
Time Condition	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Condition Type = *Periods*, Condition Settings = *Saturday - Sunday*
Start Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *00* Minute *00*

Field	Menu	Value
Stop Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *23* Minute *59*
Description	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *Switch off WLAN interface*
Command Type	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Interface Status*
Event List	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Trigger switch off WLAN interface*
Event List Condition	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*All*
Interface	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *vss1-0*
Set interface status	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Down*
Schedule Interval	**Local Services** -> **Scheduling** -> **Options**	*Enabled*, *55* sec

Monthly configuration backup

Field	Menu	Value
Event List	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*New*
Description	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	e.g. *Trigger configuration backup*
Event Type	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	*Time*
Time Condition	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Condition Type = *Day of Month*, Condition Settings = *1*
Start Time	**Local Services** -> **Scheduling** -> **Trigger** -> **New**	Hour *03* Minute *00*
Description	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Configuration backup
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** ->	All

Field	Menu	Value
	Actions -> **New**	
Action	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Export configuration
Server URL	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *tftp://192.168.2.5*
CSV File Format	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Enabled*
Remote File Name	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *monthly-backup.cf*
File Name in Flash	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*boot*
Configuration contains certificates/keys	**Local Services** -> **Scheduling** -> **Actions** -> **New**	*Enabled*
Schedule Interval	**Local Services** -> **Scheduling** -> **Options**	*Enabled*, *55* sec

17.8 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.

17.8.1 Hosts

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Hosts** menu.

17.8.1.1 Edit or New

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

The menu **Local Services**->**Surveillance**->**Hosts**->**New** consists of the following fields:

Fields in the Host Parameters menu

Field	Description
Group ID	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. 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 *New ID* option. If entries have been created, you can select one from the list of created groups. Each host to be monitored must be assigned to a group. The operation configured for the select **Interface** is only executed if no group member can be reached.

Fields in the Trigger menu.

Field	Description
Monitored IP Address	Enter the IP address of the host to be monitored. Possible values: • *Default Gateway* (default value): The default gateway is monitored. • *Specific*: Enter the IP address of the host to be monitored manually in the adjacent input field.
Source IP Address	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. Possible values: • *Automatic* (default value): The IP address is determined automatically. • *Specific*: Enter the IP address in the adjacent input field.
Interval	Enter the time interval (in seconds) to be used for checking the availability of hosts. Possible values are *1* to *65536*.

Field	Description
	The default value is *10*. Within a group, the smallest **Interval** of the group members is used.
Successful Trials	Specify how many pings need to be answered for the host to be regarded as accessible. 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. Possible values are *1* to *65536*. The default value is *3*.
Unsuccessful Trials	Specify how many pings need to be unanswered for the host to be regarded as inaccessible. 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. Possible values are *1* to *65536*. The default value is *3*.
Action to be performed	Not for **Action** = *Monitor*. Select which **Action** should be execude, when the Host is regarded as inaccessible. For most actions, you select an **Interface** to which the **Action** relates. All IP interfaces can be selected. For each interface, select whether it is to be enabled (*Enable*), disabled (*Disable* default value), reset (*Reset*), or the connection restablished (*Redial*). The **Actions** *Enable* and *Disable* are also cancelled if the hosts is regarded as accessible again. With **Action** = *Monitor* you can monitor the IP address that is specified under **Monitored IP Address**. This information can be used for other functions, such as the **Tracking IP Address**

Field	Description
	used in IP Load Balancing.

17.8.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Interfaces** menu.

17.8.2.1 Edit or New

Choose the icon to edit existing entries. Choose the **New** button to set up monitoring for other interfaces.

The menu **Local Services**->**Surveillance**->**Interfaces**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Monitored Interface	Select the interface on your device that is to be monitored.
Trigger	Select the state or state transition of **Monitored Interface** that is to trigger a particular **Interface Action**. Possible values: • *Interface goes up* (default value) • *Interface goes down*
Interface Action	Select the action that is to follow the state or state transition defined in **Trigger**. The action is applied to the Interface(s) selected in **Interface**. Possible values: • *Enable* (default value): Activation of interface(s) • *Disable*: Deactivation of interface(s)
Interface	Select the interface(s) for which the action defined in **Interface** is to be performed. You can choose all physical and virtual interfaces as well as options *All PPP Interfaces* and *All IPSec Interfaces*.

17.8.3 Ping Generator

In the **Local Services**->**Surveillance**->**Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

17.8.3.1 Edit or New

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

The menu **Local Services**->**Surveillance**->**Ping Generator**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.
Source IP Address	Enter the source IP address of the outgoing ICMP echo request packets. Possible values: • *Automatic*: The IP address is determined automatically. • *Specific* (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.
Interval	Enter the interval in seconds during which the ping is sent to the address specified in **Remote IP Address**. Possible values are *1* to *65536*. The default value is *10*.
Trials	Enter the number of ping tests to be performed. The default value is *3*.

17.9 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 into the LAN by ISDN if under **WAN**->**Internet + Dialup**->**ISDN**-> the field **Always on** is activated.)

17.9.1 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.

The menu **Local Services**->**ISDN Theft Protection**->**Options** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
ISDN Theft Protection Service	Enable or disable the ISDN theft protection function. The function is enabled with *Enabled*. The function is disabled by default.
Dialling Number	Only if **ISDN Theft Protection Service** is enabled. Enter the subscriber number that the gateway dials to call itself.
Incoming Number	Only if **ISDN Theft Protection Service** is enabled. Enter the subscriber number to be compared with the current

Field	Description
	calling party number.
Outgoing Number	Only if **ISDN Theft Protection Service** is enabled. Enter the subscriber number to be set as calling party number.
Monitored Interfaces	Only if **ISDN Theft Protection Service** is enabled. Use **Add** 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
Number of Dialling Retries	Enter the number of dial attempts that the gateway is to make to call itself by ISDN after a reboot. Possible values are `1` to `255`. The default value is `3`.
Timeout	Enter the time in seconds that the gateway is to wait before trying again after an unsuccessful attempt to call itself. Possible values are `2` to `20`. The default value is `5`.

17.10 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*.

17.10.1 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 menu **Local Services**->**UPnP**->**Interfaces** consists of the following fields:

Fields in the Interfaces menu.

Field	Description
Interface	Shows the name of the interface for which the UPnP settings are to be made. The entry cannot be changed.
Answer to client request	Determine whether UPnP requests from clients are to be answered via the particular interface (from the local network). The function is enabled with *Enabled*. The function is disabled by default.
Interface is UPnP controlled	Determine whether the NAT configuration of this interface is controlled by UPnP. The function is enabled with *Enabled*.

Field	Description
	The function is disabled by default.

17.10.2 General

In this menu, you make the basic UPnP settings.

The **Local Services**->**UPnP**->**General** menu consists of the following fields:

Fields in the General menu.

Field	Description
UPnP Status	Decide how the gateway processes UPnP requests from the LAN. The function is enabled with *Enabled*. 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. The function is disabled by default. The gateway rejects UPnP requests, NAT releases are not made.
UPnP TCP Port	Enter the number of the port on which the gateway listens for UPnP requests. The possible values are *1* to *65535*, the default value is *5678*.

17.11 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 elmegbintec elmeg Hotspot hosting (article number 5510000198)
- Access data
- Documentation
- Software licensing

  Please note that you must first activate the licence.

  Go to *www.bintec-elmeg.com* then **Service/Support** -> **Services** -> **Online Services**.

  - Enter the required data (please note the relevant explanations on the license sheet), and follow the instructions of the online licensing.

  - You then receive the Hotspot server's login data.

Note

Activation may require 2-3 business days.

Access data for gateway configuration

RADIUS Server IP	62.245.165.180
RADIUS Server Password	Set by bintec elmeg GmbH
Domain	Individually set for customers by customer/dealer
Walled Garden Network	Individually set for customers by customer/dealer
Walled Garden Server URL	Individually set for customers by customer/dealer
Terms & Conditions URL	Individually set for customers by customer/dealer

Access data for configuration of the Hotspot server

Admin URL	https://hotspot.bintec-elmeg.com/
Username	Individually set by bintec elmeg
Password	Individually set by bintec elmeg

Note

Also refer to the WLAN Hotspot Workshop that is available to download from *www.bintec-elmeg.com*

17.11.1 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.

You can use the **Enabled** option to enable or disable the corresponding entry.

17.11.1.1 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.

The **Local Services**->**HotSpot Gateway**->**HotSpot Gateway**-> menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Choose the interface to which the Hotspot LAN or WLAN is connected. When operating over LAN, enter the Ethernet interface here (e. g. en1-0). If operating over WLAN, the WLAN interface to which the access point is connected must be selected. **Caution** 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. 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.
Domain at the HotSpot Server	Enter the domain name that you used when setting up the HotSpot server for this customer. The domain name is required so that the Hotspot server can distinguish between the different clients (customers).
Walled Garden	Enable this function if you want to define a limited and free area of websites (intranet). The function is not activated by default.
Walled Network / **Netmask**	Only if **Walled Garden** is enabled. Enter the network address of the **Walled Network** and the corresponding **Netmask** of the intranet server. For the address range resulting from **Walled Network** / **Net-**

Field	Description
	mask, clients require no authentication. 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.
Walled Garden URL	Only if **Walled Garden** is enabled. Enter the **Walled Garden URL** of the intranet server. Freely accessible websites must be reachable over this address.
Terms &Conditions	Only if **Walled Garden** is enabled. In the **Terms &Conditions** input field, enter the address of the general terms and conditions on the intranet server, or public server, e.g., http://www.webserver.de/agb.htm. The page must lie within the address range of the walled garden network.
Additional freely accessible Domain Names	Only if **Walled Garden** is enabled. Add further URLs or IP addresses with **Add**. The web pages can be accessed via these additional freely accessible addresses.
Post Login URL	Here you can specify the URL a user is redirected to after logging in to the Hotspot Solution.
Language for login window	Here you can choose the language for the start/login page. The following languages are supported: *English*, *Deutsch*, *Italiano*, *Français*, *Español*, *Português* and *Nederlands*. The language can be changed on the start/login page at any time.

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

Fields in the menu Advanced Settings

Field	Description
Ticket Type	Select the ticket type. Possible values:

Field	Description
	• *Voucher*: Only the user name must be entered. Define a default password in the input field. • *Username/Password* (default value): User name and password must be entered.
Allowed HotSpot Client	Here you can define which type of users can log in to the Hotspot. Possible values: • *All*: All clients are approved. • *DHCP Client*: Prevents users who have not received an IP address from DHCP from logging in.
Devices per ticket	Enter the maximum number of devices per ticket.
Login Frameset	Enable or disable the login window. The login window on the HTML homepage consists of two frames. When the function is enabled, the login form displays on the left-hand side. When the function is disabled, only the website with information, advertising and/or links to freely accessible websites is displayed. The function is enabled by default.
Pop-Up window for status indication	Specify whether the device uses pop-up windows to display the status. The function is enabled by default.
Default Idle Timeout	Enable or disable the **Default Idle Timeout**. If a hotspot user does not trigger any data traffic for a configurable length of time, they are logged out of the hotspot. The function is enabled by default. The default value is *600* seconds.

17.11.2 Options

In the **Local Services**->**HotSpot Gateway**->**Options** menu, general settings are performed for the hotspot.

The menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host for multiple locations	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.

17.12 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**.

17.12.1 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.

17.12.1.1 Edit or New

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

The **Local Services**->**Wake-On-LAN**->**Wake-On-LAN Filter**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter the name of the filter.
Service	Select one of the preconfigured services. The extensive range

Field	Description
	of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *Any*.
Protocol	Select a protocol. The option *Any* (default value) matches any protocol.
Type	Only for **Protocol** = *ICMP* Select the type. Possible values: *Any*, *Echo reply*, *Destination unreachable*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. See RFC 792. The default value is *Any*.
Connection State	With **Protocol** = *TCP*, you can define a filter that takes the status of the TCP connections into account. Possible values: • *Established*: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter. • *Any* (default value): All TCP packets match the filter.
Destination IPv4 Address/Netmask	Enter the destination IPv4 address of the data packets and the corresponding netmask. Possible values: • *Any* (default value): The destination IP address/netmask are

Field	Description
	not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the corresponding netmask.
Destination IPv6 Address/Length	Enter the destination IPv6 address of the data packets and the prefix length. Possible values: • *Any* (default value): The destination IP address/length are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the prefix length.
Destination Port/Range	Only for **Protocol** = *TCP*, *UDP* or *TCP/UDP* Enter a destination port number or a range of destination port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Source IPv4 Address/ Netmask	Enter the source IPv4 address of the data packets and the corresponding netmask. Possible values: • *Any* (default value): The source IP address/netmask are not specified. • *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the corresponding netmask.
Source IPv6 Address/ Length	Enter the source IPv6 address of the data packets and the prefix length. Possible values: • *Any* (default value): The source IP address/length are not specified.

Field	Description
	• *Host*: Enter the source IP address of the host. • *Network*: Enter the source network address and the prefix length.
Source Port/Range	Only for **Protocol** = *TCP*, *UDP* or *TCP/UDP* Enter a source port number or a range of source port numbers. Possible values: • *-All-* (default value): The source port is not specified. • *Specify port*: Enter a source port. • *Specify port range*: Enter a source port range.
DSCP/TOS Filter (Layer 3)	Select the Type of Service (TOS). Possible values: • *Ignore* (default value): The type of service is ignored. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	Enter the service class of the IP packets (Class of Service, CoS). Value range *0* to *7*. The default value is *0*.

Field	Description
	The default value is *Ignore*.

17.12.2 WOL Rules

The menu **Local Services**->**Wake-On-LAN**->**WOL Rules** displays a list of all the WOL rules that have been configured.

17.12.2.1 Edit or New

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

The **Local Services**->**Wake-On-LAN**->**WOL Rules**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Wake-On-LAN Rule Chain	Select whether to create a new rule chain or to edit an existing one. Possible values: • *New* (default value): You can create a new rule chain with this setting. • *<Name of the rule chain>*: Shows a rule chain that has already been created, which you can select and edit.
Description	Only where **Wake-On-LAN Rule Chain** = *New* Enter the name of the rule chain.
Wake-On-LAN Filter	Select a WOL filter. If the rule chain is new, select the filter to be set at the first point of the rule chain. If the rule chain already exists, select the filter to be attached to the rule chain. To select a filter, at least one filter must be configured in the **Local Services**->**Wake-On-LAN**->**WOL Rules** menu.

Field	Description
Action	Define the action to be taken for a filtered data packet. Possible values: • *Invoke WOL if filter matches*: Run WOL if the filter matches. • *Invoke if filter does not match*: Run WOL if the filter does not match. • *Deny WOL if filter matches*: Do not run WOL if the filter matches. • *Deny WOL if filter does not match*: Do not run WOL if the filter does not match. • *Ignore rule and skip to next rule*: This rule is ignored and the next one in the chain is examined.
Type	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 **Send WOL packet over Interface**.
Send WOL packet over Interface	Select the interface which is to be used to send the Wake on LAN magic packet.
Target MAC-Address	Only where **Action** = *Invoke WOL if filter matches* and *Invoke if filter does not match* Enter the MAC address of the network device that is to be enabled using WOL.
Password	Only where **Action** = *Invoke WOL if filter matches* and *Invoke if filter does not match* 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.

17.12.3 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.

17.12.3.1 Edit or New

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

The **Local Services**->**Wake-On-LAN**->**Interface Assignment**->**New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.

17.13 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 elmegbintec elmeg-specific implementation of the VRRP (Virtual Router Redundancy Protocol). A router redundancy procedure is used mainly to safeguard the availability of a physical gateway in a LAN or WAN.

Terms and Definitions

A number of special terms are used to describe the function. The following terms are defined in the relevant RFC and in the Internet draft.

BRRP terms

Field	Description
VRRP router	“A router that uses the Virtual Router Redundancy Protocol. It can be integrated into one or more “virtual routers”.”
Virtual Router	“An abstract object controlled by the VRRP, which is used as default router for the hosts of a LAN. It comprises a Virtual Router Identifier (**Virtual Router ID**) and an IP address or a group of associated IP addresses in a common LAN. A VRRP router can protect the data traffic of one or more virtual routers.”

Field	Description
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.”
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."

17.13.1 Virtual Routers

When using a route redundancy protocol, multiple routers are combined into a logical unit. The router redundancy protocol BRRP manages the routes involved and organises these as follows:

It ensures that only one routers within the logical connection is active.

It guarantees that if the active route fails, another router takes over the function of the failed device. The time that each router is active is determined by the priority assigned to the router.

Let us take the example of a simple scenario, in which gateway A provides Internet access for the hosts in a LAN. If this gateway fails, all hosts cannot access the Internet and their routes are configured statically. To allow the hosts continued access to the Internet, gateway B offers all hosts in the LAN the service that gateway A previously performed. All the tasks of a “virtual router” and the switching of services from one gateway to the other are controlled by the BRRP redundancy procedure.

The BRRP conforms to the specifications in RFC 2338 and the relevant Internet draft (see *www.ietf.org*).

The configuration of the router redundancy procedure is carried out in the following steps:

- Configuration of the interface via which the BRRP advertisement data packets are sent.

Note

This interface is used to transmit the BRRP advertisement data packets and possibly to transmit keepalive monitoring data packets. Another interface must be configured in the next step to transmit the usage data.

Configuration of the advertisement interface is performed in the **Local Services**->**BRRP**->**Virtual Router**->**New** menu under **BRRP Advertisement Interface**.

Only the active router in the router group sends advertisement data packets. The IPv4 multicast address 224.0.0.18 is used as the destination address for all routers in the group. All passive routers in the group must monitor this address so that if the advertisement data packets are not received that can react according to their priority and BRRP configuration.

- Configuration of the interface for transmitting usage data (configuration of the virtual interface).

  A virtual interface is activated and deactivated by assigning it to a virtual router over the BRRP router redundancy protocol.

  Configuration is performed in the **Local Services**->**BRRP**->**Virtual Router**->**New**->**Ethernet Interface** menu.

  In this step, you configure the IP address settings and assign the interface to a virtual router. The properties of the virtual router (e.g. the priority) are also defined here.

Note

The system automatically assigns the MAC address of the virtual interface according to the following model: 00:00:5E:00:01:<ID of the virtual router>. The ID of the virtual router therefore determines the MAC address of the interface, which is used to transmit the usage data.

The configuration of the virtual interface (MAC address, IP address) and the configuration of the virtual router (sending interval for advertisement, 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.)

17.13.1.1 New

Choose the **New** button to configure other virtual routers.

The **Local Services**->**BRRP**->**Virtual Routers**->**New** menu consists of the following fields:

Fields in the BRRP Advertisement Interface menu.

Field	Description
Ethernet Interface	Choose the interface via which BRRP advertisement packets are sent and expected. If you edit a Virtual Router, the Ethernet interface is displayed and cannot be changed. Please note: The Ethernet interface for sending the advertisements is always up and running and cannot therefore be used as the **Virtual Router Interface**.
IP Address	Shows the IP address(es) of the interface via which BRRP advertisement packets are sent and expected.

Fields in the BRRP Monitored Interface menu.

Field	Description
Virtual Router Interface	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. Shows the name of the virtual interface, if a virtual interface that has already been created is edited.
Virtual Router IP Address	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. **Note** To avoid problems in the LAN, the **IP Address** for advertisements and the **Virtual Router IP Address** cannot originate from the same subnet.
Virtual Router ID	Select the ID of the virtual router. This ID identifies the “virtual router” in the LAN and is part of every BRRP advertisement packet that is sent by the current master. Possible values are whole numbers between `1` and `255`.
Virtual Interface Priority	Define the transmitted BRRP priority of the interface for the virtual router. Higher priorities determine the master interfaces during the initialization pahse as well as with active Pre-Empt-Mode.Possible values are between `1` and `255`. The higher the value, the higher the priority. The value `255` defines that this virtual router always functions as master as soon as it is active. The default value is `100`. A priority of 255 is used for routers the IP address of which is idential with the IP address of the virtual router.

In the **Advanced Settings** menu you must configure all of the parameters for all virtual routers identically on all devices in the group. We recommend leaving the preset values.

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

Fields in the Advanced Settings menu.

Field	Description
Advertisement send interval	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. Possible values are whole numbers between `1` and `255`. The value is indicated in seconds and the default value is 1. `1`. An advertisement timer based on the sending interval for advertisements runs in the router and an advertisement packet is sent when the timer expires.
Master down trials	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. A master down timer based on the **Master down trials** parameter runs in the router; when this timer expires, the backup assumes that the master is not reachable if no advertisement has been received. The effective master down interval is the time calculated from the number of expected but omitted BRRP advertisements, the advertisement interval and the skew time, which adds a 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). Possible values are `1` to `255` and the default value is `10`.
Pre-empt mode (go back into master state)	Define whether a backup router with higher priority has priority over a master router with low priority. Pre-empt mode is used to prevent unnecessary switching. The function is enabled with `Enabled`. 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

Field	Description
	accessible once more, although the priority of the master router is higher than the priority of the backup router which is currently enabled. The function is enabled by default. Note the following exception: If **Virtual Interface Priority** *255* is selected, the gateway with this priority certainly takes over the master role, i.e. the setting in **Pre-empt mode (go back into master state)** is ignored. You should therefore select a **Virtual Interface Priority** lower than *255255*if you wish to use Pre-empt Mode.
Enable authentication	Enable or disable authentication. The function is enabled with *Enabled*. If the function is active, an input field is displayed. Enter the authentication key here. Please note: Note that the authentication key must be the same for all virtual routers in the group. The function is disabled by default.

17.13.2 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.

17.13.2.1 New

Select the **New** button to create new synchronisations.

The **Local Services**->**BRRP**->**VR Synchronisation**->**New** menu consists of the following fields:

Fields in the Monitoring VR / Interface menu.

Field	Description
Monitoring Mode	Shows which mechanism is used for monitoring a virtual router. Possible values: • *BRRP*:The BRRP-specific state advertisements are used for determining the state of the master. (The master sends advertisements as per its configuration in the **Local Services**->**BRRP**->**Virtual Routers**->**New**->**Advanced Settings** menu.)
Virtual Router ID	Select a virtual router using the **Virtual Router ID** and define which interface is to be checked. You can choose previously defined IDs (see **Virtual Router ID** in the **Local Services**->**BRRP**->**Virtual Router**->**New** menu under **BRRP Monitored Interface**). The watchdog daemon requests detailed information entered in the **Virtual Routers**.

Fields in the Synchronisation VR / Interface menu.

Field	Description
Synchronisation Mode	Indicates the mechanism with which virtual routers or interfaces are synchronised: Possible values: • *BRRP*: BRRP is used to synchronise the virtual router.
Virtual Router ID	Select the ID of the virtual router to be synchronised. Synchronising the virtual router implicitly synchronises the virtual interface associated with the virtual router.

17.13.3 Options

In the **Local Services**->**BRRP**->**Options** menu,you can enable or disable the BRRP function.

The menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Enable BRRP	Enable or disable the BRRP function. The function is enabled with *Enabled*. The function is disabled by default.

17.14 Trace Interface

The menu **Trace Interface** allows recording the data traffic of a specific interface and allows you to save the recording as a PCAP file once the process has been stopped.

17.14.1 Trace Interface

Fields in the Trace Settings menu

Field	Description
Interface Selection	Select the interface the data traffic of which is to be recorded.
Trace Mode	Here you can choose the layers on which the data traffic of the selected interface is to be recorded. Available choices are: • *Layer 2* • *PPP* • *Layer 3* • *IP*

As soon as you start the recording with the **START** button, a window informs you about the recording. During recording you can leave the menu and use the GUI as usual. Once you stop the recording with the **STOP** button, information on the created file is displayed and you can either delete ot save it as a PCAP file.

17.14.2 Trace VoIP/SIP

The menu **Trace VoIP/SIP** allows you to capture VoIP/SIP messages at various levels and save them to a text file on your computer. You can choose from the following capture levels, a description what information is written to the file is provided depending on your selection:

- State information: The device writes the current state of the VoIP/SIP subsystem to a file you can then download.
- Events: The device continuously writes VoIP/SIP information to the capture buffer as

soon as you click the Start button. Once you click the Stop button, you are presented with the download option.

- SIP: The device continuously writes all SIP messages (only) to the capture buffer as soon as you click the Start button. Once you click the Stop button, you are presented with the download option.

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.

Fields in the manu Log out Users

Field	Description
Class	Dislays the class the signed-on user belongs to.
User	Displays the user name.
Remote IP Address	Displays the IP address from which the connection has been established. This may be the address ofa PC, but it may also be the address of an intermediate router.
Expires	Displays when the connection will be automatically terminated by the device.
Log out immediately	If you activate the check box, this user will be disconnected from the system when you click **Logout**.

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.

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

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
Test Ping Mode	Select the IP version to be used for the ping test. Possible values: • *IPv4* • *IPv6*
Test Ping Address	Enter the IP address to be tested.
Use Interface	Only for **Test Ping Mode** = *IPv6* For link local addresses select the interface to be used for the ping test. *Default* 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 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

You use the traceroute test to display the route to a particular address (IP address or domain name), if this can be reached.

Fielder in the Traceroute Test menu

Field	Description
Traceroute Mode	Select the IP version to be used for the Traceroute test. Possible values: • *IPv4* • *IPv6*
Traceroute Address	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* . 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.

The **Maintenance**->**Software &Configuration**->**Options** menu consists of the following fields:

Fields in the Currently Installed Software menu.

Field	Description
BOSS	Shows the current software version loaded on your device.
System Logic	Shows the current system logic loaded on your device.
xDSL Logic	Shows the current version of the xDSL logic loaded on your device.

Fields in the Software and Configuration Options menu.

Field	Description
Action	Select the action you wish to execute. After each task, a window is displayed showing the other steps that are required. Possible values: • *No Action* (default value): • *Export configuration*: The configuration file **Current File Name in Flash** is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. • *Import configuration*: Under **Filename** select a configuration file you want to import. Please note: Click **Go** to first load the file under the name *boot* in the flash memory for the device. You must restart the device to enable it. Please note: The files to be imported must be in CSV format! • *Copy configuration*: The configuration file in the **Source File Name** field is saved as **Destination File Name**.

Field	Description
	• *Delete configuration*: The configuration in the **Select file** field is deleted. • *Rename configuration*: The configuration file in the **Select file** field is renamed to **New File Name**. • *Restore backup configuration*: Only if, under **Save configuration** with the setting *Save configuration and back up previous boot configuration* the current configuration was saved as boot configuration and the previous boot configuration was also archived. You can load back the archived boot configuration. • *Delete software/firmware*: The file in the **Select file** field is deleted. • *Import language*: You can import additional language versions of the **GUI** into your device. You can download the files to your PC from the download area at *www.bintec-elmeg.com* and from there import them to your device • *Update system software*: You can launch an update of the system software, the xDSL logic and the BOOTmonitor. • *Export configuration with state information*: The active configuration from the RAM is transferred to your local host. If you click the **Go** button, a dialog box is displayed, in which you can select the storage location on your PC and enter the desired file name. The following options require that an MMC/SD card is inserted (if supported by your device) or that your device is equipped with an additional internal storage. • *Import Voice Mail Wave Files*: In **file name**, select the *vms_wavfiles.zip* file that you wish to import. • *Import Additional Files (to usb storage)*: You can upload additional files to the USB memory. Choose which file to load under **File Name** • *Format MMC/SD Card*: Occasionally, the additional internal Flash memory has to be formatted. All stored data are deleted.
Current File Name in Flash	For **Action** = *Export configuration*

Field	Description
	Select the configuration file to be exported.
Include certificates and keys	For **Action** = *Export configuration*, *Export configuration with state information* Define whether the selected **Action** should also be applied for certificates and keys. The function is activated by selecting *Enabled*. The function is enabled by default.
Configuration Encryption	Only for **Action** = *Import configuration*, *Export configuration*, *Export configuration with state information*. Define whether the data of the selected **Action** are to be encrypted. The function is activated by selecting *Enabled*. The function is disabled by default. If the function is enabled, you can enter the **Password** in the text field.
Filename	Only for **Action** = *Import configuration*, *Import language Update system software*. Enter the path and name of the file or select the file with **Browse...** via the explorer/finder.
Source File Name	Only for **Action** = *Copy configuration* Select the source file to be copied.
Destination File Name	Only for **Action** = *Copy configuration* Enter the name of the copy.
Select file	Only for **Action** = *Rename configuration*, *Delete configuration* or *Delete software/firmware* Select the file or configuration to be renamed or deleted.
New File Name	Only for **Action** = *Rename configuration*

Field	Description
	Enter the new name of the configuration file.
Source Location	Only for **Action** = *Update system software* Select the source of the update. Possible values: • *Local File* (default value): The system software file is stored locally on your PC. • *HTTP Server*: The file is stored on a remote server specified in the **URL**. • *Current Software from Update Server*: The file is on the official update server.
URL	Only for **Source Location** = *HTTP Server* Enter the URL of the update server from which the system software file is loaded.

In the **Advanced Settings** menu, the version of the currently installed system flash files will be displayed.

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.

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.

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 Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at *www.bintec-elmeg.com*).

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.

The menu **External Reporting**->**Syslog**->**Syslog Servers**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
IP Address	Enter the IP address of the host to which syslog messages are passed.
Level	Select the priority of the syslog messages that are to be sent to the host. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* (default value) • *Debug* (lowest priority) Syslog messages are only sent to the host if they have a higher or identical priority to that indicated, i.e. at syslog level *Debug* all messages generated are forwarded to the host.
Facility	Enter the syslog facility on the host. This is only required if the **Log Host** is a Unix computer. Possible values: *local0 - 7* . The default value is *local0*.

Field	Description
Timestamp	Select the format of the time stamp in the syslog. Possible values: • *None* (default value): No system time indicated. • *Time*: System time without date. • *Date &Time*: System time with date.
Protocol	Select the protocol for the transfer of syslog messages. Note that the syslog server must support the protocol. Possible values: • *UDP* (default value) • *TCP*
Type of Messages	Select the message type. Possible values: • *System &Accounting* (default value) • *System* • *Accounting*

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.

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.

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
%I	Destination IP Address
%R	Destination Port
%F	Destination interface index
%p	Packets sent
%o	Octets sent
%P	Packets received

Field	Description
%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 -> %I:%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.

The menu **External Reporting**->**Alert Service**->**Alert Recipient**->**New** consists of the following fields:

Fields in the Add / Edit Alert Recipient menu.

Field	Description
Alert Service	Displays the alert service. You can select an alert service for devices with UMTS. Possible values: • E-mail • SMS
Recipient	Enter the recipient's e-mail address. The entry is limited to 40 characters.
Message Compression	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.

Field	Description
	Enable or disable the field. The function is enabled by default.
Subject	You can enter a subject.
Event	This feature is available only for devices with Wireless LAN Controller. Select the event to trigger an email notification. Possible values: • *Syslog contains string* (default value): A Syslog message includes a specific string. • *New Neighbor AP found*: A new adjacent AP has been found. • *New Rogue AP found*: 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. • *New AP (WTP) found*: A new unconfigured AP has reported to the WLAN. • *Managed AP offline*: A managed AP is no longer accessible.
Matching String	You must enter a "Matching String". This must occur in a syslog message as a necessary condition for triggering an alert. 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" entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter "*".
Severity	Select the severity level which the string configured in the **Matching String** field must reach to trigger an e-mail alert. Possible values: *Emergency* (default value), *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Information*, *Debug*
Monitored Subsystems	Select the subsystems to be monitored.

Field	Description
	Add new subsystems with **Add**.
Message Timeout	Enter how long the router must wait after a relevant event before it is forced to send the alert mail. Possible values are `0` to `86400`. The value `0` disables the timeout. The default value is `60`.
Number of Messages	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. Possible values are `0` to `99`; the default value is `1`.

19.3.2 Alert Settings

The menu **External Reporting**->**Alert Service**->**Alert Settings** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Alert Service	Select whether the alert service is to be enabled for the interface. The function is enabled with `Enabled`. The function is enabled by default.
Maximum E-mails per Minute	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
Sender E-mail Address	Enter the mail address to be entered in the sender field of the E-mail.
SMTP Server	Enter the address (IP address or valid DNS name) of the mail server to be used for sending the mails. The entry is limited to 40 characters.

Field	Description
SMTP Port	Encryption of e-mails (SSL / TLS). The field **SMTP Port** is per default preset to *25* and **SSL** Encryption is enabled.
SMTP Authentication	Authentication expected by the SMTP server. Possible values: • *None* (default value): The server accepts and send emails without further authentication. • *ESMTP*: The server only accepts e-mails if the router logs in with the correct user name and password. • *SMTP after POP*: The server requires that e-mails are called via POP3 by the sending IP with the correct POP3 user name and password before sending an e-mail.
User Name	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP* Enter the user name for the POP3 or SMTP server.
Password	Only if **SMTP Authentication** = *ESMTP* or *SMTP after POP* Enter the password of this user.
POP3 Server	Only if **SMTP Authentication** = *SMTP after POP* Enter the address of the server from which the e-mails are to be retrieved.
POP3 Timeout	Only if **SMTP Authentication** = *SMTP after POP* Enter how long the router must wait after the POP3 call before it is forced to send the alert mail. The default value is *600* seconds.

Fields in the SMS Parameters menu (for devices with UMTS only)

Field	Description
SMS Device	You can receive notification of system alerts in text messages. Select the device to be used to send the text message.
Maximum SMS per Day	Limit the maximum number of SMS sent during a single day.

Field	Description
	Activating *No Limitation* allows any number of SMS to be sent. The defualt value is 10 SMS per day. Note: Entering a value of *0* is equivalent to activating *No Limitation*.

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.

The menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
SNMP Trap Broadcasting	Select whether the transfer of SNMP traps is to be activated. Your device then sends SNMP traps to the LAN's broadcast address. The function is activated by selecting *Enabled*.

Field	Description
	The function is disabled by default.
SNMP Trap UDP Port	Only if **SNMP Trap Broadcasting** is enabled. Enter the number of the UDP port to which your device is to send SNMP traps. Any whole number is possible. The default value is *162*.
SNMP Trap Community	Only if **SNMP Trap Broadcasting** is enabled. 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. A character string of between *0* and *255* characters is possible. The default value is *SNMP Trap*.

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.

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.

Chapter 20 Monitoring

This menu contains information that enable you to locate problems in your network and monitor activities, e.g. at your device's WAN interface.

20.1 Internal Log

20.1.1 System Messages

In the **Monitoring**->**Internal Log**->**System Messages** menu, a list of all internally stored system messages is displayed. Above the table you will find the configured vales for the **Maximum Number of Syslog Entries** and **Maximum Message Level of Syslog Entries** fields. These values can be changed in the **System Management**->**Global Settings**->**System** menu.

Values in the System Messages list

Field	Description
No.	Displays the serial number of the system message.
Date	Displays the date of the record.
Time	Displays the time of the record.
Level	Displays the hierarchy level of the message.
Subsystem	Displays which subsystem of the device generated the message.
Message	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.

Values in the IPSec Tunnels list

Field	Description
Description	Displays the name of the IPSec tunnel.
Remote IP	Displays the IP address of the remote IPSec Peers.

Field	Description
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by clicking the ^ button or the v button in the **Action** column.

By clicking the Q button, you display detailed statistics on the IPSec connection.

Values in the IPSec Tunnels list

Field	Description
Description	Shows the description of the peer.
Local IP Address	Shows the WAN IP address of your device.
Remote IP Address	Shows the WAN IP address of the connection partner.
Local ID	Shows the ID of your device for this IPSec tunnel.
Remote ID	Shows the ID of the peer.
Negotiation Type	Shows the exchange type.
Authentication Method	Shows the authentication method.
MTU	Shows the current MTU (Maximum Transfer Unit).
Alive Check	Shows the method for checking that the peer is reachable.
NAT Detection	Displays the NAT detection method.
Local Port	Shows the local port.
Remote Port	Shows the remote port.
Packets	Shows the total number of incoming and outgoing packets.
Bytes	Shows the total number of incoming and outgoing bytes.
Errors	Shows the total number of errors.
IKE (Phase-1) SAs (x) **Role** / **Algorithm** / **Lifetime remaining** / **Status**	The parameters of the IKE (Phase 1) SAs are displayed here.
IPSec (Phase-2) SAs	Shows the parameters of the IPSec (Phase 2) SAs.

Field	Description
(x) **Role** / **Algorithm** / **Life-time remaining** / **Status**	
Messages	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.

The menu consists of the following fields:

Fields in the licenses menu

Field	Description
IPSec Tunnels	Shows the IPSec licenses currently in use (**In Use**) and the maximum number of licenses usable (**Maximum**).

Fields in the Peers menu

Field	Description
Status	Displays the number of IPSec tunnels by their current status. • **Up**: Currently active IPSec tunnels. • **Going up**: IPSec tunnels currently in the tunnel setup phase. • **Blocked**: IPSec tunnels that are blocked. • **Dormant**: Currently inactive IPSec tunnels. • **Configured**: Configured IPSec tunnels.

Fields in the SAs menu.

Field	Description
IKE (Phase-1)	Shows the number of active phase 1 SAs (**Established**) from the total number of phase 1 SAs (**Total**).
IPSec (Phase-2)	Shows the number of active phase 2 SAs (**Established**) from the total number of phase 2 SAs (**Total**).

Fields in the Packet Statistics menu.

Field	Description
Total	Shows the number of all processed incoming (**In**) or outgoing (**Out**) packets.

Field	Description
Passed	Shows the number of incoming (**In**) or outgoing (**Out**) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (**In**) or outgoing (**Out**) packets.
Encrypted	Shows the number of all incoming (**In**) or outgoing (**Out**) packets protected by IPSec.
Errors	Shows the number of incoming (**In**) or outgoing (**Out**) packets for which processing led to errors.

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.

Values in the Current Calls list

Field	Description
Service	Displays the service to or from which the call is connected: *PPP*, *IPSec*, *X.25*, *POTS*.
Remote Number	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).
Interface	Displays additional information for PPP connections.
Direction	Displays the send direction: *Incoming*, *Outgoing*.
Charge	Displays the costs of the current connection.
Duration	Displays the duration of the current connection.
Stack	Displays the related ISDN port (STACK).
Channel	Displays the number of the ISDN B channel.
Status	Displays the state of the connection: *null*, *c-initiated*, *ovl-send*, *oc-procd*, *c-deliverd*, *c-present*, *c-recvd*, *ic-procd*, *up*, *discon-req*, *discon-ind*, *suspd-req*, *resum-req*, *ovl-recv*.

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.

Values in the Call History list

Field	Description
Service	Displays the service to or from which the call was connected: *PPP*, *IPSec*, *X.25*, *POTS*.
Remote Number	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).
Interface	Displays additional information for PPP connections.
Direction	Displays the send direction: *Incoming*, *Outgoing*.
Charge	Displays the costs of the connection.
Start Time	Displays the time at which the call was made or received.
Duration	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.

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

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.

Field	Description
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Click the button to display the statistical data for the individual interfaces in detail.

Values in the Statistics list

Field	Description
Description	Displays the name of the interface.
MAC Address	Displays the MAC address.
IP Address / Netmask	Shows the IP address and the netmask.
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections menu

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.
Remote Port	Displays the port to which an active TCP connection exists.

20.4.2 Network Status

The menu **Monitoring**->**Interfaces**->**Network Status** provides an overview of all IP interfaces currently configured on the device. You can find information on the status of an interface as well as on relevant parameters like its IPv4 and/or IPv6 IP address, the MAC address of the interface and the currently valid MTU.

20.5 Bridges

20.5.1 br<x>

In the **Monitoring**->**Bridges**-> **br<x>** menu, the current values of the configured bridges are shown.

Values in the br<x> list

Field	Description
MAC Address	Shows the MAC addresses of the associated bridge.
Port	Shows the port on which the bridge is active.

20.6 HotSpot Gateway

20.6.1 HotSpot Gateway

A list of all linked hotspot users is displayed in the **Monitoring**->**HotSpot Gateway**->**HotSpot Gateway** menu.

Values in the HotSpot Gateway list

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Displays the time of the notification.
Interface	Shows the interface used.

20.7 QoS

In the **Monitoring**->**QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

20.7.1 QoS

A list of all interfaces for which QoS was configured is displayed in the **Monitoring**->**QoS**->**QoS** menu.

Values in the QoS list

Field	Description
Interface	Shows the interface for which QoS has been configured.
QoS Queue	Shows the QoS queue, which has been configured for this interface.
Send	Shows the number of sent packets with the corresponding packet class.
Dropped	Shows the number of rejected packets with the corresponding packet class in case of overloading.
Queued	Shows the number of waiting packets with the corresponding packet class in case of overloading.

20.8 OSPF

In the **Monitoring**->**OSPF** menu information on OSPF is monitored . The OSPF monitor is arranged horizontally in three sections and shows information about OSPF interfaces, the detected neighbor and the LinkStateDatabase entries.

20.8.1 Status

In the **Monitoring**->**OSPF**->**Status** menu, a list of all interfaces configured for OSPF is displayed.

Values in the Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: *All*, *OSPF Interfaces*, *OSPF Neighbors*

Field	Description
	and *OSPF Link State Database*

In the **OSPF Interfaces** area all enabled OSPF interfaces are listed:

Values in the OSPF Interfaces list

Field	Description
Interface	Shows the interface for which OSPF has been configured.
Designated Router	Shows the IP address of the designated router. The designated router generates network links and distributes these to all gateways within the BMA network (BMA = Broadcast Multi Access Network, e.g. Ethernet, FDDI, Tokenring). A designated router is not shown for non-BMA networks, e.g. X.25, Frame Relay, ATM.
Backup Designated Router	Shows the IP address of the backup designated router.
Admin Status	Shows the OSPF Admin Status (*active* or *passive*) of the interface.
State	The OSPF status of the interface displayed here can take on the following values: • *Down*: OSPF is not running on this interface. • *Waiting*: The initial phase of the OSPF, in which the DR and BDR are determined. • *Point-to-point*: The interface is a point-to-point interface. DR or BDR are not shown. • *Designated Router*: The gateway is the designated router within the BMA network. • *Designated Router Backup*: The gateway is the backup designated router within the BMA network. • *Other Designated Router*: Another gateway is designated router or backup designated router within the BMA network.

The **Neighbor** section lists the neighbor gateways that have been identified via the HELLO protocol.

Values in the OSPF Neighbors list

Field	Description
Neighbor	Shows the IP address of the neighbor gateway.
Router ID	Shows the system-wide router ID of the neighbor gateway.
Interface	Indicates the interface over which the neighbor gateway was identified.
State	The OSPF status with this neighbor gateway can have the following values: • *Down*: The connection to this OSPF neighbor is inactive. • *Init*: The initial phase. A HELLO packet is received from the neighbor. • *Bidirectional*: Bidirectional communication with the neighbor. The HELLO packets sent are accepted by the neighbor gateway (with correct parameters). • *Start Exchange*: The exchange of Database Description packets between the gateways has started. • *Exchange*: Active exchange of Database Description packets with the neighbor. • *Loading*: The gateway now exchanges Link State Advertisements with the neighbor. • *Complete*: The Link State Databases of the gateway and its neighbor are now synchronized.

The headers of all Link State Advertisements (LSA) are listed in the section for the Link State Database.

Values in the OSPF Link State Database list

Field	Description
Area	Indicates the area database to which the LSA is assigned.
Type	Indicates the LSA type. There are five LSA types: Router Link, Network Link, Summary Link, Summary ASBR, and AS External.
Link State ID	The Link State ID of the LSA. The meaning of the Link State ID depends on the type of advertisement.
Router ID	Identifies the gateway that has generated this LSA.
Sequence Age	The age of the LSA (in seconds)

20.8.2 Statistics

In the **Monitoring**->**OSPF**->**Statistics** menu, current values and activities are displayed.

Values in the Statistics list

Field	Description
Received Hello Messages	Displays the number of Hello packets received.
Sent Hello Messages	Displays the number of Hello packets sent.
Received Database Description Packets	Displays the number of received databank entries.
Sent Database Description Packets	Displays the number of sent databank entries.
Received Link State Acknowledge Packets	Displays the number of Link State Acknowlede packets received.
Sent Link State Acknowledge Packets	Displays the number of Link State Acknowlede packets sent.
Received Link State Request Packets	Displays the number of Link State Request packets received.
Sent Link State Request Packets	Displays the number of Link State Request packets sent.
Received Link State Update Packets	Displays the number of Link State Update packets received.
Sent Link State Update Packets	Displays the number of Link State Update packets sent.
Routing table updates caused by Summary Links Advertisements	Displays the number of incremental routing table updates performed when new Summary Link Advertisements have been received.
Routing table updates caused by External Advertisements	Displays the number of incremental routing table updates performed when new external Advertisements have been received.

20.9 PIM

20.9.1 Global Status

The status of all configured PIM components is displayed in the **Monitoring**->**PIM**->**Global Status** menu.

Values in the Global Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: *All*, *PIM Interfaces*, *PIM Neighbors* and *Multicast Group / RP Mappings*

Values in the PIM Interfaces list

Field	Description
Interface	Displays the name of the PIM interface.
IP Address	Displays the primary IP address of the PIM interface.
Designated Router	Displays the primary IP address of the designated router on this PIM interface.

Values in the PIM Neighbors list

Field	Description
Interface	Displays the interface via which the PIM Neighbor is reached.
Generation ID	Displays the ID of the neighbor gateway.
IP Address	Displays the primary IP address of the PIM Neighbor.
Uptime	Indicates how long the last PIM Neighbor is a neighbor of the local router.
Expiry Timer	Indicates when the PIM Neighbor is no longer entered as neighbor. If the value *0* is displayed, the PIM Neighbor always remains entered as neighbor.

Values in the Multicast Group / RP Mappings list

Field	Description
Multicast Group Address	Displays the multicast group address.
Multicast Group Prefix Length	Displays the related network mask.
Rendezvous Point IP	Displays the IP address of the Rendezvous point.

Field	Description
Address	

20.9.2 Not Interface-Specific Status

The menu **Monitoring**->**PIM**->**Not Interface-Specific Status** includes status information for all PIM interfaces.

Values in the Not Interface-Specific Status list

Field	Description
View	Select the desired view from the dropdown menu. Are available: *All*, *(*,*,RP) States*, *(*,G) States*, *(S,G) States* and *(S,G,RPT) States*

Values in the (*,*,RP) States list

Field	Description
Rendezvous Point IP Address	Displays the IP address of the Rendezvous Point (RP) for the group.
Upstream Join State	The Upstream (*,*,RP) Join/Prune Status indicates the status of the Upstream (*,*,RP) State Machine in the PIM-SM Specification.
Upstream Neighbor IP Address	Displays the primary IP address of the Upstream Neighbors, or unknown (0) if the Upstream Neighbor IP address is not known, or if it is not a PIM Neighbor.
Uptime	Indicates the timespan of the RP's existence.
Upstream Join Timer	Join/Prune Timer is used to periodically send Join(*,*,RP) messages, and to correct Prune(*,*,RP) messages from peers on an Upstream LAN interface.

Values in the (*,G) States list

Field	Description
Multicast Group Address	Displays the multicast group address.
Upstream Neighbor IP Address	Displays the primary IP address of the Neighbor on pimStarGRPFIfIndex, to which the local router periodically (*,G) sends Join messages. The InetAddressType is defined through the pimStarGUpstreamNeighborType. In the PIM-SM specification,

Field	Description
	this address is named RPF'(*,G).
Reverse-Path-Forwarding (RPF)	Indicates the address type of the RPF Next Hop to the RP, or unknown(0), if the Next Hop is not known.
Upstream Join State	Indicates whether the local router should join the group's RP Tree. This corresponds to the status of the Upstream (*,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Join Timer	Indicates the remaining time until the local router sends out the next periodic (*,G) Join message on pimStarGRPFIfIndex. In the PIM-SM specification, this address is named (*,G) Upstream Join Timer. If the timer is deactivated, it has the value `0`.

Values in the (S,G) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimSGAddressType object.
Source IP Address	Displays the source IP address. InetAddressType is defined in the pimSGAddressType object.
Upstream Neighbor IP Address	Displays the primary IP address of the Neighbor on pimSGRPFIfIndex, to which the router periodically (S,G) sends Join messages. The value is `0`, if the RPF Next Hop is unknown or is no PM Neighbor. InetAddressType is defined in the pimSGAddressType object. In the PIM-SM specification, this address is named RPF'(S,G).
Upstream Join State	Indicates whether the local router should join the Shortest-Path-Tree for the source and the group represented by this entry. This corresponds to the status of the Upstream (S,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Join Timer	Indicates the remaining time until the local router sends out the next periodic (S,G) Join message on pimSGRPFIfIndex. In the PIM-SM specification, this timer is named (S,G) Upstream Join Timer. If the timer is deactivated, it has the value `0`.
Shortest Path Tree	Indicates whether the Shortest Path Tree Bit is set, i.e. whether forwarding via the Shortest Path Tree should take place.

Values in the (S,G,RPT) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimStarGAddressType object.
Source IP Address	Displays the source IP address. InetAddressType is defined in the pimStarGAddressType object.
Reverse-Path-Forwarding (RPF)	Indicates the address type of the RPF Next Hop to the RP, or unknown(0), if the RPF Next Hop is not known.
Uptime	Indicates the timespan since the entry was generated by the local router.
Upstream Override Timer	Indicates the remaining time until the local router sends out the next Triggered (S,G, rpt) Join message on pimSGRPFIfIndex. In the PIM-SM specification, this timer is named (S,G, rpt) Upstream Override Join Timer. If the timer is deactivated, it has the value *0*.

20.9.3 Interface-Specific States

The menu **Monitoring**->**PIM**->**Interface-Specific States** includes interface-specific status information.

Values in the Interface-Specific States list

Field	Description
View	Select the desired view from the dropdown menu. Are available: *All*, *(*,G,I) States*, *(S,G,I) States* and *(S,G,RPT) States*

Values in the (*,G,I) States list

Field	Description
Multicast Group Address	Displays the multicast group address. InetAddressType is defined in the pimStarGAddressType object.
Interface	Displays the name of the interface.
Join/Prune State	Indicates the status that results from the (*,G) Join/Prune messages received on this interface. This corresponds to the status of the Downstream Per-Interface (*,G) State Machine in the PIM-SM specification.
Uptime	Indicates the timespan since the entry was generated by the local router.
Expiry Timer	Displays the remaining time until the (*,G) Join State becomes

Field	Description
	invalid for this interface. In the PIM-SM specification, this address is named (*,G) Join Expiry Timer. If the timer is deactivated, it has the value `0`. The value 'FFFFFFFF'h stands for infinite.
Assert State	Displays the (*,G) Assert State for this interface. This corresponds to the status of the Per-Interface (*,G) Assert State Machinen in the PIM-SM specification. If pimStarGPimMode is 'bidir', this object must 'noInfo' be.
Assert Winner IP Address	Indicates the address of Assert Winner, if pimStarGIAssertState runs 'iAmAssertLoser'. InetAddressType is defined through the object pimStarGIAssertWinnerAddressType.

Values in the (S,G) States list

Field	Description
Multicast Group Address	Displays the multicast IP address. InetAddressType is defined through the object pimSGAddressType.
Source IP Address	Displays the source IP address. InetAddressType is defined through the object pimSGAddressType.
Interface	Displays the name of the interface.
Join/Prune State	Indicates the status that results from the (S,G) Join/Prune messages received on this interface. This corresponds to the status of the Downstream Per-Interface (S,G) State Machine in the PIM-SM and PIM-DM.
Uptime	Indicates the time remaining before the local router reacts to an (S,G) Prune message received on this interface. The router waits this period to check whether another downstream router corrects the Prune message. In the PIM-SM specification, this timer is named (S,G) Prune-Pending Timer. If the timer is deactivated, it has the value `0`.
Expiry Timer	Displays the remaining time until the (S,G) Join State becomes invalid for this interface. In the PIM-SM specification, this timer is named (S,G) Join Expiry Timer . If the timer is deactivated, it has the value `0`. The value 'FFFFFFFF'h stands for infinite. In the PIM-DM specification, this timer is named (S,G) Prune Timer.
Assert State	Displays the (S,G) Assert State for this interface. This corresponds to the status of the Per-Interface (S,G) Assert State Machine in der PIM-SM Specification See "I-D.ietf-pim-sm-v2-new section 4.6.1"

Field	Description
Assert Winner IP Address	Indicates the address of Assert Winner, if pimStarGIAssertState runs 'iAmAssertLoser. InetAddressType is defined through the object pimSGIAssertWinnerAddressType.

Values in the (S,G,RPT) States list

Field	Description
Multicast Group Address	Displays the multicast IP address. InetAddressType is defined through the object pimSGAddressType.
Source IP Address	Displays the source IP address. InetAddressType is defined through the object pimStarGAddressType.
Interface	Displays the name of the interface.
Uptime	Indicates the timespan since the entry was generated by the local router.
Join/Prune State	Indicates whether the local router should sever the source of the RP tree. This corresponds in the PIM-SM specification to the status of the Upstream (S,G,rpt) State Machine for Triggered Messages.
Expiry Timer	Displays the remaining time until the (S,G, rpt) Prune State becomes invalid for this interface. In the PIM-SM specification, this timer is named (S,G, rpt) Prune Expiry Timer. If the timer is deactivated, it has the value `0`. The value 'FFFFFFFF'h stands for infinite. In the PIM-DM specification, this timer is named (S,G) Prune Timer.

Index