bintec elmeg.

Manual
elmeg hybird 120 / hybird 130

Copyright© Version 10.2.2 RC 01/2018 bintec elmeg GmbH

Legal Notice

Warranty

This publication is subject to change.

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

Copyright © bintec elmeg GmbH.

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

Open source software in this product

Along with other components, this product contains open source software that has been developed by third party suppliers and which is licensed under an open source software license. These open source software files are subject to copyright. For a current list of the open source software programs and the open source software licenses, go to *www.bintec-elmeg.com* .

GEMA

This product uses internal music for calls on hold for which approval from GEMA (German Society for Musical Performance and Mechanical Reproduction Rights) is not required. This has been confirmed by GEMA with the following approval certification. The approval certification can be viewed at the following web address: *www.bintec-elmeg.com* . System hold music: elmeg Song, Hold the line.

Table of Contents

Chapter 1 Installation

1.1 Introduction

This chapter will show you how to set your device up, connect it and get it working in just a few minutes.

We shall then explain, step-by-step, more detail about the configuration. No particular in-depth knowledge of telephone systems or routers is required. A detailed online help system gives you extra support.

1.2 Setting up and connecting

A number of connection variants are available to you with the **hybird 120** / **hybird 130**: Firstly, connection to an ISDN exchange connection through using an ADSL connection. Then you can use both IP telephony and classical ISDN for telephone connections. As an alternative to the ISDN connection, an external analogue connection (FXO) is also provided for this variant. You can also operate the **hybird 120** / **hybird 130** on a pure IP connection. You then only make calls via VoIP, but there are no restrictions in connecting your terminals in comparison with the first variant: You can connect SIP, analogue and ISDN terminals and PCs.
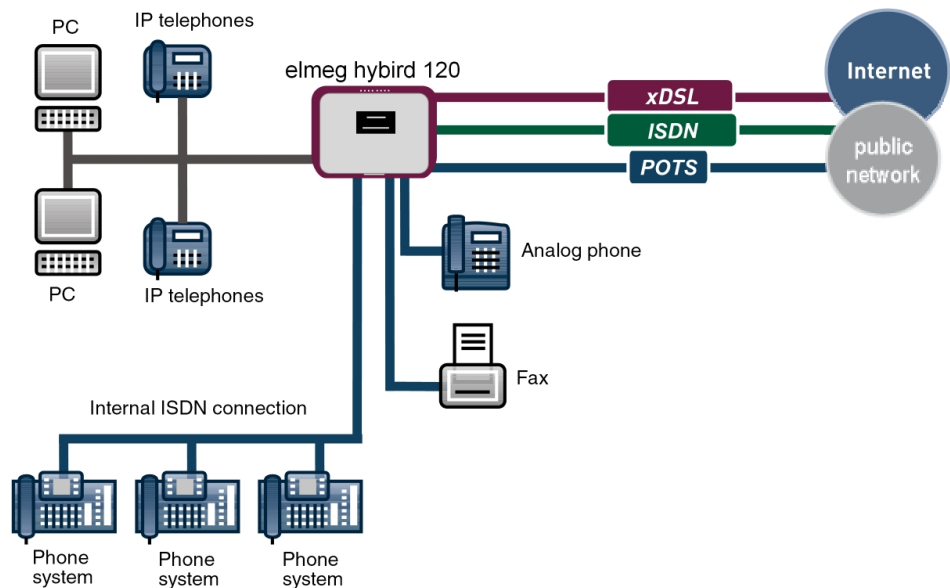
> ⚠ **Caution**
>
> Please read the safety instructions carefully before installing and starting up your device.

> ⚠ **Caution**
>
> Using an incorrect power supply unit may damage your device! You should only use the power supply unit provided!
>
> Incorrect cabling of the telephone and LAN interface may also damage your device. You should only ever connect the device's LAN interfaces to the LAN interface on the PC, and only connect the device's external ISDN interface to the external telephone connection (that is, the provider's connection).

Set up and connect in the following sequence:

(1) Installation: When operational, the device must be securely attached to a wall (please read chapter *Mounting* on page 16 carefully).

(2) LAN: To configure your device via Ethernet, use a suitable network cable to connect the PC's Ethernet port to one of the device's 10/100/1000 Base-T Ethernet interfaces (9-12).

(3) Mains connection: Connect the network connection on the device (1) with the power supply unit provided to a 230 V mains socket.

Optional connections

- DSL: If you wish to use the internal ADSL modem, use the yellow cable provided to connect the DSL interface on the device (13) to the DSL socket on the splitter or the relevant wall connection.

- SIP telephones: Connect your SIP telephones to the 10/100/1000 Base-T Ethernet interfaces (9-12).

- Analogue telephones/fax machines: Connect your analogue terminals to the internal interfaces for analogue terminals (4-5). To do this, use the cable provided with the terminal. Other analogue terminals can be connected to the device by clips.

- ISDN telephones: Connect ISDN telephones to the internal ISDN connector (6).

- External ISDN connection: If you have ordered an external ISDN connector, use the cable provided to connect the interface for external phone cables on the device (7) to your phone socket.

- Analogue telephone connection: If you have an analogue phone connection, connect the

FXO interface (2) to the phone socket using a suitable cable. Please note that the FXO socket is an RJ12 socket.

Your device is now functional and ready to be further configured using the configuration interface.

1.2.1 Emergency mode

The device does not have an emergency mode set up. If you have ordered an ISDN connector, you can proceed as follows if there a 230 V network fails: Remove the connecting cable from the network termination unit (ISDN NTBA). You can then plug an ISDN terminal that is emergency power capable into the network termination unit, and resume making calls. When power is restored, remember to reverse this procedure.

Note

Note the settings on the emergency power capable telephone: If emergency power is being provided, a setting has to be made for the current ISDN connector (point-to-multipoint or point-to-point access).

No emergency mode is possible with an IP-based connection.
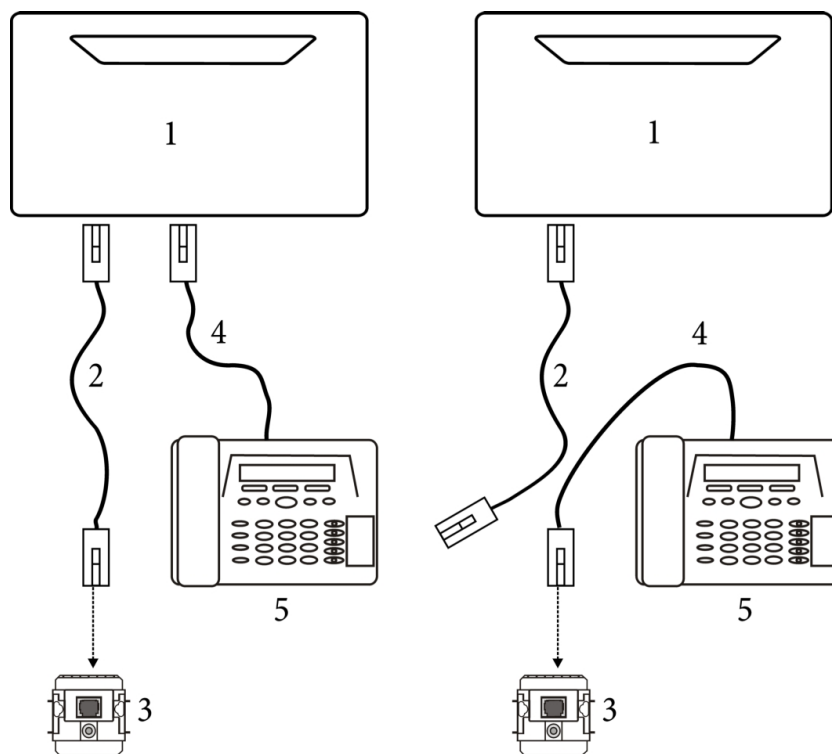
1	**hybird 120** / **hybird 130**
2	Connecting cable RJ45 plug
3	ISDN connector on the network termination unit
4	Connecting cable for the ISDN telephone with RJ45 plug
5	Emergency power capable ISDN telephone

1.2.2 Connectors

1	Socket for the power supply unit
2	External interface for analogue terminals FXO 1
3	Internal interface for analogue FXS 1 terminals (internal number 10, ex works state)
4	Internal interface for analogue FXS 2 terminals (internal number 11, ex works state)
5	Interface for ISDN BRI connections (ISDN S/U internal, ex works state, plug selectable) (internal numbers 20 and 21, ex works state)
6	Interface for ISDN BRI connections (ISDN S/U external, ex works state, plug selectable)
7	USB connection type B
8	10/100/1000 Base-T Ethernet interface (LAN 1)
9	10/100/1000 Base-T Ethernet interface (LAN 2)
10	10/100/1000 Base-T Ethernet interface (LAN 3)
11	10/100/1000 Base-T Ethernet interface (LAN 4)
12	ADSL2+ interface

1.2.3 Connections (on the side)
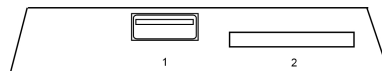
1	USB type A socket (not currently functional)
2	SD card slot

1.2.4 LEDs

The LEDs provide information on the device's activities and statuses.

The LEDs on your **hybird 120** / **hybird 130** are arranged as follows:
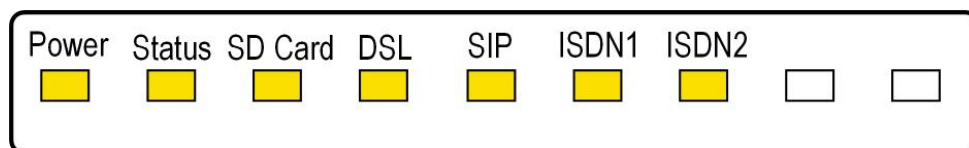
LEDs **hybird 120**
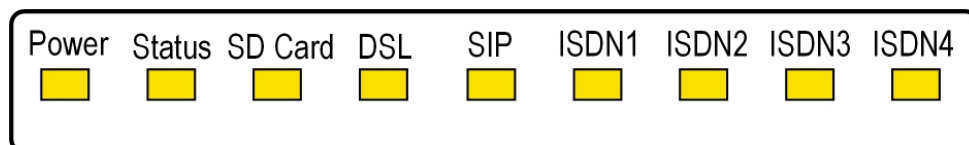
LEDs **hybird 130**

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

LED status display

LED	Colour	Status	Information
Power	Yellow	on	Power supply is connected
		off	No power supply
Status	Yellow	on	after switching on: Device is starting, during operation: Error
		slow flashing	Device is active
SD card	Yellow	on	SD card inserted, no read/write access
		off	no SD card inserted
		flickering	Read/write access
DSL	Yellow	off	no synchronisation
		slow flashing	Synchronisation running
		on	Connection established
		flickering	Data transfer
SIP	Yellow	on	registered successfully with SIP provider
		off	no SIP registration
ISDN1 to ISDN 2	Yellow	on	Layer 1 is active
		off	Idle or not operational
		slow flashing	one B channel is active
		quick flash-ing	two B channels are active
ISDN1 to ISDN 4 (**hybird 130**)	Yellow	on	Layer 1 is active

LED	Colour	Status	Information
		off	Idle or not operational
		slow flashing	one B channel is active
		quick flash-ing	two B channels are active

The LEDs on the Ethernet sockets indicate the following status information:

Ethernet LEDs

LED	Colour	Status	Information
ETH 1 to 4	green	on	The device is connected to the Ethernet at 1 Gbps
	green	flashing	Data traffic with 1 Gbps.
	yellow	on	The device is connected to the Ethernet at 100 mbps.
	yellow	flashing	Data traffic with 100 mbps.
	green and yellow	on	The device is connected to the Ethernet at 10 mbps.
	green and yellow	flashing	Data traffic with 10 mbps.

1.2.5 Scope of supply

Your device is supplied with the following parts:

Product name	Cable sets/other	Software	Documentation
hybird 120 / **hybird 130**	Ethernet cable (yellow) ISDN BRI cable (black) Power supply SD card with voicemail data Screws and rawl plugs for wall mounting	Quick Install Guide, User's Guide and otjer document-ation on DVD (if provided) or as a download from our website	Installation Instructions Safety notices

1.2.6   General Product Features

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

General Product Features hybird 120 / hybird 130

Property	
Dimensions and weights:	
Equipment dimensions without cable (B x H x D):	300 x 215 x 40 mm
Weight	approx. 900 g
Transport weight (incl. documentation, cables, packaging)	approx. 1,400 g
Memory	64 MB RAM, 16MB Flash ROM
Flash card slot	Supports version 3 SD standard SD cards. See also *SD card* on page 28.
LEDs	Seven or nine status LEDs, two LEDs per Ethernet interface
Power consumption of the device	30 W 12 VDC
Voltage supply	12 V DC 2.4 A
Environmental requirements:	
Storage temperature	-20 °C to +70 °C
Operating temperature	+5 °C to +40 °C
Relative atmospheric humidity	max. 85 %
Room classification	Operate only in dry rooms
Available interfaces:	
ADSL interface	Internal ADSL2+ modem for Annex B and for Annex J, and for Annex A
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, autosensing, MDIX

Property	
ISDN-BRI	2 switchable ISDN interfaces, support S0 external and internal, Up0 internal; ISDN termination with 2x 100 Ohm, 2 watts voltage, connection via socket or terminal technology
FXS	4 FXS interfaces (**hybird 120**), connection via socket and/or terminal technology 6 FXS interfaces (**hybird 130**), connection via socket and/or terminal technology
FXO	1 FXO interface
UP0 interface (**hybird 130** only)	2x UP0 interfaces
Switch contact (**hybird 130** only)	Terminal block for connecting e. g.: door intercom adapters
USB console (Type B)	Baudrates: 1200 - 115200 Baud, standard: 9600 Baud
USB (Type A)	not currently supported
Available sockets:	
USB Console	Standard USB Type B socket
USB	Standard USB Type A socket
Ethernet interfaces	RJ45 socket
ISDN BRI interface	RJ45 socket
FXS interface	RJ12 socket
FXO interface	RJ12 socket
ADSL interface	RJ45 socket
DC socket for power supply	

1.3 Reset

Resetting is done using the Reset button on the device (see *Reset button* on page 26).

If the key is pressed (for approx. one second) then the device resets. Pressing the key is equivalent to an interruption of the power supply. Any saved data will be retained, but all connections will be broken.

If you press the reset key for approx. 30 to 40 seconds, the device performs a factory reset. This means the device is returned to its ex works state. The connection data is not deleted. The boot configuration is deleted and all passwords are reset. The reset has finished once the device finds itself in the operating status after 30 to 40 seconds.

Note

If a configuration (boot) is saved on an SD card which is plugged in, the behaviour is different. In this case, a longer button press causes the configuration on the device itself to be deleted and the device to be started with the configuration saved on the SD card. The device also starts with a configuration saved on the SD card if no configuration has been saved on the device itself.

1.4 Presettings

Certain settings have already been pre-configured so that it only takes you a few steps to start using your device for the first time.

Note

Consult the user's guide for your existing terminals to find out how the features can be used and with which settings.

You can change these presettings to meet your personal requirements and connection situation.

Telephony presettings

Analogue connections	Set up as telephone. Permanently set to *tone dialling (MFC)*.
Call waiting	Set up with analogue telephones (for FXS 2 but disabled where a fax or multifunctional unit is connected).
Waiting calls	If both B-channels of the ISDN connection are occupied, waiting calls are rejected.
Manually switching call variants	Allowed
Receive simplex operations	Allowed

Message	Allowed
Net Direct (keypad)	Allowed
DoorLine permission	Allowed
TAPI	Allowed
Save connection data	Set up
Outside line	Outside line via *0* is set up.
International prefix	Not set up
Country code	Not set up
National prefix	Not set up
<olink>Area code</olink>	Not set up
Currency for billing	Not set up
Authorisation for the terminals	Unrestricted authorisation
Dir. call	Not set up
Own telephone number	Transmitted to caller
External calls	Are signalled to all pre-configured internal numbers (*Team global*).
Outgoing phone calls	For all internal numbers via the preset external ISDN connection (*ISDN external*).
Manual bundle assignment	Set up for all internal numbers for the preset external ISDN connection (*ISDN external*).
Call pickup	Set up
Internal telephone numbers	For the **ISDN (BRI) internal** to the internal ISDN bus, the internal telephone number *30* is provided, for the analogue connections

	FXS1 and **FXS2** the internal telephone numbers *10* and *11* are provided, for system telephones the telephone numbers *20* and *21* are provided, and for DECT systems the internal telephone number *22* is provided.
Pre-configured teams	Internal number *40*: Team global (internal numbers assigned: *10*, *20*, *21*, *22*)
Misdial routing	To internal number *40* (Team global)
Team call forwarding	Allowed
Voicemail system	Set up for the internal numbers *10* and *20*. With no PIN query. (Only if there is an SD card).
Display in system phone book	Set up for all internal numbers
Busy lamp field	Set up for all internal numbers
Switching times (calendar)	Not set up
Keypad function	Not set up
PIN 1	Not set up
PIN 2	*000000*
Telephone number of the calling subscriber (CLIP)	Displayed
Telephone number transmission	Set up
ISDN point-to-point connection	Set up for the ISDN 2 connection
Standard MSN	*20 (#20)*
Time on the internal ISDN (BRI)	

> **Note**
>
> After a restart you should always check that the system time is correct!

If you have ordered a point-to-point ISDN access, the time is taken after the first outgoing connection from the ISDN.

If you are connected to the Internet via a configured Internet access, the time can be taken from a time server.

Device as internal time server	Set up
Automatic Route Selection	Set up for all internal numbers, but no numbers set up
Dialling control	Set up for all internal numbers, but no numbers set up
Priority numbers	No priority numbers have been configured. The usual numbers are: Emergency call *110* Emergency call *112* Ambulance *19222*
Music on hold 1	*MOH Internal 1* set up.
Time for call forwarding	Time after set to *15* seconds.
Preset public holidays	No public holidays have been configured. The usual public holidays are: 01.01. New year 06.01. Twelfth Day 01.05. Labour Day 15.08. Feast of the Assumption

	03.10. Day of German Unity
	31.10. Reformation Day
	01.11. All Saints' Day
	25.12. 1. Boxing Day
	26.12. 2. Boxing Day
IP address assignment to VoIP terminals and PCs in the LAN	Via DHCP servers with IP address range *192.168.0.10 - 192.168.0.30* Time server: *192.168.0.250* Provisioning server: *http://192.168.0.250/eg_prov*

Configuration interface

In the ex works state, you can access your device's configuration interface through one of the LAN connections at this address:

- **IP Address**: *192.168.0.250*
- **Netmask**: *255.255.255.0*

In the ex works state, you should use the following access data to configure your device using the configuration interface:

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

> **Note**
>
> After you log into the device for the first time, you will be prompted to enter a secure password. When you do this, please note the guidance that is displayed on secure passwords! When the configuration procedure is complete, select the **Save configuration** button! Otherwise the new, secure password will be lost when there is a restart.

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. The **guide** describes, in the "**Maintenance**" chapter, how you can check the software version for your device and how to up-

date it if necessary.

1.5 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* .

Chapter 2 Mounting

> ⚠ **Warning**
>
> To avoid electric shocks, please take care when connecting telecommunications net-
> works (TNV electric circuits). LAN ports also use RJ connectors.

> ⚠ **Caution**
>
> To ensure that the **hybird 120** / **hybird 130** can operate free of faults, it must be
> mounted upright on a wall. The device should not be exposed to direct sunlight or oth-
> er sources of heat. Please note, too, the gaps that you need to comply with (see *Wall
> mounting* on page 26).

> ☞ **Note**
>
> If you want to connect a terminal with a TCU plug, you can use a TCU-to-RJ12 ad-
> apter, remove the plug on the device's cable and connect the device to a terminal
> block or change the plug on the terminal's cable.

2.1 Connection variants
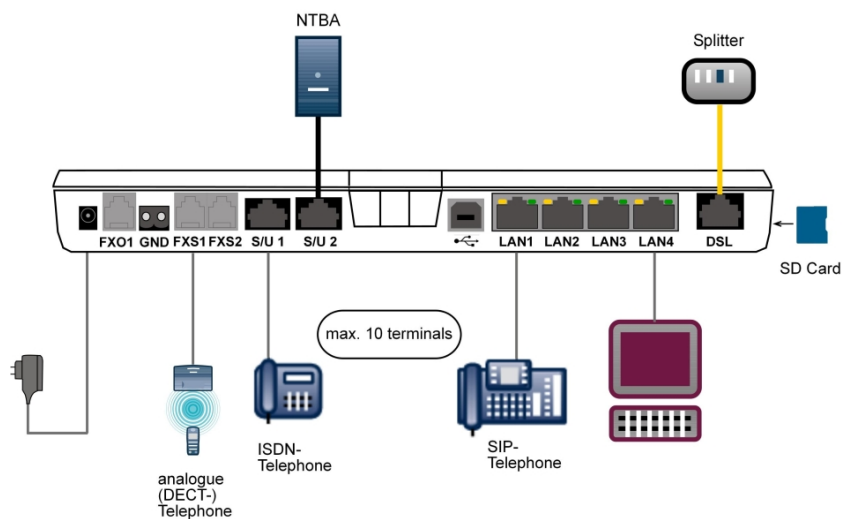
2.1.1 Connection to the ISDN network

The second ISDN connection (ISDN 2 or terminal block on the bottom right) is configured, in its ex works state, as an external S0 connector (S0 TE) (to configure the ISDN connectors, see *Configuring the ISDN connections* on page 25). You can switch terminators on and off with switches when configuring the ISDN connectors. In its ex works state, all the terminators are switched on.

2.1.1.1 Direct connection to the NTBA

Example 1: The device is connected directly to the ISDN NTBA.
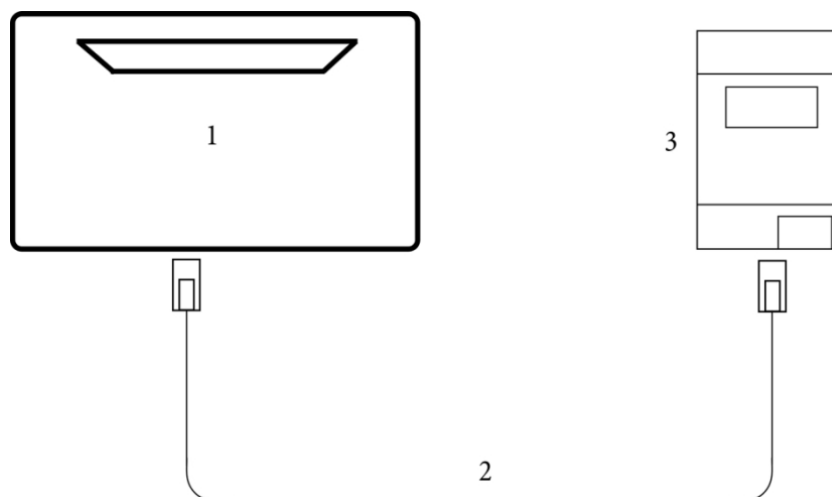
1	**hybird 120** / **hybird 130**
2	RJ45 connector cable for the ISDN connection
3	ISDN NTBA with 2x 100 Ohm terminators switched on

2.1.1.2 Connection to a socket

Example 2: The device and ISDN NTBA are more than about 2.5 metres away from one another.
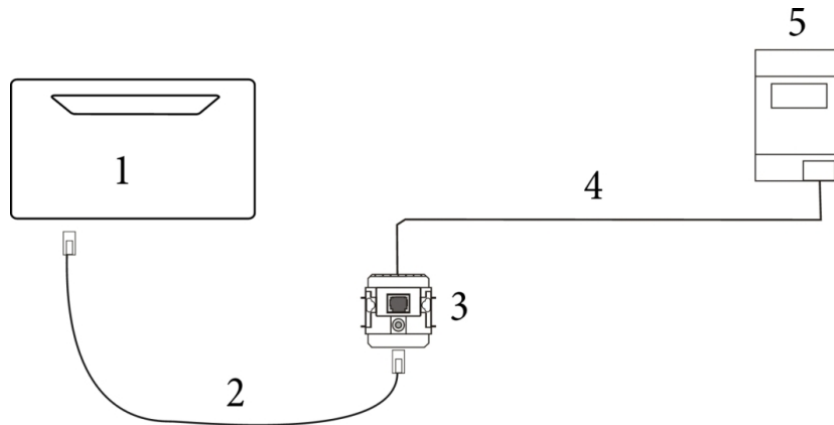
1	**hybird 120** / **hybird 130**
2	RJ45 connector cable for the ISDN connection
3	RJ45 connection socket with 2x 100 Ohm terminators
4	Fixed connection cable
5	ISDN NTBA with 2x 100 Ohm terminators switched on

2.1.1.3 Connection to an existing ISDN bus

Example 3: The device is running on an existing ISDN bus.
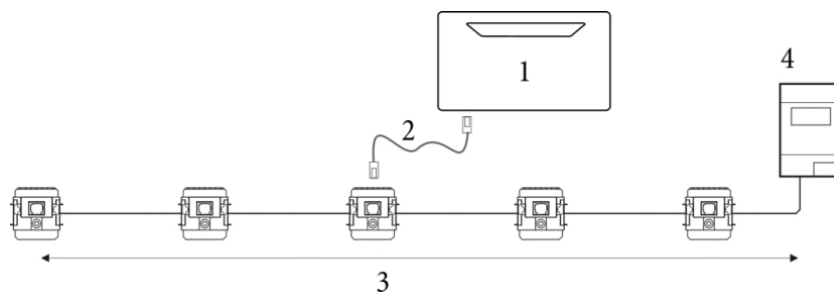
1	**hybird 120** / **hybird 130**
2	RJ45 connector cable for the ISDN connection
3	Existing ISDN bus is closed off on both sides
4	ISDN NTBA with 2x 100 Ohm terminators switched on

> ☞ **Note**
>
> The ISDN bus must be closed off at both ends with 2x 100 Ohm terminators. In this
> scenario, the terminators integrated into the **hybird 120** / **hybird 130** should be
> opened.

2.1.2 IP-based connection

With a pure IP-based connection, you initially connect the **hybird 120** / **hybird 130** as de-
scribed in the installation, to the network operator's transfer point. In such cases a splitter is
rarely used, and the connection is made directly to the first socket. Alternatively, you can
connect your device to an existing modem (e. g. a VDSL modem).

2.1.2.1 ADSL connection

Example 1: The **hybird 120** / **hybird 130** runs directly on the ADSL connection: To do this,
you merely need to connect your device to the wall socket of the ADSL connection and fol-
low the setup steps, for which you can refer to the installation poster or chapter *Installation*
on page 1.
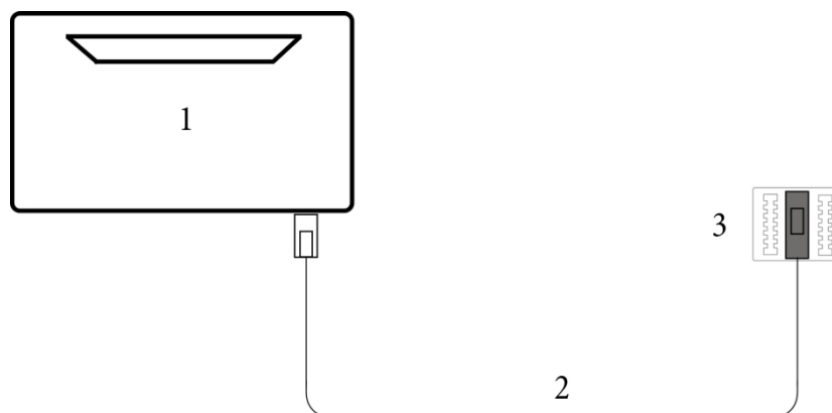
1	**hybird 120** / **hybird 130**
2	Connection cable for the connection to the ADSL socket
3	ADSL socket

2.1.2.2 VDSL connection

Example 2: The **hybird 120** / **hybird 130** runs on an existing VDSL modem: Installation is easy with this connection variant, too. Use the yellow network cable provided to connect your device to the existing VDSL modem and follow the steps described on the installation poster or in chapter *Installation* on page 1.
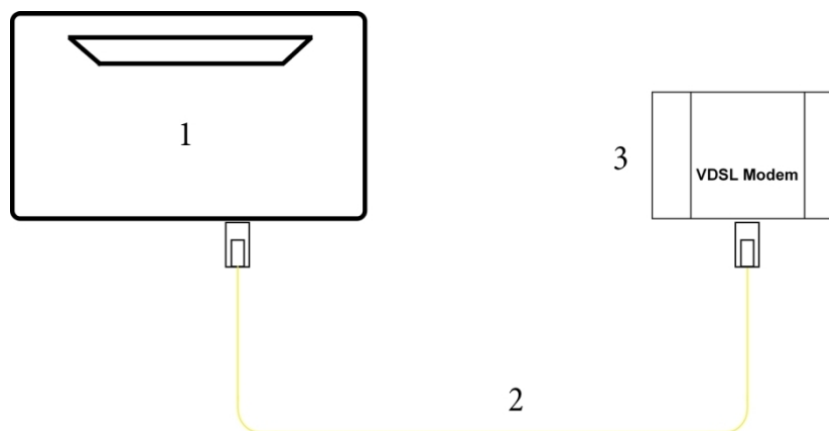
1	**hybird 120** / **hybird 130**
2	Yellow RJ45 connection cable for connecting to the VDSL modem
3	VDSL modem

2.1.3 Connection to the analogue telephone network

To connect to the analogue telephone network, you connect your network operator's socket to the FXO interface on your **hybird 120** or **hybird 130** using a suitable cable.

Note

Note that you require a cable that connects the TCU socket to the RJ12 socket on your device. This type of cable is not supplied.
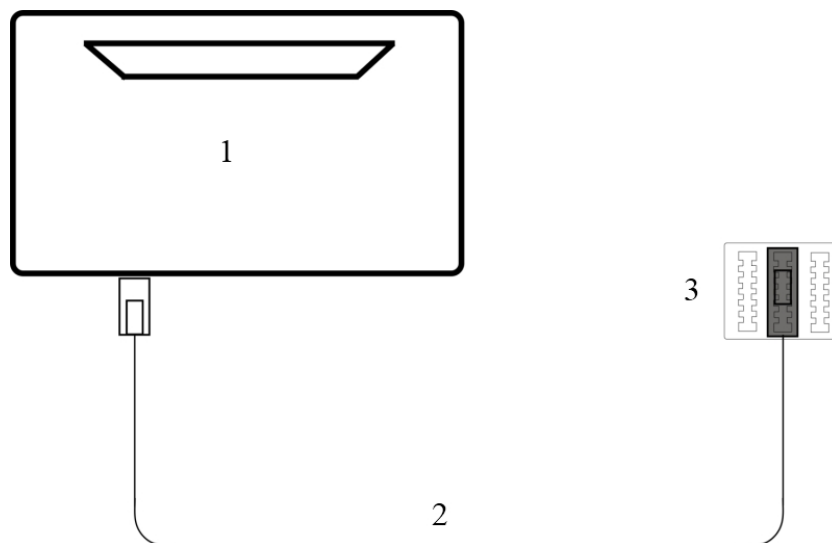
1	**hybird 120** / **hybird 130**
2	Connecting cable for connecting to the TCU socket (RJ12 to TCU)
3	TCU socket

2.1.4 Connecting terminals

2.1.4.1 Connection for analogue terminals

Only analogue terminals with the tone dialing method (MFC) should be connected to the analogue connectors. Analogue telephones, fax machines, answering machines, multifunctional units, modems and door intercoms can be connected to the analogue connectors.

Note

Two RJ12 sockets (**FXS1** and **FXS2**) are included for connecting two analogue terminals directly. These connectors equate to the fixed connectors on the connection terminals in the top left of the terminal block.

Note

The fixed connectors and the direct connectors are connected in parallel. So you can operate terminals from either the fixed or direct connector.

The R key must perform the flash function (70 ms to 310 ms). With these devices, the functions described in the user guide and configuration can be used with no restrictions. The internal analogue connectors support the clip and clip-off-hook function. Analogue telephones with the pulse dialling method (PDM) cannot dial. With analogue telephones, your devices supports the flash. So you should never hang the receiver up for even just a short while, or touch the cradle switch even briefly with your hand, or the device will detect a flash instead of you hanging up.

Cable assignment to the connection terminals on TDO sockets.

The line length from the device to the terminal is 1000 metres maximum. The line lengths apply to cables J-Y (St) Y2x2x0.6.
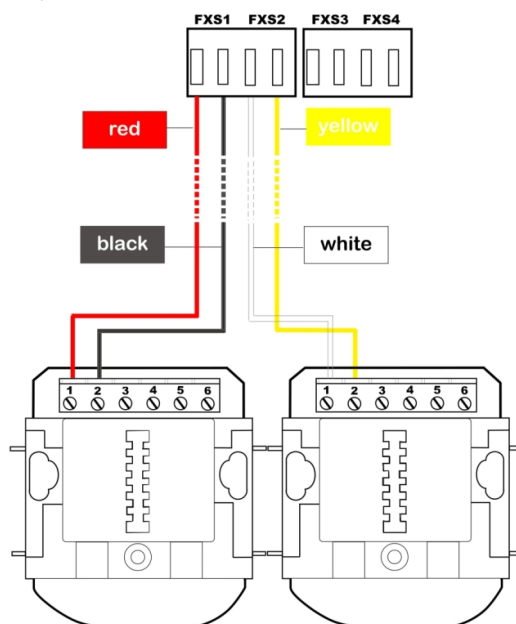
Connecting to a TCU socket
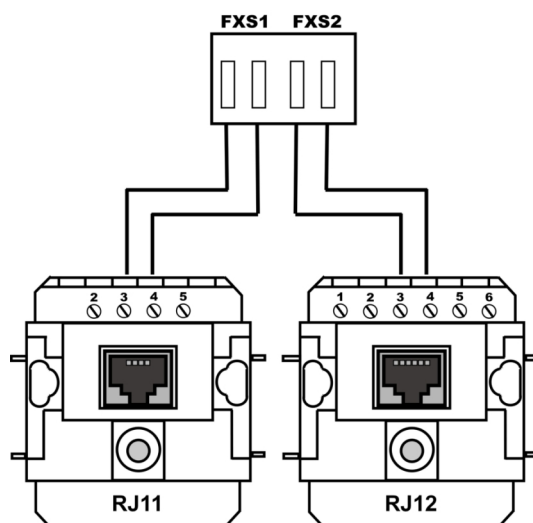
Connecting to an RJ11 or RJ12 socket

2.1.4.2 Internal ISDN connection

The internal ISDN connection on the **hybird 120** / **hybird 130** gives each internal ISDN connection a 2.5 watt power supply for connecting a maximum of two unpowered ISDN terminals. In its ex works state, the internal ISDN connection is set up as a "short passive bus" ("S0 bus"). It is the simple bus cabling in an ISDN system with a length of up to 120 m.

Installing the internal ISDN connection

You can plug a terminal straight into the **ISDN 1** (internal ISDN connection) socket. You can connect other ISDN terminals to a permanently installed ISDN bus. You can connect an ISDN system telephone, an ISDN telephone or an ISDN card to this connector.

Connecting other ISDN terminals is done via an ISDN distributor or via a permanent cable to an ISDN bus. The line length to the ISDN sockets for the terminals can be up to 120 m, with a cable diameter of 0.6 mm. The length of the ISDN connection cables from the ISDN sockets to the ISDN terminals may not exceed 10 metres.

The line lengths apply to cables J-Y (St) Y2x2x0.6 (0.4). Greater ranges can also be achieved with other types of cable. You should take care that the cable's sheath is not removed for any longer than necessary and that the wires to the socket remain twisted, or stranded.

> ⚠ **Important**
>
> The 100 Ohm terminators should be connected to the last ISDN socket installed on the ISDN bus.

2.1.5 Permanent connections

> **Note**
>
> When removing the lid, a certain amount of force may initially be required. Hold the lid, pressing lightly on the upper side, while you release the bracket on the lower side with your thumb and forefinger.

There are 4-pin connection terminals for the permanent connections. Take care that the wires to the connection terminals remain stranded. 2 wires can be plugged into each connector. The diameter of the cable can be 0.4 … 0.8 mm. If you press with a screwdriver on the area indicated with the arrow on the connection terminal (see picture), the wires can be removed by pulling gently.
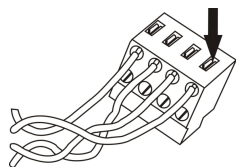
Connection terminal

Plastic cable fixes are included for fixing the connecting cable. However, you should ensure the installation cable cannot be pulled out by placing cable clips [D] in front of the device. The wires [B] in the connecting cable [A] should protrude about 100 mm from the cable sheath. The length of cable sheath [C] from the cable clips should be around 80 mm. The insulation on the ends of the wires should be stripped back by about 6-7 mm.

Connection terminal	Name	Telephone numbers
Terminal 1	**FXS1** and **FXS2**	*10* and *11*
Terminal 2	**FXS3** and **FXS4**	*12* and *13*
Terminal 3 (**hybird 130** only)	**FXS 5** and **FXS 6**	
Terminal 4	**Switch contact**	
Terminal 5	**ISDN 1 (configurable)**	*20, 21*
Terminal 6	**ISDN 2 (configurable)**	*External*
Terminal 7 (**hybird 130** only)	**Up0**	
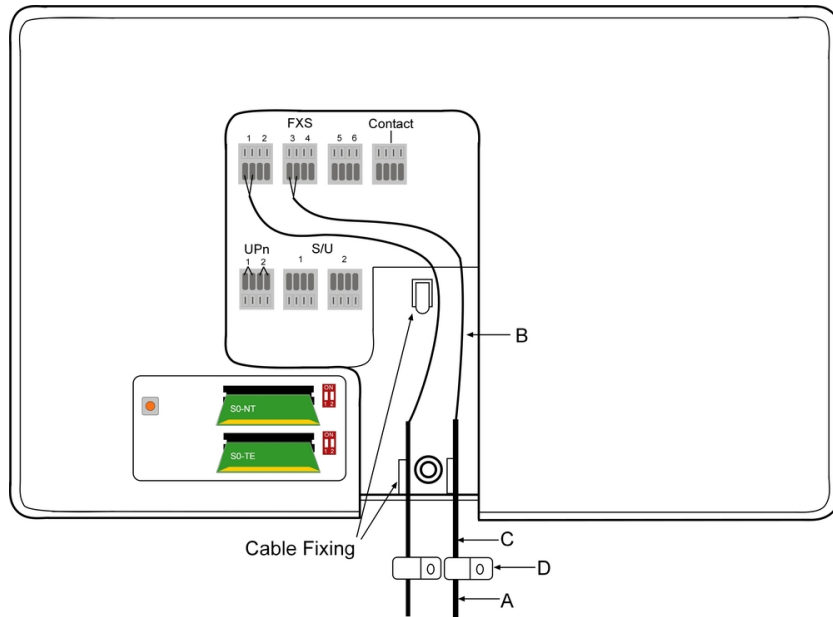
Cable fix
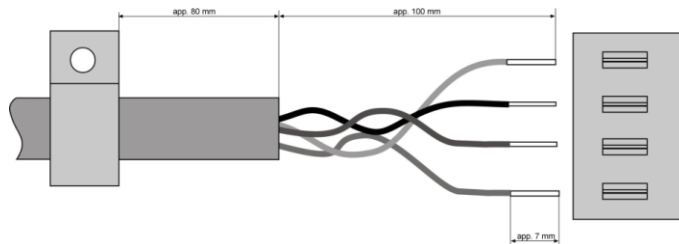
Strip the insulation

2.2 Configuring the ISDN connections

You can set the operating mode by plugging in the mini module belonging to each connection (ISDN 1 above, ISDN 2 below) in such a way that, when viewed from above, you can see the label you want (for guidance: the connections on the device are located on the bottom).

Also, adjacent to the slots for switching over the operating mode you will find two switch blocks for switching the terminators on and off. In its ex works state, the terminators for both ISDN connections are active.

> ⚠ **Caution**
>
> Before configuring the ISDN connections, disconnect the device from the power supply. Pulling out and/or plugging in the modules while operational will cause errors.

2.3 Reset button

To the left of the slots for configuring the ISDN connections there is the reset button, which you can use to restart the device or restore the ex works state (see *Configuring the ISDN connections* on page 25).

2.4 Wall mounting

The various assembly processes are described in this section. Please comply with these processes.

(1) Find an installation site which is a maximum of 1.5 metres away from a 230 V mains socket and 2.5 metres from the network operator's transfer point.

(2) To prevent devices interfering with each other, do not install the device close to electronic devices such as hi-fi systems, office equipment or microwave ovens. Neither should you install it near heat sources such as radiators, or in damp rooms.

(3) Comply with the gaps as indicated at the bottom in the picture.
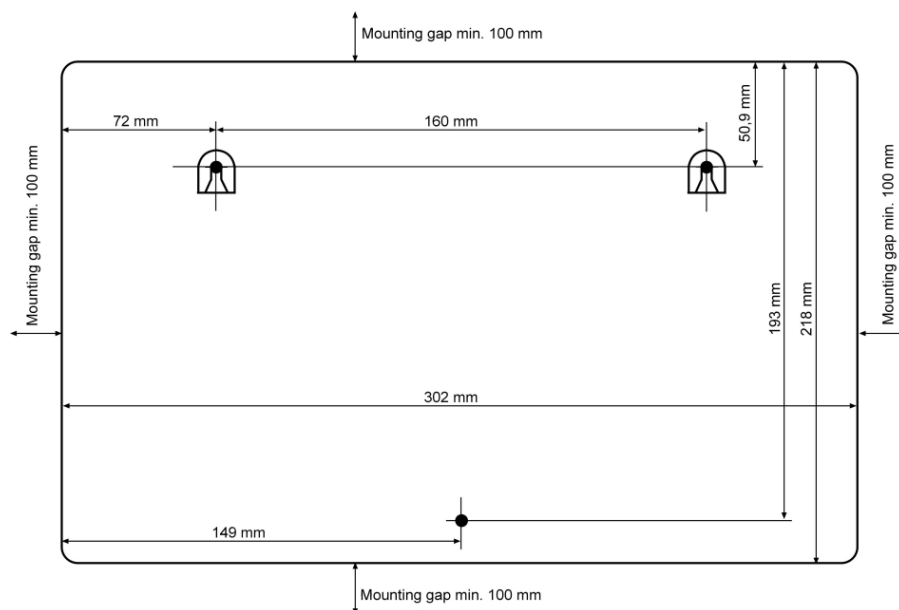
(4)   Mark the drilling holes in the wall.

(5)   Check that all the points where the **hybird 120** / **hybird 130** is attached to the wall can bear its weight. Ensure that there are no utility lines, cables etc. located in the area where the holes are marked.

(6)   Drill the holes at the points marked (if inserting into rawlplugs, use a 5 mm masonry drill). Insert the rawlplug.

(7)   Screw the top two screws in such a way that there is still a gap of about 5 mm between the screw head and the wall.

(8)   Open the device by carefully removing the faceplate.

(9)   Hang the **hybird 120** / **hybird 130** with the rear brackets from above behind the screw heads.

(10) Screw the lower screws through the device so that it is fixed firmly to the wall.

(11) If necessary, install the sockets for the terminals. Connect the socket installation to that of the device. The sockets are used for a permanent installation, for example in a hallway. When they are installed, the connecting cables are connected to the connectors on the device,

(12) Plug the connectors on the device into the sockets.

(13) Connect the **hybird 120** / **hybird 130** to the external connections (ISDN and ADSL). To do this, you can follow the instructions given on the installation poster provided.

(14) Plug the power supply unit into the 230 V~ socket.

(15) Plug the barrel connector on the power supply unit into the corresponding socket on your device.

(16) Now you are ready to use the device.

2.5 Service access

When the product has been mounted and connected, and you are not going to use a local PC to configure it, the **hybird 120** / **hybird 130** can also be configured via ISDN by bintec elmeg Customer Service department. To do this, contact Customer Service department and discuss the configuration you want.

For the basic configuration without using your own PC, via ISDN, proceed as follows:

(1) Enter the key sequence *99 into one of the connected telephones (analogue or ISDN terminal). The **hybird 120** / **hybird 130** is now authorised for the service connection for 30 minutes.

(2) bintec elmeg Customer Service will now connect to your **hybird 120** / **hybird 130**. If necessary, you can terminate the authorisation with #99.

2.6 SD card

Basically, **hybird 120** / **hybird 130** supports version 3 SD standard SD cards. bintec elmeg GmbH has approved the following cards:

• SanDisk SDSDAA-001G - 1 GB
• SanDisk SDSDAA-002G - 2 GB

2.7 Pin Assignments

2.7.1 USB console interface

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

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

The pin assignment is as follows:

Pin assignment in USB Type B socket

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

You may need a serial to USB driver for the CP210x component. You can download it from *www.bintec-elmeg.com* .

2.7.2 Ethernet interfaces

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

The 4-port switch is used to connect individual PCs or other switches. The connection is made via RJ45 sockets.

1 8
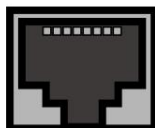
The pin assignment for the Ethernet 10/100/1000 Base-T interface (RJ45 connector) is as follows:

RJ45 socket for Ethernet connection

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

2.7.3 ISDN BRI interface

The connection is made via an RJ45 socket:

1 8
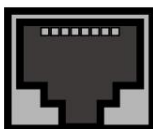
The pin assignment for the ISDN BRI interface (RJ45 socket) is as follows:

RJ45 socket for ISDN connection

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

2.7.4 FXS/FXO interfaces

The terminals are connected to the FXS/FXO interfaces (RJ12 socket) with an RJ11 plug.

1 6
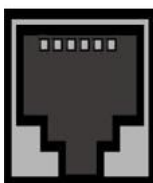
The pin assignment for the FXS/FXO interface (RJ12 socket) is as follows:

RJ12 socket for FXS/FXO connection

Pin	Position
1	Not used
2	Not used
3	FXS
4	FXS
5	Not used

Pin	Position
6	Not used

2.7.5 ADSL interface

The **hybird 120** / **hybird 130** has an ADSL interface.

The ADSL interface is connected via an RJ45 plug.

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

1 8
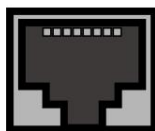
The pin assignment for the ADSL interface (RJ45 socket) is as follows:

RJ45 socket for ADSL connection

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

2.7.6 FXS terminal blocks

1 2 3 4
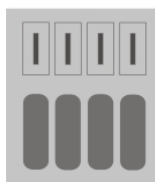
Pin assignment in FXS blocks

Pin	Position
1	a1
2	b1
3	a2
4	b2

The switching in the other blocks is analogue (a/b3 bis a/b6).

2.7.7 Terminal block switch contact

The switch contact block is assigned as follows:
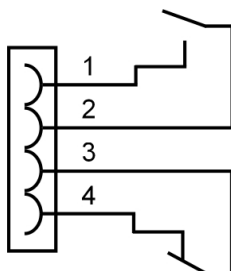
2.7.8 ISDN terminal blocks

Pin assignment in ISDN blocks in TE mode

Pin	Position
1	RX+

Pin	Position
2	RX-
3	TX+
4	TX-

Pin assignment in ISDN blocks in NT mode

Pin	Position
1	TX+
2	TX-
3	RX+
4	RX-

Pin assignment of ISDN blocks in UP0 mode

Pin	Position
1	UP0 a
2	UP0 b

2.7.9 UP0 terminal block

Pin assignment in the UP0 block

Pin	Position
1	UPn1 La
2	UPn1 Lb
3	UPn2 La
4	UPn2 Lb

Chapter 3 Basic configuration

You can also use the configuration interface to configure the device yourself.

The way to obtain the basic configuration is explained below step-by-step. A detailed online help system gives you extra support.

3.1 Preparations

Your device is factory configured as a DHCP server so that it can provide PCs on your LAN that have no IP configuration with all the information required for a connection. How you set up the PC that you want to do the basic configuration on so that it automatically gets an IP configuration is described in *Configuring a PC* on page 36.

> **Note**
>
> If you already run a DHCP server on your LAN, it is recommended that you configure the device on a separate PC that is not connected to your LAN. Connect this PC alone to your **hybird 120** / **hybird 130** so that you have your own network to do the configuration.

3.1.1 System Software

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 update it using the configuration interface in the **Maintenance**->**Software &Configuration** menu. For a description of the procedure, see *hybird 120 / hybird 130 software updates* on page 41.

3.1.2 System requirements

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

• Microsoft Windows operating system Windows 2000 or higher; Windows XP SP3 requires the following hotfix: *http://support.microsoft.com/kb/953761.*

• Internet Explorer 7 or 9 (possibly adjust the security settings), Mozilla Firefox version 4 or higher

• Installed network card (Ethernet)

• Installed TCP/IP protocol

• High colour display (more than 256 colours) to show the graphics correctly

3.1.3 Gathering data

You will quickly collect the main data for doing the configuration with the configuration interface.

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

- Network settings (only if you intend to integrate your device into an existing network infrastructure)
- SIP provider
- ISDN telephone connection
- Internet access

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.

Basic configuration

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

Network settings

Access data	Example value	Your values
IP address of your gateway	*192.168.0.250*	
Netmask of your gateway	*255.255.255.0*	

SIP provider

Access data	Example value	Your values
Description	Enter the name of your SIP provider, e.g. *Sipgate*.	
Authentication ID	Enter your ID, e. g. for Sipgate: *3223174e1*	
Password	Enter the password you received from the SIP provider.	
Registrar	Enter the relevant regis-	

Access data	Example value	Your values
	trar. For Sipgate: *sipg-ate.de*	
Call number	e. g. *123456*	

ISDN point-to-multipoint connection

Access data	Example value	Your values
Multipoint connection number	*123456*	
Direct dial-in numbers	*10, 11, 12, 13 etc.*	

Data for internet access over ADSL

Access data	Example value	Your values
Provider name	*GoInternet*	
Protocol	*PPP over Ethernet (PPPoE)*	
Encapsulation	*LCC Bridged no FCS*	
VPI (Virtual Path Identifier)	*1*	
VCI (Virtual Circuit Identifier)	*32*	
Connection ID (12-digit)	*000123456789*	
T-Online number (usually 12 digits)	*06112345678*	
Joint user account	*0001*	
Password	*TopSecret*	

3.1.4 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

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.

Configuring a Windows PC as a DHCP client

Assign an IP address to your PC as follows:

(1)   Initially, proceed as described to display the network properties.

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

(3)   Choose **Determine IP address automatically**.

(4)   Also choose **Determine DNS server address automatically**.

(5)   Close all the windows by selecting **OK**.

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

Note

You can now launch the configuration interface for doing the configuration by entering the preconfigured 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-set login data (**User**: *admin*, **Password**: *admin*).

3.2 Configuring the system

3.2.1 Modify system password

All bintec elmeg devices are delivered with the same username and password. So, after you log into the device for the first time, you will be prompted to enter a secure password. Please comply with the following rules on secure passwords:

- The password must be at least eight characters long.

- Use characters out of at least three of the following four character groups:

  - lower case letters [a-z]

  - upper case letters [A-Z]

  - numbers [0-9]

  - special characters

Note

When the configuration procedure is complete, select the **Save configuration** button!
Otherwise the new, secure password will be lost when there is a restart.

3.2.2 Network setting (LAN)

If you intend to integrate your device into an existing network infrastructure, select the **Assistants**->**First steps**->**Basic Settings** menu for the network settings. For the LAN IP configuration, the **Address Mode** is set to **Static** by default, since your system is delivered ex works with a fixed IP. Enter the necessary **IP Address** for your device in your LAN and the associated **Netmask**. Leave all the other settings and click **OK**. Save the configuration by clicking on the **Save Configuration** button above the menu navigation.

3.2.3 Enter SIP provider

As an option, you may enter SIP providers for external telephone connections. Please note the description in the online help for the menu **VoIP**->**Settings**->**SIP Provider**->**New**.

3.2.4 ISDN point-to-multipoint connection

In its ex works state, the **hybird 120** / **hybird 130** is ready to operate on a point-to-multipoint ISDN connection. When the **hybird 120** / **hybird 130** has been connected to the ISDN point-to-multipoint connection, the status display must change to a green arrow.

(1)   Go to the **Physical Interfaces**->**ISDN Ports**->**ISDN External** menu.

Go to the following menu to configure the individual number (MSN):

(1)   Go to **Numbering**->**Trunk Settings**->**Trunk Numbers**->**New**.

(2)   For **Trunk**, select the connection for which you want to configure the numbers, here

ISDN External.

(3)   The *Single Number (MSN)* option has been pre-configured for **Type of Number**.

(4)   In the **Single Number (MSN)** field, one of the numbers issued by the provider is entered, e.g. *123456*.

(5)   Confirm with **OK**.

You enter point-to-point access numbers in a later step, in the **User Settings**. If necessary, use the values preset for the users.

Your device is now set up for making calls via your point-to-multipoint ISDN connection.

3.2.5   Point-to-point ISDN access

If you have ordered a point-to-point ISDN access, you need to make a few more entries.

Go to the following menu to configure the external ISDN port:

(1)   Go to **Physical Interfaces**->**ISDN Ports**->**ISDN External**->.

(2)   Enter a user-defined **Description** for the ISDN interface, e. g. *ISDN External*.

(3)   For **Access Configuration**, select the setting *ISDN P-P*.

(4)   Confirm the inputs with **OK**.

Go to the following menu to configure the external ISDN connection:

(1)   Go to **Numbering**->**Trunk Settings**->**Trunks**.

(2)   Delete the predefined entry *ISDN External* by clicking the icon.

Use **New** to add a new entry to the configuration of your ISDN access.

(1)   Go to **Numbering**->**Trunk Settings**->**Trunks**->**New** at the entry with **Description** *ISDN External*.

(1)   For **Access Type**, select *ISDN P-P*.

(2)   At **External Port**, use the **Add** option to insert the external port which has already been configured, e.g. *ISDN External*.

(3)   Click **OK** to confirm your entries.

Go to the following menu to configure the point-to-point access numbers:

(1)   Go to **Numbering**->**Trunk Settings**->**Trunk Numbers**->**New**.

(2)   For **Trunk**, select the connection for which you want to configure the numbers, here *ISDN External*.

(3)   For **Type of Number** leave the selection *P-P Base Number*.

(4)   For **P-P Base Number**, enter your point-to-point access number (without the direct

dial-in number), e. g. *123456*.

(5)   Confirm with **OK**.

You enter point-to-point access numbers in a later step, in the **User Settings**. If necessary, use the values preset for the users.

Your device is now set up for making calls via your point-to-point ISDN access.

3.3 Setting up an internet connection

You can establish an Internet connection with your device.

3.3.1 Internet connection over internal ADSL modem

To make it easier to configure an ADSL internet connection, the configuration interface has a wizard to guide you through the connection set-up process simply and quickly.

(1)   In the user interface, go to 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.

3.3.2 Other internet connections

In addition to an ADSL connection over the internal ADSL modem, you can connect your device to the internet with other types of connection or via an external modem. The **Internet Access** wizard in the configuration interface provides support for this type of configuration.

3.3.3 Testing the configuration

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

Carry out the following steps to test your device:

(1)   Test the connection from any device in the local network to your device. In the Windows Start menu, click **Run** and enter ping followed by a space and then the IP address of your device (e.g. *192.168.0.250*). A window appears with the response "Reply from...".

(2)   Test the internet access by entering *http://www.bintec-elmeg.com* in the internet browser.

> **Note**
>
> Incorrectly configured terminals may lead to unwanted connections and higher charges! Monitor your device and make sure it only sets up connections at the times you want it to. Watch the light indicators on your device (indicators for ISDN, DSL and the Ethernet interfaces).

3.4 User access

The system administrator can set up individual configuration access for each user. This will enable the users to view their main personal settings and customise them individually.

> **Note**
>
> The administrator can access the settings and data of all users. It is only the personal telephone book (**User Phonebook**) which the user can set up for themselves which can only be managed and viewed with the personal user login data.

To log into the configuration interface with the access data you have been assigned, enter your **user name** and your **password** in the login window.

The administrator configures the user accesses in the **Numbering**->**User Settings**->**Users** menu.

Users can also find help with the available configuration options in the online help system.

3.5 hybird 120 / hybird 130 software updates

The range of functions in the **hybird 120** / **hybird 130** is continuously being extended. These extensions are made available to you by bintec elmeg GmbH. 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**.

Software and Configuration Options

Action	Update system software ▼
Source Location	Current Software from Update Server ▼

START

The device will now connect to the bintec elmeg GmbH download server and check wheth-
er 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 Operation via a telephone

The operation and configuration of the system via a connected telephone is described in two separate documents:

- You can find a deatiles description of all availabe procedures in "Operation via the telephone". The document is available as download from *http://bintec-elmeg.com*.
- A flyer detailing the most essential procedures is likewise available as a download.

Chapter 5   Access and configuration

This chapter describes all the access and configuration options.

5.1 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 (for service technicians and debug purposes only)

5.1.1 Access via LAN

Access via one of the Ethernet interfaces in your device allows the configuration interface to be opened in a web browser.

5.1.1.1 HTTP/HTTPS

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

• *http://192.168.0.250*

  or

  https://192.168.0.250

5.1.2 Access via the Serial Interface

The **hybird 120** / **hybird 130** features a serial interface which allows a direct connection with a PC. 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.

> ⚠ **Caution**
>
> Access via the serial interface is only recommended for service technicians for debug purposes and if no LAN access is possible via the pre-configured IP address (192.168.0.250/255.255.255.0). The possible operations that can be run are displayed if you enter `?` in the command line and confirm with the **Enter key**.

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) Start the terminal program, e. g. 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`

5.2 Configuration

The configuration is done using the HTML configuration interface.

5.2.1 Configuration interface

The configuration interface 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.

You can use the configuration interface to carry out any configuration task easily and conveniently. It is integrated in your device and is available in English.

The setting changes you make are applied with the **OK** or **Apply** button in the relevant menu, without the device needing to be rebooted.

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 configuration interface to monitor the most important function parameters of your device.

System Information	
Uptime	0 Day(s) 22 Hour(s) 50 Minute(s)
System Date	Thursday, 2016 Dec 15, 09:34:58
Serial Number	BE2CCA015030025
BOSS Version	V.10.1.21.100 IPv6, IPSec, PBX from 2016/12/09 00:00:00
Last configuration stored	No boot config stored
Night Mode Status	Off

Resource Information	
CPU Usage	0%
Memory Usage	46.8/127.9 MByte (36%)
Internal Storage	0.046/3.963 GByte (1%) 1%
Active Sessions (SIF, RTP, etc...)	5
Active IPSec Tunnels	0 / 0
DSP Channels	SoftCoder 0 / 4
	LANTIQ 0 / 5

Modules	
DSP Module	
SoftCoder (0/4)	LANTIQ (0/5)

VoIP Trunk Lines				
No.	Description	Registrar	Access Type	Status
1	123456	tel.t-online.de	Single Number(s)	⏲
2	Fremd	fremd.de	Single Number(s)	⏲

5.2.1.1 Open the configuration interface

(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.

(3) Open a web browser.

(4) Enter *http://192.168.0.250* 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 configuration interface.

5.2.1.2 Operating elements

Windows in the configuration interface

The configuration interface window is divided into three areas:

• The header

• The navigation bar

• The main configuration window

Navigation   **Header**

Main configuration window

Header

Configuration interface header bar

Menu	Function
☰	Opens the navigation bar.
Logout	**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.
⑦	**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.

Menu	Function
LANGUAGE English Deutsch	**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 Standard ▼	**View**: Select the desired view from the dropdown menu. Standard and SNMP browsers can be selected.
SAVE CONFIGURATION	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

Assistants	⌄
System Management	⌄
Physical Interfaces	⌄
VoIP	⌄
Numbering	⌄
Terminals	⌄
Call Routing	⌄
Applications	⌄
LAN	⌄
Wireless LAN Controller	⌄
Networking	⌄
Multicast	⌄
WAN	⌄
VPN	⌄
Firewall	⌄
Local Services	⌄
Maintenance	⌄
External Reporting	⌄
Monitoring	⌄
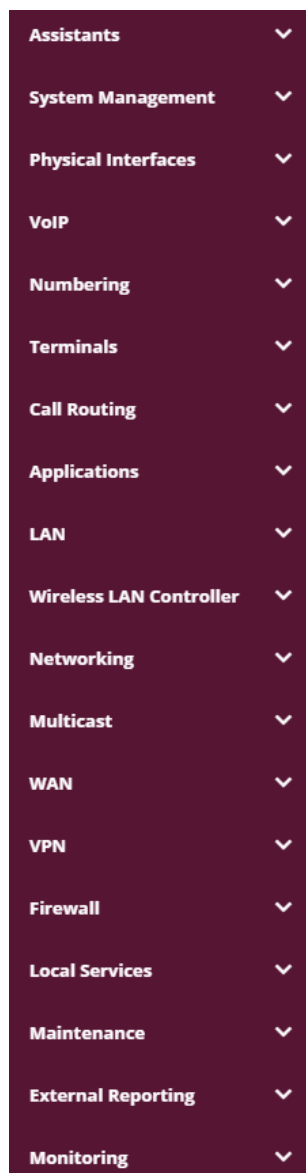
The **Save configuration** button is found in the navigation bar.

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

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

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

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

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

Status page

If you call the 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 tabs. These are called using the tabs at the top of the main window. If you click a tab, the window is opened with the basic parameters. You can extend this by clicking the **Advanced Settings** button, which then 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
APPLY	Updates the view.
CANCEL	If you do not want to save a newly configured list entry, cancel this and any settings made by pressing **Cancel**.
OK	Confirms the settings of a new entry and the parameter changes in a list.
GO	Immediately starts the configured action.
NEW	Calls the sub-menu to create a new entry.
ADD	Inserts an entry in an internal list.

GUI buttons for special functions

Button	Position
IMPORT	In the **System Management**->**Certificates**->**Certificate List** menu and the **System Management**->**Certificates**->**CRLs** menu, this button activates the sub-menus for configuration of

Button	Position
	the certificate or CRL imports.
REQUEST	In the **System Management**->**Certificates**->**Certificate List** menu, this button activates the sub-menu for the configuration of the certificate request.
(Release Call)	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.

Icon	Function
❌	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.
«	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 **View** x **per page**. Use the « and » buttons to scroll one page forward and one page back. You can filter according to certain keywords within the configuration parameters by selecting the filter rule you want under **Filter in** x **<Option> y** and entering the search word in the input field. 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.

Automatic Refresh Interval 60   Seconds **APPLY**

Configuration of the update interval

View 20   per page ⟪ ⟫ Filter in None   ▼ equal   ▼   **GO**

Filter list

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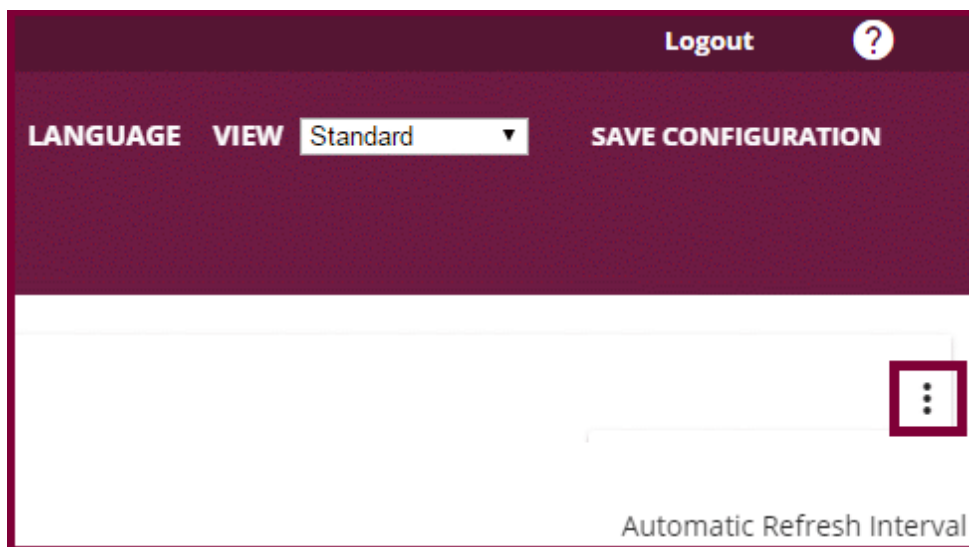
Click **Automatic Refresh Interval** .

Enter the time and click **APPLY** .
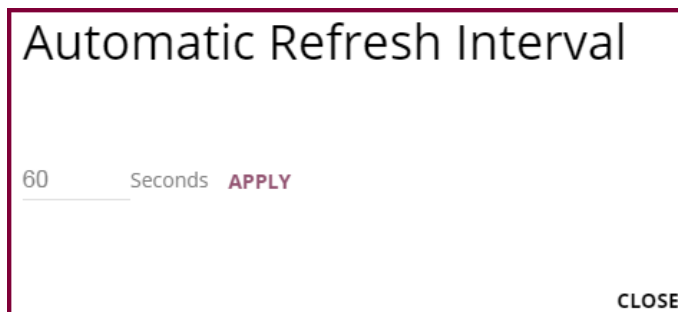
Structure of the configuration menu
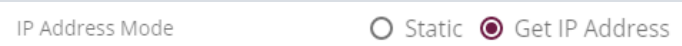
The menus contain the following basic structures:
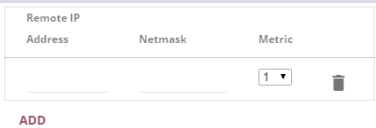
Menu structure

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.
Sub-menu **NEW**	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 + ADVANCED SETTINGS	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 Description Text field with hidden input •••••••• Enter the data.
Radiobuttons	e.g. IP Address Mode ○ Static ● Get IP Address Select the corresponding option.
Checkbox	e.g. activation by selecting checkbox 🔘 Enabled
Dropdown-Menüs	e.g. Full Autonegotiation ▼ Click the arrow to open the list. Select the required option using

Menu	Function
	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.

5.2.1.3 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. Use your product specification to check which software is on your device.

Chapter 6 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 7 System Management

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

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

7.1 Status

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

You see an overview of the following data:

• System status

• Your device's activities: Resource utilisation, active sessions and tunnels

• Status and basic configuration of the LAN, WAN, ISDN, and ADSL interfaces

• Information on plugged add-on modules (if any)

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

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

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 configura-	Indicates whether a backup configuration is available on the SD

Field	Value
tion on SD card	card or not.
Last configuration stored	Displays day, date and time of the last saved configuration (boot configuration in flash).
Night Mode Status	Indicates whether your device is in the normal mode (*Off*) or in night mode (*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.
Active Sessions (SIF, RTP, etc...)	Displays the total of all SIF, TDRC, and IP load balancing sessions.
DSP Channels	Shows the currently used DSP channels.

Fields in the Modules menu

Feld	Wert
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 Interface specifics for xDSL interfaces: • Last Change • DSL operation mode • DSL Speed • DSL Volume

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.

7.2 Global Settings

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

7.2.1 System

The **System Management**->**Global Settings**->**System** menu is used for entering your system's basic data.

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

Fields in the menu Basic Settings

Field	Value
System Name	Enter the system name of your device. This is also used as the PPP host name. A character string of up to 255 characters is possible. The device type is entered as the default value.
Location	Enter the location of your device.
Contact	Enter the relevant contact person. Here you can enter the e-mail address of the system administrator, for example. A character string of up to 255 characters is possible. Only for compact systems: The default value is *BINTECELMEG*.
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 prior-

Field	Value
	ity 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.
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*.
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.
Autosave Configuration	Here you can choose whether configuration changes are automatically saved. If you enable this option, settings are immediately saved so that they persist after a reboot of the device as soon as you confirm them on a configuration page (usually with the **OK** button).

Transfer to busy subscriber

You can define in the configuration whether a call can be transferred to a busy subscriber or, if it is off, that the caller will hear the engaged tone so that the call is terminated. Otherwise the caller is held and hears the ringing tone or the on-hold music. If the destination subscriber hangs up, the held subscriber hears the ringing tone. The destination subscriber is called and can take the held call.

Fields in the menu System Settings

Field	Value
Transfer Signalling	Specify how the call is to be transferred to an internal extension.

Field	Value
	Possible values:
	• *With the ringing tone* (the default value): Caller hears the ringing tone while being transferred.
	• *With music on hold (MoH)*: The caller hears the system's on-hold music while being transferred.
Transfer to busy extension	Set whether a caller may be transferred to a busy subscriber.
	The function is activated with *Enabled*.
	The function is disabled by default.
Rerouting to Number	Set the destination to which incoming calls should be diverted to, e. g. in the case of a misdial.
	Possible values:
	• *None - Busy Tone*: The caller hears the engaged tone by default and cannot be redirected to a destination.
	• *<Extension number>*: By default, the incoming call is routed to the number selected.
	The default value is the preset internal number *40 (Team global)*.
Interconnect external calls	When brokering with two external subscribers, select whether they are to be connected after you hang up.
	The function is activated with *Enabled*.
	The function is disabled by default.

Country settings

Your business is an international company with subsidiaries in several countries. Despite the differences in network implementation in the different countries, you want to use the same system in each subsidiary. By setting the respective country variants, the system can be adjusted to the particular features of the network in the required country.

As the system requirements vary from country to country, the functionality of certain features needs to be customised. The basic settings for different country variants are stored in the system.

Fields in the menu Country Settings

Field	Value
Country Profile	Select the country in which you want to use the system.
	Note: This does not change the language of the text in the system menu of system telephones.
	Possible values:
	• *Deutschland* (default value)
	• *Nederland*
	• *Great Britain*
	• *België*
	• *Italia*
	• *Danmark*
	• *España*
	• *Sverige*
	• *Norge*
	• *France*
	• *Portugal*
	• *Österreich*
	• *Schweiz*
	• *Česko*
	• *Slovenija*
	• *Polska*
	• *Magyarország*
	• *Ellada*
International Prefix / Country Code	Enter the country code.
	You need this entry if, e. g., you wish to automatically generate an international number under **SIP Provider**. You dial, as usual, the national prefix e. g. 05151 909999 and the system then automatically dials +495151 909999. If you fail to enter the country code, you may misdial, as the system will then dial +5151 909999. Without the entry **Generate international phone number** and **International Prefix / Country Code**, the full number plus the country code always has to be dialled in the

Field	Value
	case of SIP providers. Note: Not every SIP provider supports this setting.
National Prefix / City Code	Enter the national prefix and the area code for the location where your system is installed. With a point-to-point ISDN access, this area code is essential, because otherwise e. g. no automatic external callback is possible.

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

Fields in the menu Charge Settings

Field	Value
Charge Rate Factor	Enter the factor for the connection costs. The default value is *0.00*.
Currency	Here, enter the name of the currency, e. g. *EUR*, (max. three characters). This entry is just a name which is not involved in any calculation of the tariff unit factor. Special characters are not permitted.
Charge Information (S0 / Upn Extension)	Select the transmission method for charge information on the internal S0 bus. Possible values: • *Keypad*: Depending on country and provider, the charging information is transmitted so as to allow direct display by the terminal. • *Functional*: The charge information is transmitted in binary, coded form, and the terminal first needs to decode it (EURO ISDN). • *Both* (default value): Both protocols are recognised.

Fields in the menu Day Mode

Field	Value
Global Rerouting	Select the call variant in day modus that shall apply to the overall system if no specific redirect has been set up. The default value is *Variant 1*.

Night operation

You can switch the system to night operation and thus enable particular call variants for the team signalling, the door intercom signalling and the rejection functions.

An advanced switching of the call variants is possible via a code or the calendar that has been configured for night operation. You configure a calendar for night operation in the **Applications**->**Calendar**->**Calendar**->**New** menu.

Fields in the menu Night Mode

Field	Value
Team Signalling	Select the call variants for team signalling in night operation. The default value is *Variant 1*.
Doorcom Signalling	Select the door intercom variants for door intercom signalling in night operation. The default value is *Variant 1*.
Rerouting of Incoming Distribution	Select the call variants for reject to message in night operation. The default value is *Variant 1*.
Extension Rerouting	Select the call variants for reject to direct dial-in in night operation. The default value is *Variant 1*.
Global Rerouting	Select the call variants for general rejection in night operation. The default value is *Variant 1*.
Alarm Input	Select the call variants for alarm in night operation. The default value is *Variant 1*.

7.2.2 Passwords

Setting the passwords is another basic system setting.

Note

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

When you log onto your device for the first time, you are prompted to change the password. You need to change the system administrator password in order to be able to configure your device.

Make sure you change all passwords and PIN's to prevent unauthorised access to the device.

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. The default password is *admin*. This password is also used with SNMPv3 for authentication (MD5) and encryption (DES). Some devices have an individual password configured ex works. In this case you can find the password printed on the type label on the bottom of your device.
Confirm Admin Password	Confirm the password by entering it again.

PIN1 and PIN2

You can use various protection functions to prevent misuse of your system. Your system settings protect you by means of a 4-digit PIN1 (pin number). Access from outside (remote access) is protected by a 6-character PIN2.

PIN1 is a 4-digit pin number that allows you to protect system settings from unauthorised access. PIN2 is a 6-digit pin number that prevents unauthorised external subscribers from being able to use your system. These functions can only be used after entering a 6-digit PIN2.

Various settings are protected by the system's PIN1. In the basic setting, the PIN1 is set to

none.

The following performance features are protected using PIN2:

• Remote access for Follow me, room monitoring

Fields in the Configuration via Phone (4-Digit Numeric PIN) menu.

Field	Value
PIN1	Enter PIN1. The default value is *none*. With the 4-digit PIN1 (PIN number) you protect your system settings through configuration via telephone.

Fields in the Remote Access to Phone (6-Digit Numeric PIN) menu.

Field	Value
Remote Access (e.g. Follow me, Room Monitoring)	Select whether a remote access of your system is to be permitted. The function is activated with *Enabled*. The function is disabled by default.
PIN2	Only if **Remote Access (e.g. Follow me, Room Monitoring)** is enabled. Enter the **PIN2**. The default value is *000000*. Through the 6-digit **PIN2** you protect from external access (remote access).

Fields in the SNMP Communities menu.

Field	Value
SNMP Read Community	Enter the password for the user name read. The default password is *admin*.
SNMP Write Community	Enter the password for the user name write. The default password is *admin*.

Field 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. After pressing **OK** or calling the menu again, they are displayed as asterisks.

7.2.3 Date and Time

You need the system time for tasks such as correct time-stamps for system messages, or accounting.

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

ISDN/Manual

The system time can be updated via ISDN, i.e. with every existing external connection the date and time are taken from the ISDN. The date and time can also be entered manually, e. g. if time and date are not sent in the ISDN or no time server is provided. The time remains for approx. 3 hours after the system's power supply is switched off.

The clock switches from summer to winter time (and back) automatically. 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.

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.

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 Basic Settings menu.

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.
	compact systems: The default value is *Europe/Berlin*.
Current Local Time	The current date and current system time are shown here. The entry cannot be changed.

Fields in the Manual Time Settings menu.

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 Automatic Time Settings (Time Protocol) menu.

Field	Description
ISDN Timeserver	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.

Field	Description
	Updating over ISDN is deactivated for the period in which the time is determined by means of a time server. The function is activated with *Enabled*. The function is enabled 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.
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.

Field	Description
	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 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 enabled by default. Clients' time requests are answered in the LAN.

7.2.4 Timer

In the **Timer** menu you can configure the times at which particular system features are to be switched on by default.

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

Fields in the Basic Settings menu.

Field	Description
Call Forwarding (CFNR)	Enter the time in seconds after which a **Call Forwarding (CFNR)** will be executed. Possible values are *1* to *99*. The default value is *15*.
Direct Call	Enter the time in seconds after which the configured number will be dialled when the receiver is lifted. You wish to set up a telephone for which the connection to a specific number is established without entering the number (e.g. emergency telephone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone if necessary (e. g. children or grandparents). If you have set up the "Direct Call" function for one or more telephones, the receiver of the corresponding telephone only needs to be lifted. After a time period without further entries set in configuration, the system automatically dials the configured direct call number. If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated. Possible values are *1* to *30*. The default value is *5*.
External Door Connections	If an external telephone requests a door intercom call, here you can set the time in seconds after which this call is forcefully terminated. Possible values: • *infinite*

Field	Description
	• *60 seconds*
	• *120 seconds*
	• *180 seconds* (default value)
	• *240 seconds*
	• *300 seconds*

Fields in the Advanced Settings menu.

Field	Value
Explicit Call Transfer	Enter the time in seconds after which the initiating subscriber is to be called back or hear call waiting if the required subscriber could not be reached.
	You have passed a caller to another subscriber by brokering or transfer. This subscriber cannot be reached or is engaged. But you wish to prevent the subscriber terminating the call or being diverted by the system after a time. You achieve this using an automatic callback to your telephone. In the case of calls which are transferred with no message (special call transfer, UbA), a callback or call waiting (if there is already a new call) is made to the initiating subscriber after the time entered here.
	Possible values are *10* to *179*.
	The default value is *30*.
Transfer to busy extension	Enter the time in seconds after which a subscriber in the waiting loop is reconnected with the switchboard.
	The switchboard wishes to pass a call to a particular employee. However, this person is currently on the phone. The call can then be switched to the subscriber's waiting loop. If the call is not taken in the time entered here, the switchboard is called again.
	Possible values are *10* to *600*.
	The default value is *30*.
System Parking (Open Enquiry)	Enter the time in seconds after which an open hold for enquiry is terminated and the subscriber called back or given a call waiting.

Field	Value
	You are making a call and want to transfer it to a colleague. Unfortunately, you do not know where this colleague is. **System Parking (Open Enquiry)** holds the caller in the system's queue. You can now make an announcement from your telephone to notify your colleague that the call is waiting. Using a code for the open hold for enquiry, the colleague can take the call on any telephone.
	If a call waiting in the queue is not taken by a subscriber within the time entered here, the initiating subscriber is called back or given a call waiting.
	Possible values are *10* to *600*.
	The default value is *30*.

7.2.5 System Licences

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

The following licence types exist:

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

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

Entering licence data

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

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

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

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

Possible values for Status

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

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

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

7.2.5.1 Edit or New

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

Activating extra licences

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

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

Fields in the Basic Settings menu.

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

> **Note**
>
> If *Not OK* is displayed as the status:

- Enter the licence data again.

- Check your hardware serial number.

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

(2) Press the 🗑 icon in the line containing the licence you want to delete.

(3) Confirm with **OK**.

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

7.3 Access Codes

In your day-to-day work you have employed codes to use particular features and you wish to use them again with your new system. However, other codes are set for these features in the basic setting. No problem - you can change the codes for different features. So you can use your usual codes for these features in the future.

7.3.1 Alternative Access Codes

You use the **Alternative Access Codes** menu to configure the system's access number plan.

The access number can be set individually for some performance features in the system configuration. The access number preset in the system is supplemented with a call number from the system's internal number plan. For performance features **Open inquiry** and **Bundles**, several access codes can be assigned. The performance feature with modified access number is operated as described for the corresponding performance feature. You can use the modified access number (internal number) or the access number described in the user guide (excluding dialling code).

The **System Management**->**Access Codes**->**Alternative Access Codes** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Line Access Digit	Select the exchange code. Possible values: • *None* • *0* (default value) • *6* • *7* • *8* • *9*
Pick-up Group	Enter the new code for performance feature **Pick-up (group)**.
Pick-up (Extension)	Enter the new code for performance feature **Pick-up (internal subscriber)**.
Assign project codes	Enter the new code for performance feature **Assign project codes**.
Speed Dial	Enter the new code for performance feature **Speed Dial**.
Trunk Group Selection	Create the new access numbers for the **Trunk Group Selection** feature. To do this, first click **Add** to create a bundle selection, select the bundle and enter the access number you require for the bundle.
System Parking (Open Enquiry)	Create the new access numbers for the **System Parking (Open Enquiry)** feature. To do this, first click **Add** to create a queue in which the caller is to be held, and enter the access number you require for the queue. You can create a maximum of 10 entries.

7.4 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)

7.4.1 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.

7.4.1.1 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 settings 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 appears, it is forwarded to the MAC address from which the last non-IP unicast frame or non-ARP unicast frame was received on the Ethernet interface of the device. This wildcard MAC address is renewed with each non-IP unicast frame or non-ARP unicast frame.

Field	Value
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.

7.5 Administrative Access

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

7.5.1 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 Set-tings	Only when you make changes to the administrative access con-figuration are relevant access rules set up and activated. You can restore the default settings with the 🗑 icon.

7.5.1.1 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 con-figured.

7.5.2 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 authentication of the SSH connection. Possible options: • *MD5* • *SHA-1* • *RipeMD 160*

Field	Value
	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.
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.
DSA Key Status	Shows the status of the DSA key.
	If no DSA 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,

Field	Value
	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. • *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.

7.5.3 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.
SNMP Listen UDP Port	Shows the UDP port (161) at which the device receives SNMP requests. The value cannot be changed.

Field	Value
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.

7.6 Remote Authentication

This menu contains the settings for user authentication.

7.6.1 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 AC-CESS_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.

7.6.1.1 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 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.

Field	Value
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.
	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 un-

Field	Value
	til 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 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

Field	Value
	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.

7.6.2 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.

7.6.2.1 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+ serv-

Field	Description
	ers 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*. 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.

7.6.3 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.

7.7 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.

7.7.1 Access Profiles

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

By default, the access profiles *TCC_ADMIN*, *HOTEL*, *CHARGES*, *PHONEBOOK* , *PBX_USER_ACCESS* are preconfigured for PABX systems. You can change these using the icon 🖉 or reset them to the default settings using the icon ↻.

7.7.1.1 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.
	Enable or disable **Save configuration**.

Field	Description
	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.

Field	Description
	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.
	Possible values:

Field	Description
	• *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.

7.7.2 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 Q 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.

7.7.2.1 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**.

7.8 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 is-
suer is extremely important. The quality of a certificate is regulated by the German Signa-
ture Act or respective EU Directives.

Certification authorities that issue so-called qualified certificates are organised in a hier-
archy 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 valid-
ity period.

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

7.8.1 Certificate List

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

7.8.1.1 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 fol-
lowing 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.

7.8.1.2 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*.

Field	Description
	Please note that a key with a length of 512 bits could be rated as unsecure, whereas a key of 4096 bits not only needs a lot of time to create, but also occupies a major share of the resources during IPSec processing. A value of 768 or more is, however, recommended and the default value is 1024 bits.
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.

7.8.1.3 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.

7.8.2 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.

7.8.2.1 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.

7.8.3 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.

7.8.3.1 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 8 Physical Interfaces

8.1 Ethernet Ports

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

The Ethernet ports **ETH1** to **ETH4** are assigned to a single logical Ethernet interface in ex works state. The logical Ethernet interface *en1-0* is assigned and is preconfigured with the **IP Address** *192.168.0.250* and **Netmask** *255.255.255.0* .

> **Note**
>
> To ensure your system can be reached, when splitting ports make sure that Ethernet interface *en1-0* with the preconfigured IP address and netmask is assigned to a port that can be reached via Ethernet. If in doubt, carry out the configuration using a serial connection via the **Serial 1** 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.

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.

8.1.1 Port Configuration

Port Separation

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

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

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 four interfaces, *en1-0* to *en1-3*. In the basic setting, switch port **1** - **4** has the *en1-0* interface assigned to it.
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*

Field	Description
	• *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 admin interface.
	Possible values:
	• *1000 mbps / Full Duplex*
	• *100 mbps / Full Duplex*
	• *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 will be controlled.
	• *Auto*: Flow will be controlled automatically.

8.2 ISDN Ports

The system's ISDN connections can be configured as either internal or external ISDN connections. The external ISDN connections are used for connection to the network operator's ISDN network. The internal ISDN connections are provided for connecting various ISDN terminals (system telephones, ISDN telephones, ...).

8.2.1 ISDN External

You configure your system's external ISDN connections in the **Physical Interfaces**->**ISDN Ports**->**ISDN External** menu.

The access configuration for an external ISDN can be set up for point-to-multipoint (P-MP) and point-to-point (P-P).

The following variants are possible when connecting to more than one ISDN connection:

- All external ISDN connections are only point-to-multipoint connections (P-MP).

- All external ISDN connections are only point-to-point connections (P-P).

- The external ISDN connections are point-to-multipoint connections (P-MP) and point-to-point connections (P-P).

8.2.1.1 Working with ✎

Choose the ✎ button to edit an entry.

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

Fields in the Basic Settings menu.

Field	Description
Description	Enter a user-defined description of the ISDN interface. The default value is *ISDN Extern*.
Name	Shows the name of the ISDN interface. Possible values: • *S/U*: 4 wire (S) • */*: Displays the port on the module to which the ISDN connection is connected. Example: *S/U 1* = The interface is in Port 1 and is used as an S connector.
Access Configuration	Select whether the ISDN interface will be operated as a point-to-multipoint connection or as a point-to-point connection. Possible values: • *ISDN P-P* (default value) • *ISDN P-MP*

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

Fields in the Advanced Settings menu.

Field	Description
Permanent Layer 2 Ac-	This function (also known as permanent monitoring) constantly

Field	Description
tivation	monitors the functionality and transmission quality of an external ISDN connection. For this purpose, the system is in permanent contact with your network operator's exchange. If the exchange does not keep the ISDN layer 2 permanently enabled, the system can initiate the repeated establishment of layer 2. The function is activated by selecting *Enabled*. The function is disabled by default.
ISDN Synchronisation	When an external device (e. g. GSM gateway) is connected to an external point-to-point ISDN access in the system, the external device's signal can disturb the synchronisation in the ISDN signal. Only if such a disturbance occurs should you switch off the layer 1 synchronisation. The function is activated by selecting *Enabled*. The function is enabled by default.

8.2.2 ISDN Internal

You configure your system's internal ISDN interfaces in the **Physical Interfaces**->**ISDN Ports**->**ISDN Internal** menu.

A predefined entry with the parameters **Name** = *S/U* 1, **Usage** = *S0*, **Default MSN** = *30 (ISDN 30)* is displayed.

Internal ISDN connections are always point-to-multipoint connections.

When connecting terminals to an internal ISDN connection, please note that not every ISDN terminal sold be retailers is able to use the features provided by the system via your key interface.

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

Fields in the ISDN Internal menu.

Field	Description
Name	Shows the name of the ISDN interface. Possible values:

Field	Description
	• S/U: 4 wire (S)
	• $/$: Displays the port on the module to which the ISDN connection is connected.
	Example: S/U 2 = The interface is in Port 2 and is used as an S connector.
Usage	Shows the function of the ISDN interface.
	Possible values:
	• Upn: Interface for CAPI terminals.
	• Upn: Interface for UPN terminals.
	• $S0$: Interface for ISDN S0 connection.
Default MSN	Shows whether a standard MSN is assigned for an internal S0 bus.
	You can use a standard MSN to access unconfigured S0 terminals.
	As a standard MSN, you can dial the internal numbers configured in the **Numbering**->**User Settings**->**Users** menu and assigned to a terminal in the **Terminals** menu.
Status	Displays the status of the interface.

8.2.2.1 Edit

Choose the button to edit an entry.

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

Fields in the Basic Settings menu.

Field	Description
default MSN	Dial the number you want. You can dial any number that you have configured in the **Numbering**->**User Settings**->**Users**->**Numbers** menu.
	Possible values:

Field	Description
	• *Not configured*
	• *<Subscriber Number>*

8.3 Analogue Ports

8.3.1 Analogue External (FXO)

The **Analogue External (FXO)** menu displays all of your system's available analogue external connections.

The **Physical Interfaces**->**Analogue Ports**->**Analogue External (FXO)** menu consists of the following fields:

Values in the Analogue External (FXO) list

Field	Description
Name	Shows the name of the analogue interface.
	Possible values:
	• *FXO*: Name for the analogue connection.
Description	Shows the user-defined description of the analogue interface.
Dialling Method	Displays the dialling method used.
	Possible values:
	• *Tone Dialling (DTMF)* (default value)
	• *Pulse Dialling (PD)*
Status	Displays the status of the interface.
Action	Change the status of the interface by pressing the ∧ button or ∨ button in the **Action** column.

8.3.1.1 Edit

Choose the ✏ button to edit an entry.

The menu **Physical Interfaces**->**Analogue Ports**->**Analogue External (FXO)**-> 🖉 con-sists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a user-defined description of the analogue interface.
Name	Shows the name of the analogue interface. Possible values: • *FXO*: Name for the analogue connection.
Dialling Method	Select which dialling method should be used. Possible values: • *Tone Dialling (DTMF)* (default value) • *Pulse Dialling (PD)*
CLIP	Select whether the CLIP feature is to be used, i. e. whether the caller's number should be displayed to the person called. Possible values: • *Off* (default value): The caller's number is not displayed to the person called. • *FSK*: The data is sent as DTMF.
Receive charges	Select whether your device is to receive charge information from the network. For this purpose, you can define the charge impulse at 12 kHz or 16 kHz. Possible values: • *Off* (default value) Charge information is not received. • *12 kHz* • *16 kHz*

Fields in the Advanced Settings menu.

Field	Description
Busy Tone Detection	Select whether **Busy Tone Detection** should be used.

Field	Description
	The function is activated by selecting *Enabled*.
	The function is enabled by default.
Dial Tone Detection	Select whether **Dial Tone Detection** should be used.
	The function is activated by selecting *Enabled*.
	The function is enabled by default.
	If the **Dial Tone Detection** is enabled and the external dial tone has been recognised, your **hybird 120** / **hybird 130** immediately starts to dial.
Dial Tone Pause	Only for **Dial Tone Detection** disabled.
	Enter the value you want which the system is to wait for, as a maximum, when dialling a telephone number, before it begins dialling.
	You can switch on the **Dial Tone Pause** if the **hybird 120** / **hybird 130** fails to recognise the external dial tone or if no dial tone is being sent. You must decide the duration of the **Dial Tone Pause**.
	Possible values are whole number values between *1* second and *5* seconds.
	The default value is *1* second.
End-of-Selection Signal	Enter the time that the system is to wait, after dialling a number, before it considers the telephone number to be complete and makes the connection. The default value is *5* seconds.

8.3.2 Analogue Internal (FXS)

The **Analogue Internal (FXS)** menu displays all of your system's available analogue internal connections: the entries *FXS 1* - *FXS 4* for **hybird 120** and *FXS 1* - *FXS 6* for **hybird 130**.

For the entry *FXS 2* the **Usage** *Multi Function Device/Telefax*, for all other entries the **Usage** *Telephone* is set by default.

The menu **Physical Interfaces**->**Analogue Ports**->**Analogue Internal (FXS)** consists of the following fields:

Values in the Analogue Internal (FXS) list

Field	Description
Name	Shows the name of the analogue interface.
	Possible values:
	• *FXS*: Name for the analogue connection.
Usage	Shows the usage of the analogue interface.
	Possible values:
	• *Telephone*
	• *Doorcom Units*
	• *Multi Function Device/Telefax*
	• *Modem*
	• *Answering Machine*
	• *Emergency Phone*
	The function of the analogue terminal is configured in the **Terminals**->**Other phones**->**analog** menu.
Status	Displays the status of the interface.

8.4 DSL Modem

The ADSL modem is ideal for high-speed Internet access and remote access use in SMEs or remote offices.

8.4.1 DSL Configuration

In this menu, you make the basic settings for your ADSL 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 ADSL 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* • *ADSL2 Annex J* • *ADSL2+ Annex J*

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	Select the ADSL synchronization type.

Field	Description
	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.
	• *Automode (Annex-M)*: Only for Annex A devices. The ADSL mode is automatically adapted to the other end with reference to G.992.3 Annex M.
	• *ADSL2 Plus (Annex-M)*: Only for Annex A devices. ADSL2 Plus / G.992.3 Annex M is used.
	• *ADSL2 Annex J*: Only for Annex J devices. ADSL2 Plus / G.992.3 Annex J is used.
	• *ADSL2+ Annex J*: Only for Annex J devices. ADSL2 Plus / G.992.5 Annex J is used.
	• *Inactive*: The ADSL interface is not active.
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**.
	The default value is *Default (Line Speed)*.
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
ADSL Line Profile	Select the internet service provider you require and, in doing so, implicitly select the modem parameter set used by this provider.
	Deutsche Telekom is entered as the default value.
	If your provider is not shown in the list, use the *default* setting.

8.5 Relay

The **hybird 130** has an independent switch contact.

A switch contact may be configured as an on/off switch or as a key. The corresponding function can either be switched on from inside or outside using a code number (with an additional PIN).

Note

The switch contact is reset to idle if the PABX is reset or has a power failure!

8.5.1 Relay Configuration

The switch contact is configured in the **Physical Interfaces**->**Relay**->**Relay Configuration** menu.

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

Fields in the Basic Settings menu.

Field	Description
Contact 1	Enter the desired description of the switch contact at **Description**. Only one function can be assigned to each switch contact.
	Select the type of usage under **Usage**.
	Possibe values:

Field	Description
	• *Access Codes*: The relay is switched via a dial code. • *Access Codes (period only)*: The relay is switched via acces codes for a given period (e.g. a door opener is on for three seconds). • *Access Codes (toggle only)*: The relay is toggled via acces codes. • *Alarm Output*: The relay is switched when an alarm call is received. Enter the duration of the key for **Signalling Period**. The programmed switching time for the button can be anything between 1 and 999 seconds. The default value is *3* seconds.

Chapter 9   VoIP (PABX)

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.

9.1   Settings

You set up your VoIP connections in the **VoIP**->**Settings** menu.

You can telephone over the internet using all internally connected telephones. The number of connections depends on various parameters:

- The availability of the system's free channels.
- The available bandwidth of the DSL connection.
- The configured, available SIP providers.
- The SIP-out licenses that have been entered.

9.1.1   SIP Provider

You configure the SIP provider you want in the **VoIP**->**Settings**->**SIP Provider** menu.

You change the status of the SIP provider by pressing the ∧ button or the ∨ button in the **Action** column.

After about one minute, registration with the provider has taken place and the status is automatically set to ✅ (active).

9.1.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

The menu **VoIP**->**Settings**->**SIP Provider**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	You can enter a name for the SIP provider. A 20 digit alpha-numeric sequence is possible.
Provider Status	Select whether this VoIP provider entry is enabled (*Enabled*, default value) or not (*disabled*).
Access Type	Select which type of VoIP phonenumbers you wish to configure. Possible values: • *Single Number(s)* (default value): Enter the individual DSL phonenumbers. • *Direct Dial-In*: Enter a basic number in conjunction with an extension number block.
Authentication ID	Enter your provider's authentication ID. A 64 digit alpha-numeric sequence is possible.
Password	At this point, you can assign a password. A 64 digit alpha-numeric sequence is possible.
User Name	Enter the user name you received from your VoIP provider. A 64 digit alpha-numeric sequence is possible.
Domain	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. Note: Enter a name or IP address only if this is explicitly specified by the provider.

Fields in the Outgoing Signalisation Settings menu.

Field	Description
Outgoing Signalisation	Select the signal you want for outgoing calls. Possible values: • *Standard* (default value) • *Global CLIP no Screening Number* • *Individual CLIP no Screening Number*

Field	Description
	• *Fixed Out DDI* (Only for **Access Type** = *Direct Dial-In*)
Global CLIP no Screening Number	Only for **Outgoing Signalisation** *Global CLIP no Screening Number* Enter the number that is to be displayed to the person called with any outward connection. This number is not checked.
Signal remote caller number	Only for **Outgoing Signalisation** = *Global CLIP no Screening Number* and *Individual CLIP no Screening Number* You can display the number of an external subscriber if it is signalled. The function is enabled with *Enabled*. The function is disabled by default.
Signal fixed out number	Only for **Outgoing Signalisation** = *Fixed Out DDI* Enter the number that is to be displayed to the person called with any outward connection.

Fields in the Registrar menu.

Field	Description
Registrar	Enter the DNS name or IP address of the SIP server. A 26 digit alpha-numeric sequence is possible.
Registrar Port	Enter the number of the port to be used for the connection to the server. The default value is *5060*. A 5 digit sequence is possible.
Transport Protocol	Select the transport protocol for the connection. Possible values: • *UDP* (default value) • *TCP* • *TLS*

Fields in the STUN menu.

Field	Description
STUN server	Enter the name or the IP address of the STUN server.
	STUN = Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
	A STUN server is required to allow VoIP devices access to the internet behind an active NAT. This determines the current public IP address for the connection, which is used for precise remote addressing.
	Maximum number of characters: 32.
Port STUN server	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 is possible.

Fields in the Timer menu.

Field	Description
Registration Timer	Enter the time in seconds within which the SIP client must re-register to prevent the connection from disconnecting automatically.
	The default value is *600*.

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

Fields in the Advanced Settings menu.

Field	Description
Proxy	Enter the DNS name or IP address of the SIP server. A 26 digit alpha-numeric sequence is possible.
Proxy Port	Enter the number of the port to be used for the connection to the proxy. The default value is *5060*. A 5 digit sequence is possible.
Transport Protocol	Select the transport protocol for the connection.
	Possible values:

Field	Description
	• *UDP* (default value)
	• *TCP*

Fields in the Further Settings menu

Field	Description
From Domain	Enter the SIP provider's "From Domain". It is used after the @ as sender data in the SIP header of the SIP data packages.
Number of allowed simultaneous Calls	Select the maximum number of calls that shall be simultaneously possible Please also note the settings for bandwidth management here. Possible values: • *International* (default value): An unlimited number of simultaneous calls is possible. • *1* • *2* • *3* • *4* • *5* • *10*
Location	Select the location of the SIP server. Locations are defined in the **VoIP**->**Settings**->**Locations** menu. Possible values: • *Any Location* (default value): The server is not operated at any defined location. • *<Location Name>*
Codec Profiles	Select the codec profile for this SIP server. Codec profiles are defined in the **VoIP**->**Settings**->**Codec Profiles** menu. Possible values: • *System Default* (default value): The server is operated with a codec profile predefined in the system. • *<Codec profile name>*

Field	Description
Dial End Monitoring Time	Select the time in seconds (after dialling the last digit of a call number) after which the system begins external dialling. The default value is *5*.
Call Hold inside the PBX system	The network-centric functions call hold, call switching, 3-way conference call and call waiting can be enabled by disabling the option **Call Hold inside the PBX system**. The functions are then no longer provided by the PABX, but by the public network, instead. A corresponding contract with provider and customer is required which incluides a bandwidth limitation (number of simultaneously usable voice channels).
	If a SIP provider - such as Deutsche Telekom - offers multiple SIP accounts / numbers via a single connection, this option should be deactivated for each of them. This is required to support the bandwidth limitation for several numbers via a single network connection.
	If an external call is held, no MoH is played through the PABX, but the public network provides MoH or an announcement for the remotely held party.
Call Forwarding extern (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.
Generate international phone number	If you enable this function and, under **Global Settings**, you have entered the **Country Profile** (*49* for Germany), the 0049 is generated automatically in front of the number when a number with an area code is dialled.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.
Generate national subscriber number	If you enable this function and, under **Global Settings**, you have entered the **National Prefix / City Code** (e.g. *40* for Hamburg), the number dialed is automatically prefixed with 040.
	The function is activated by selecting *Enabled*.

Field	Description
	The function is disabled by default.
Deactivate number suppression	If you enable this function, the number is always sent, independently of whether you have switched **Suppress outgoing CLIP (CLIR)** on or off for an extension.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.
	If the function is disabled, you have additional options.
	In order to ensure that your system can forward anonymous calls with SIP connections you can specify in which part of the SIP header information the string "anonymous call" is is transferred. The information can be transferred in multiple parts. For most prviders you can simply keep the preconfigured setting *Privacy ID* = *Enabled*. For the service provider 1 & 1 you need to additionally enable *Privacy Header*.
	Possible values:
	• *Display*
	• *Users*
	• *Domain*
	• *Privacy Header*
	• *Privacy User*
	• *Privacy ID*
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.

Field	Description
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 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.
Substitution of Interna-	Select whether the prefix (e.g. 00) should be replaced by + for

Field	Description
tional Prefix with "+"	international numbers. The function is activated by selecting *Enabled*. The function is disabled by default.
PBX coupling	Select whether another PABX can log into your system. In this way, several PABX systems can be linked. The function is activated by selecting *Enabled*. The function is disabled by default.
Delete SIP bindings after Restart	If after registering with a provider a reset of the system should occur, for example, or a power failure, depending on the provider, another registration may prove impossible. Enabling these performance features allows re-registration after restart. The function is activated by selecting *Enabled*. The function is disabled by default.
Upstreaming Device with NAT	If you enable this function, you can use a gateway with NAT and still make VoIP calls. Without this function, it may not be possible to call you with VoIP if you use a gateway with NAT. The function is activated by selecting *Enabled*. The function is disabled by default.
Early media support	Select whether you'll allow exchange of voice and audio data before a receiver accepts a call. The function is enabled with *Enabled*. The function is enabled by default.
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

Field	Description
	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.
T.38 FAX support	Select whether faxes shall be transmitted with T.38.
	The function is enabled with *Enabled*.
	The function is enabled by default.
	If the function is disabled, faxes are transmitted with G.711.
Substitution of Incoming Number Prefix	For incoming calls, if the call number should be forwarded in the system in modified form: in the first input field enter the sequence of the incoming number to be replaced by the number sequence entered in the second input field.
Send SIP UPDATE	This function ensures that after a call transfer the number of the new call partner is displayed for the initial calling party.
	Note
	Note that this function is not supported by all service providers.
	Enabled activates the functions.
	The function is not enabled by default.
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. The option is not active per default.
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,

Field	Description
	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.

Fields in the Codec Settings menu

Field	Description
Codec Profiles	Select the location of the SIP server. Locations are defined in the **VoIP**->**Settings**->**Codec Profiles** menu. Possible values: • *System Default* (default value): The server is not operated at any defined location. • *<Codec-Profil-Name>*
Video	Select if calls between IP telephones are to support the transmission of video data. Video transmission can only be negotiated between the participants if both support this feature.
SRTP	Select if calls via this SIP provider may be secured with SRTP (Secure Real-Time Transport Protocol).

9.1.2 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 behave when VoIP subscribers for whom no location has been defined are being registered. Possible values: • *Registration for Private Networks Only* (default value): The VoIP subscriber is only registered if they are within the private network. • *No Registration*: The VoIP subscriber is never registered. • *Unrestricted Registration*: The VoIP subscriber is always registered.

9.1.2.1 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.

Field	Description
	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.
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

Field	Description
	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.

9.1.3 Codec Profiles

In the **VoIP**->**Settings**->**Codec Profiles** , you can define the various codec profiles to control voice quality and set up specific provider-dependent default settings.

When setting up the codec, remember that a good voice quality requires a corresponding bandwidth so that the number of simultaneous calls will be restricted. The remote terminal also has to support the relevant codec choice.

9.1.3.1 Edit or New

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

The menu **VoIP**->**Settings**->**Codec Profiles**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the entry.
Codec Proposal Sequence	Choose the order in which the codecs are offered for use by the system. 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

Field	Description
	menu will be used if possible.
	• *Quality*: The codecs are sorted by quality. The codec with the best quality is used if possible.
	• *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.
G.711 uLaw	Only for **Codec Proposal Sequence** not *default*
	ISDN codec with US characteristic
	G.711 uLaw passes audio signals in the range of 300-3500 Hz and samples them at the rate of 8,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,4. This audio codec uses µlaw quantization.
G.711 aLaw	Only for **Codec Proposal Sequence** not *default*
	ISDN codec with EU characteristic
	G.711 aLaw passes audio signals in the range of 300-3400 Hz and samples them at the rate of 8,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,4. This audio codec uses alaw quantization.
G.722	Only for **Codec Proposal Sequence** not *default*
	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	Only for **Codec Proposal Sequence** not *default*
	G.729 passes audio signals in the range of 300-2400 Hz and samples them at the rate of 8,000 samples per second. At 8 kbit/s bit rate the mean opinion score (MOS) is 3,9.
G.726 (16 kbit/s)	Only for **Codec Proposal Sequence** not *default*
	G.726 (16 kbit/s) passes audio signals in the range of 200-3400

Field	Description
	Hz and samples them at the rate of 8,000 samples per second. At 16 kbit/s bit rate the mean opinion score (MOS) is 3,7.
G.726 (24 kbit/s)	Only for **Codec Proposal Sequence** not *default* G.726 (24 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 24 kbit/s bit rate the mean opinion score (MOS) is 3,8.
G.726 (32 kbit/s)	Only for **Codec Proposal Sequence** not *default* G.726 (32 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 32 kbit/s bit rate the mean opinion score (MOS) is 3,9.
G.726 (40 kbit/s)	Only for **Codec Proposal Sequence** not *default* G.726 (40 kbit/s) passes audio signals in the range of 200-3400 Hz and samples them at the rate of 8,000 samples per second. At 40 kbit/s bit rate the mean opinion score (MOS) is 4,2.
DTMF	Only for **Codec Proposal Sequence** not *default* Select whether the DTMF Outband codec is to be used. First the system attempts to use RFC 2833. If the remote terminal does not use this standard, SIP Info is used. The function is activated by selecting *Enabled*. The function is enabled by default.
G.726 Codec settings	Only for **Codec Proposal Sequence** not *default* Select the coding method for the G.726 codec. Possible values: • *I.366* • *RFC3551 / X.420*

9.1.4 Options

In the **VoIP**->**Settings**->**Options** menu, you'll find general VoIP settings.

The **VoIP**->**Settings**->**Options** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
RTP Port	Enter the port via which the RTP data is to be transported. The default value is *10000*.
Client Registration Timer	Here, enter a default value for the time in seconds within which the SIP clients must re-register to prevent the connection from disconnecting automatically. The default value is *60*.

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

Fields in the Advanced Settings menu.

Field	Description
DSCP Settings for sip Traffic	Select the Type of Service (TOS) for SIP 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 default value is *110000*. • *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.
SIP Port	Specify the port SIP data are to be transferred through.

Field	Description
	The default value is *5060*.
	Note If you change the port during operation, the change only becomes effective after the next reboot of your device.
Client Subscription Timer	Enter a value for the amount of time in seconds after which a SIP client must have re-registered all its configured busy lamp field keys in order for the status information not to get lost. The default value is *300*. You can usually keep the default value, but in case you have many keys configured, it may be a good idea to increase it.

Fields in the SIP over TLS menu

Field	Description
Local Certificate	You can select a certificate fot the use with SIP over TLS. The default certificate is the internal certificate of your device.

Chapter 10 Numbering

10.1 Trunk Settings

Your system is a telecommunication installation for external connection to the Euro ISDN (DSS1) and the Internet:

ISDN connections (S0): Depending on module extension, the system features external ISDN connections (if supported by you device) configured for connection to the network operator's ISDN connection. Depending on module extension, several ISDN connections can either be set as an internal or external ISDN connection.

10.1.1 Trunks

In the menu **Numbering**->**Trunk Settings**->**Trunks** you can see the configured external connections of your system. External connections are configured in the menu **VoIP**->**Settings**->**SIP Provider** or through the respective configuration assistant.

> **Note**
>
> Pure IP devices do not support the creation of new entries.

Values in the Trunks list

Field	Description
Nr.	Shows the sequential number of the connection.
Description	Shows the description of the connection you have configured.
External Port	Shows the port this external connections is connected to.

10.1.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to create new connections.

The **Numbering**->**Trunk Settings**->**Trunks**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	You can enter a designation for the connection you selected.
Access Type	Displays the connection type that has been configured. Possible values: • *ISDN P-MP* • *ISDN P-P* • *FXO*
Port	Only for **Access Type** = *ISDN P-MP* or *FXO* Select the description for the port via which this external connection is made.
Ports	Only for **Access Type** = *ISDN P-P* Select the description for the port via which this external connection is made. All free external ISDN interfaces are available. Select additional ports with the **Add** button, e.g. to configure a party line.

Fields in the Outgoing Signalisation Settings menu

Field	Description
Outgoing Signalisation	Select the signalling you want for outgoing calls. Possible values: • *Standard* (default value) • *Global CLIP no Screening Number* • *Individual CLIP no Screening Number* • *Fixed Out DDI*
Global CLIP no Screening Number	Only for **Outgoing Signalisation** = *Global CLIP no Screening Number* Here you can enter a number that is to be displayed to the called party for all external connections.

Field	Description
	This number is not checked.
Signal remote caller number	Only for **Outgoing Signalisation** = *Global CLIP no Screening Number* and *Individual CLIP no Screening Number* You can have the number of an external party shown if it is being signalled. The function is enabled with *Enabled*. The function is disabled by default.
Signal fixed out number	Only for **Outgoing Signalisation** = *Fixed Out DDI* For all calls "to the outside world" you can have a number displayed, e. g. your switchboard's number.

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

Fields in the Advanced Settings menu

Field	Description
Type of Number	Select the number type for outgoing calls. Possible values: • *System Setting*: The standard system setting (country setting) is used. • *Unknown*: Select this setting if the number type "unknown" is to be signalled. • *Subscriber*: This is an extension number. • *National*: This is a national number (area code + extension number).
Call Hold inside the PBX system	Select whether a telephone call is to be put on hold in the system without losing the connection. The function is activated by selecting *Enabled*. The function is disabled by default.

10.1.2 Trunk Numbers

In the menu **Numbering**->**Trunk Settings**->**Trunk Numbers** you assign the external numbers and the name indicated in a system telephone display to the external connections you've defined.

An external connection can be configured as a point-to-multipoint or point-to-point connection; in the process, the connection description is defined. The intended port name is then assigned to this connection. The port name (**Description**) can be defined under **Physical Interfaces**->**ISDN Ports**->**ISDN External** for the module connection.

External numbers at the point-to-point connection

For a point-to-point connection, you receive a PBX number together with a 1-, 2-, 3- or 4-character extension number range. This extension number range comprises the direct dial-in numbers for the PBX connection. If you've requested several point-to-point connections, the number of extensions can be expanded, or you receive another PBX number with your own extension number range.

With a point-to-point connection, external calls are signalled to the subscriber whose assigned internal number corresponds to the dialled extension number. You configure the internal numbers to be reached directly via direct dial-in of the extension numbers as **Internal Number** in the menu **Numbering**->**User Settings**->**User**->**Add**->**Trunk Numbers**->**Internal Numbers**.

Example: You have a point-to-point connection with the PBX number *1234* and extension numbers from *0* to *30*. A call under *1234-22* is normally signalled at the internal subscriber with call number *22*. However, if you enter extension number *22* in this list, you can define that calls under *1234-22* are signalled at the internal subscriber by call number *321*.

External subscriber numbers at point-to-multipoint connection

For a point-to-multipoint connection, you can request up to 10 numbers (MSN, multiple subscriber number) per ISDN connection. These MSNs are the external subscriber numbers for your ISDN connections. Definition of the internal number occurs under **Numbering**->**User Settings**->**User**->**Add**->**Trunk Numbers**.

10.1.2.1 Edit or New

Choose the icon to edit existing entries. Choose the **New** button to create new numbers.

The **Numbering**->**Trunk Settings**->**Trunk Numbers**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Trunk	Select the connection defined in **Numbering**->**Trunk Settings**->**Trunks** for which to perform the number configuration.
Type of Number	Select the call number type to be defined according to connection type. Possible values: • *Single Number (MSN)*: Only for point-to-multipoint connections. • *P-P Base Number*: Only for point-to-point connections. • *P-P DDI Exception*: Only for point-to-point connections. • *P-P Additional MSN*: Only for point-to-point connections.
Displayed Name	In general, you enter the name to be displayed for this number in the called system telephone's display. Für **Type of Number** = *P-P Base Number* this field displays the name of the connection.
Single Number (MSN)	Here, enter the MSN for a point-to-multipoint connection.
P-P Base Number	Here, enter the number for the point-to-point connection (without direct dial number).
P-P DDI Exception	Here, enter the direct dial exception for a point-to-point connection. Note: Only enter the extension according to your extension number range that should be routed to differing internal subscriber numbers. Direct dial at the point-to-point connection always proceeds to the subscriber whose number was dialled along as extension. E. g. the internal subscriber has the number *16*. If this subscriber is called from outside on *1234567-16*, the call is signalled at his telephone. However, if with direct dial *16* a subscriber with the number *888* is to be called, enter *888* as the exception number. In **Incoming Distribution** you then assign the exception number to the subscriber with the number *16*. You can subsequently perform additional settings in

Field	Description
	Incoming Distribution.
P-P Additional MSN	Here, enter an additional MSN for a point-to-point connection.
	With some providers, it's possible to also transmit a point-to-multipoint number on a point-to-point connection in parallel to the direct dial number; e.g. a fax number pre-existing setup of a point-to-point connection, or the old point-to-multipoint number.

10.1.3 Trunk Groups

In the **Numbering**->**Trunk Settings**->**Trunk Groups** menu, you can group the various external connections and individually provide these to the users.

You wish to assign specific external connections to internal subscribers for outgoing connections. You can join these external connections together to create bundles and supply these to extensions for outgoing calls. In this way, all extensions start external dialling with the same dialling code, but can only establish a connection using the bundle released for the extension in question.

The external connections of your system can be grouped into bundles. You can configure up to 99 bundles (01 - 99). The code number for bundle assignment can be modified (menu **Alternative Access Codes**).

When initiating an external call through the bundle code number, the bundle cleared for the subscriber is used in connection setup.

Only for compact systems: A predefined entry with the parameters **Description** = *ISDN External* and **Sequence in Trunk Group** = *ISDN External* is displayed.

10.1.3.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to create a new bundle.

The **Numbering**->**Trunk Settings**->**Trunk Group**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.
	The default value is *ISDN Extern*.

Field	Description
Sequence in Trunk Group	Select the desired external connections for a bundle. The order when dialling to the outside matches the sequence of external connections in this list. You wish to assign specific external connections for outgoing connections to the internal subscribers of your system. You can group external connections into bundles and provide these to subscribers for the outgoing dialling. In this way, all subscribers initiate the external dialling with same bundle access code, but can only set up a connection over the bundles for which they have been cleared.

10.1.4   X.31

Packet-switched data transmission (X.31)

To improve customer service, you wish to allow cashless payment methods such as debit or credit card, or record purchase data for a customer card. For this purpose, you connect a data device to your system, which transmits data for customers and credit cards to a central location.

You can connect a data device which operates according to the X.31 transmission standard (data transmission over the D channel) to the system's internal ISDN connections. These are, for example, checkout terminals, cashpoints or customer card terminals.

For use of these performance features, your network operator provides you TEI's (Terminal Endpoint Identifier), which you assign to individual connections when configuring your system. An additional addressing of these terminals occurs via these TEI's.

Note

You can only use this performance feature if performance feature **X.31** has been requested from the network operator, and you operate a corresponding terminal on this connection. For information on operation, please see the user's guide for your terminals.

10.1.4.1 Edit or New

Choose the ⟋ icon to edit existing entries. Select the **New** button to set up new X.31 applications.

The **Numbering**->**Trunk Settings**->**X.31**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Select Interface	Select the external interface over which you access the network operator providing you performance feature X.31.
Terminal Endpoint Identifier (TEI)	Here, select the TEI value (TEI, Terminal Endpoint Identifier) which you have received from your network operator. An additional addressing of these terminals occurs via the TEI's. Possible values are 00 to 63. The default value is 00.
Internal Assignment	Select the internal ISDN interface to which your data device, which operates according to the X.31 transmission standard (data transmission over the D channel), is connected.

10.2 User Settings

In this menu, you configure and administer your system's users. The users are organised into authorisation classes to which the desired external lines are assigned, and which may use performance features according to request. The user assigned to an authorisation class receives an internal number and specific authorisations. A default authorisation class (Default CoS) is preset ex-works, to which new users are automatically assigned.

After it's been defined in User Settings which functions and authorisations a user, or several users, have access to, authorisation of user settings is assigned to a terminal in menu **Terminals**. In this way, its possible to create settings for several terminals via an authorisation class, e. g. a user setting *Boss*, a user setting *Department Head* and a user setting *Clerk*. Now, all that's left to do is assign the corresponding terminals to one of these **Class of Service**.

10.2.1 Users

In the **Numbering**->**User Settings**->**Users** you configure the users of your system, their class, and assign them internal and external numbers.

You see an overview of the users that have been created. The entries in the **Name** column are sorted alphabetically. Click the column title of any other column to sort entries in ascending or descending order

Only for compact systems: The following users are predefined:

- *User 1 to User 4 analog Tel*
- *User 5 and User 6 Sys Tel*
- *User 7 DECT*
- *User 8 and User 9 ISDN*

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

10.2.1.1 Basic Settings

Enter basic user information in the **Numbering**->**User Settings**->**Users**->**Basic Settings**
menu.

The **Numbering**->**User Settings**->**Users**->**Basic Settings** menu consists of the following
fields:

Fields in the Basic Settings menu.

Field	Description
Name	Enter the name of the user.
	This name is displayed in the phone book if you have entered a number and cleared it for the phone book under **Mobile Number Home Number**. The name is displayed with the codes (M) for mobile communication, and (H) for home number in the system telephone display.
Description	Enter additional user information.

Fields in the External Numbers menu.

Field	Description
Mobile Number	Enter a number under which the user can be reached via mobile phone. Also select whether this number is to be shown in the system telephone display so that it can be dialled on the system telephone from the system phone book (**Access from system phone** option).
Home Number	Enter a number under which the user can be reached privately. Also select whether this number is to be shown in the system telephone display so that it can be dialled on the system tele-

Field	Description
	phone from the system phone book (**Access from system phone** option).
E-mail Address	Enter the e-mail address for the user.

Fields in the Class of Service menu.

Field	Description
Standard	Select the authorisation class = CoS (Class of Service). Definition of the authorisation class and creation of new authorisation classes occurs under **Numbering**->**User Settings**->**Class of Services**. Only selection occurs in this setting. Possible values: • *Default CoS* (default value) • *Not allowed*: No class of service • *<Authorisation class>*
Optional	Select an optional authorisation class. This CoS is required for the calendar settings. Definition of the authorisation class and creation of new authorisation classes occurs under **Numbering**->**User Settings**->**Class of Services**. Only selection occurs in this setting. Possible values: • *Default CoS* (default value) • *Not allowed*: No class of service • *<Authorisation class>*
Night	Select the authorisation class for night operation. This CoS is required for the calendar settings. Definition of the authorisation class and creation of new authorisation classes occurs under **Numbering**->**User Settings**->**Class of Services**. Only selection occurs in this setting. Possible values: • *Default CoS* (default value) • *Not allowed*: No class of service • *<Authorisation class>*

Fields in the Further Options menu.

Field	Description
Busy on busy	Select whether the performance feature "Busy on Busy" shall be enabled for this user.
	If a subscriber for whom multiple telephone numbers have been configured makes a call, you can decide whether additional calls for this user shall be signalled. If "Busy on Busy" is set for this user, other callers get an **Engaged** signal if the user is calling on one of her numbers.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.

10.2.1.2 Numbers

In the menu **Numbering**->**User Settings**->**Users**->**Numbers** internal numbers which are later assigned to the terminals can be entered. Depending on the type, one or more numbers can be assigned per terminal.

The **Numbering**->**User Settings**->**Users**->**Numbers** menu consists of the following fields:

Fields in the Internal Numbers menu.

Field	Description
Internal Numbers	Enter the internal numbers for the user and the description to be shown in the system telephone display (**Displayed Description**). In addition, select whether this internal number shall be displayed in the **System Phonebook**, and whether the LED next to the corresponding function key (**Busy Lamp Field**) should light up.
	The functions are activated by default.
	Add new **Internal Numbers** with **Add**.
	Only for compact systems: Users with the internal numbers *10*, *11*, *12*, *13*, *20*, *21*, *22*, *30* and *35* are predefined.

10.2.1.3 Outgoing Signalisation

In the **Numbering**->**User Settings**->**Users**->**Outgoing Signalisation** menu, select the outgoing numbers for the user.

For an outgoing call, if the remote subscriber should not see the number assigned to your own connection, one of the existing numbers can be selected here for display. If no number is defined, the system transmits no number to the provider.

Fields in the list Outgoing Signalisation

Field	Description
Internal Number	Displays the internal numbers configured for the user.
Displayed Description	Displays, for each internal number, the description configured for the system telephone display.
Outgoing Signalisation	Select the signal you want for outgoing calls. Possible values: • *Default, own DDI Signalling*: The user's own extension is used as the **Outgoing Signalisation**. This option is available when there is a point-to-point configuration or a SIP provider with direct dialling. • *Standard*: No **Outgoing Signalisation** is sent. In this case, the switchboard uses the port's main number. • *<Fixed phone number>*: For a FXO port, the phone number configured is already assigned as the **Outgoing Signalisation** and is displayed. • *<Phone number>* : When more than one number has been configured, you can select a number that you wish to use as the **Outgoing Signalisation**.

Select the ✎ icon to specify for each internal number (indicated in the table by **Internal Number** and **Displayed Description**) which number shall be displayed for outgoing calls. Here, for each configured external connection, select one of the numbers configured for this purpose.

If more than one external connection has been configured, you can specify the procedure for outgoing calls. When an external line is engaged, the order of the entries determines the sequence in which the other lines assigned will be used to dial.

The configured **Outgoing Signalisation** can be hidden for each outgoing line; to do so, put a tick under **Hide Number** in the relevant row.

If you wish to move an entry in the list displayed, select the $\uparrow_\downarrow$ icon in the relevant row. A new window opens.

The selected entry is displayed under **External Connection**, here e. g. *ISDN_1*.

Proceed as follows to move the selected entry:

(1) Under **Move**, select in the list the entry relative to which you wish to move the selected entry, here e. g. *1.SIP-Provider_1*.

(2) Select whether you want to insert the entry *above* or *below* the selected entry in the list, here e. g. *above*.

(3) Select **Copy**.
    The entries display in the changed order.

(4) If the list contains more than two entries, move other entries if you wish.

The sequence configured here overwrites the setting that is assigned by the permission class. However, the assigned permission class continues to determine whether a user has access to a particular external connection.

10.2.1.4 Optional Rerouting

In the **Numbering**->**User Settings**->**Users**->**Optional Rerouting** menu, to each displayed subscriber internal number you can assign a **Redirect application** and a **Active Variant (Day)**.

Here, for example, you can define to which co-worker calls shall be forwarded when you're in a conference, or whether the head office is responsible for taking calls during lunch.

Fields in the Optional Rerouting menu.

Field	Description
Internal Number	Displays the internal numbers configured for the user.
Displayed Description	Displays, for each internal number, the description configured for the system telephone display.
Rerouting Application	Select from the dropdown list the desired redirect application that you wish to assign to the internal number. You may choose from the redirect applications that you've configured in the **Applications**->**Rerouting**->**Rerouting Applications**->**New** menu

Field	Description
	with **Type of redirect application** = `Internal Subscriber`. Possible values: • `None` (default value) • <Redirect application>
Active Variant (Day)	Select the redirect application variant to be currently enabled. If a variant switch is set up via the calendar, this setting will be switched back again at the appropriate time. Possible values: • `Variant` • `Variant 2` • `Variant 3` • `Variant 4`

10.2.1.5 Authorizations

In the menu **Numbering**->**User Settings**->**Users**->**Authorizations** you can allow this user to make certain settings himself via HTML configuration. For this, a user name and password must be entered in the user HTML configuration, and personal access authorised. Once logged out, you can view and modify the corresponding settings after entering this user name and password.

The **Numbering**->**User Settings**->**Users**->**Authorizations** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Password for IP Phone Registration	Enter the password with which a user IP telephone must log into the system. The password can remain free if IP telephones log in but need not authenticate themselves.
PIN for Phone Access	Here you can change the PIN for the user's personal answering machine (voicemail box). The default value is `none`.

Fields in the User HTML Configuration menu.

Field	Description
Personal Access	Select whether this user shall receive access authorisation to a personalised user interface (user access) where he can perform his own entries and settings. The function is activated by selecting *Enabled*. The function is disabled by default.
Login Name	Only for **Personal Access** enabled. Enter a user name for this user. This is required for login on the user interface.
Password	Only for **Personal Access** enabled. Enter a password for this user. This is required for login on the user interface.

Call Through

Call Through consists in dialin to the system via an external connection and the call put through from the system via another external connection.

> **Note**
>
> In the connection data records, one data record is created for the incoming connection and one for the outgoing connection.

Fields in the Further Options menu.

Field	Description
Call Through	Select whether Call Through should be authorised for this user. The function is activated by selecting *Enabled*. The function is disabled by default. When you enable the function, you must select under **Use routing and signalisation from number** the internal number from which the authorised external lines and call options for Call Through shall be used.

10.2.2 Class of Services

In the **Numbering**->**User Settings**->**Class of Services** (CoS) the functions and perform-
ance features for the user settings are defined. These authorisation classes can then be
assigned to individual users (user groups) in the user settings.

Choose the ✎ icon to edit existing entries. Choose the **New** button to create additional au-
thorisation classes. The authorisation class *CoS Default* is configured by default.

10.2.2.1 Basic Settings

In the menu **Numbering**->**User Settings**->**Class of Services**->**Basic Settings**, the basic
settings along with the name for the new authorisation class are defined. The authorisation
class can be located via the name.

The **Numbering**->**User Settings**->**Class of Services**->**Basic Settings** menu consists of
the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.

Fields in the Line Access Authorization menu.

Field	Description
Line Access Authoriza-tion	Select line access authorisation for the authorisation class. Line access authorisation determines which calls (internal, ex-ternal,...) are allowed. The system distinguishes several author-isation levels. Possible values: • Unlimited: The telephones have unrestricted dialling author-isations and can initiate all connections. • *National*: The telephones can initiate all calls except inter-national calls. If a number starts with the code for international dialling, the number cannot be dialled. • *Incoming*: The telephones can receive incoming external calls, but cannot initiate any external calls. Internal calls are possible. • *Region*: The telephones cannot make any national or inter-

Field	Description
	national calls. For this dial permission, 10 exception numbers allowing national or international dialling can be configured. An exception number can consist of complete call numbers or sections thereof (e. g. the first numerals). • *Local*: The telephones can make local calls. National and international calls are not possible. • *Internal*: The telephones do not have authorisation for incoming or outgoing external calls. Only internal telephone calls are possible.
Automatic Outside Line	This setting defines whether automatic outside line is set up for this authorisation class. With automatic outside line, users of this authorisation class hear the external dialling tone after picking up the receiver and can immediately dial outside. To make internal calls, press the star key after picking up the receiver. If you have set up an automatic outside line for an internal subscriber, the keypad functions cannot be directly used. First disable the **Automatic Outside Line** or dial the star key, then the code for manual outside line (e. g. 0) followed by keypad dialling, beginning with the star or hash key.
Trunk Line Selection with Line Access Number	Select the connections over which outgoing calls from these telephones shall be externally routed. The order of entries determines in which sequence, in case of an engaged external line, dialling shall occur over the other assigned lines
Allow manual trunk group selection	Besides general exchange access, a telephone can also selectively use a bundle. Here an external connection is initiated with the corresponding code for the target assignment of the bundle and not by dialling the dialling code. To be able to perform a selective bundle assignment, the authorisation class must possess the appropriate authorisation. The authorisation can also include bundles that the authorisation class can otherwise not assign. If a telephone does not possess the authorisation for selective bundle assignment, or if the selected bundle is in use, the busy tone is heard after dialling the code. If **Automatic outside line** is set up for an authorisation class, users of this authorisation class must press the star key before selective bundle assignment, then initiate external dialling with the code for bundle assignment.

Field	Description
	The function is activated by selecting *Enabled*.
	The function is disabled by default.
	Then select the bundles for which manual bundle assignment is to be allowed. You can configure bundles in the **Numbering**->**Trunk Settings**->**Trunk Groups** menu.

Number display

If you call a subscriber, your number is displayed to him. The person you're calling thus sees that you are calling even before picking up the receiver. If you don't want the person you're calling to see your number before picking up the receiver, you can prevent display of your number to your called party.

If your called party has set up call forwarding, you won't know at which telephone you've reached him. In this case, you can display the number to which your called party has forwarded the call. However, the person you're calling also has the option of preventing display of this number.

Call number display allows display of the caller's number already at call signaling, even on analogue telephones. Thus, you know who wishes to speak to you even before you've accepted the call.

Note

Transmission of analogue CLIP data can be set up separately for every analogue connection. Please refer to the users' guides for your analogue terminals to determine whether these support the "CLIP" and "CLIP off Hook" performance features.

Not all described performance features are included in the ISDN standard connection. Please inquire of your network operator the extent to which individual performance features must be separately ordered for your ISDN connection.

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

Fields in the Further Settings menu.

Field	Description
Dial Control	Select whether numbers entered in the **Call Routing**->**Outgoing Services**->**Dial Control** menu shall be allowed or denied also for this authorisation class.

Field	Description
	The function is activated by selecting *Enabled*. The function is disabled by default.
Automatic Route Selection (ARS)	Select whether the routing rules entered in the **Call Routing**->**Automatic Route Selection** menu shall also be applied to this authorisation class. The function is activated by selecting *Enabled*. The function is disabled by default.
Show Outgoing Number (CLIP)	Select whether the caller number shall be displayed to the called party. The function is activated by selecting *Enabled*. The function is enabled by default.
Show Connected Number (COLP)	Select whether the called party number shall be displayed to the caller. If, for example, the called party has set up call forwarding to a third subscriber, the caller can display the number of the call forwarding destination using this performance feature. The function is activated by selecting *Enabled*. The function is enabled by default.
Additional Info for Extern Call	Select what should be displayed for an exchange call. Possible values: • *Trunk and Number Name*: The display shows the exchange connection and the assigned name alternatively. • *Trunk Name Only*: Only the name assigned to the exchange connection is displayed. • *Number Name Only* (default value): The display shows the name assigned to the external number only. • *None*: Display is blank.

10.2.2.2 Features

Additional functions are configured in the **Numbering**->**User Settings**->**Class of Services**->**Features** menu.

Call pickup

A call is signalled to a co-worker who is presently absent from his work station. You now have two options to respond to the caller. You could walk over to your colleague's telephone, or transfer your colleague's call to your phone. Assignment is done by the option **Pick-up Group** in the menu **Features**; the group is then assigned to a user. If the values are identical, a call pickup is possible. Call pickup is not possible for open inquiry.

System telephones can pick up calls via programmed function keys. You can set up line keys, connection keys and team keys on system telephones.

- Line key: An ISDN connection or a VoIP provider is set up under a connection key. The LED assigned to the line key indicates the connection status. The LED lights up if both B channels of a connection are in use, or when the maximum number of simultaneous connections over a VoIP provider is reached. If an external call is signalled on another internal telephone, you can pick it up by pressing this line key.

- Line key: A system user is set up under a connection key. The LED assigned to the connection key indicates the subscriber status (call, connection,...). If a call is signalled for this internal subscriber, you can pick it up by pressing this connection key.

- Team key: A team key is a normal line key to which the internal number of a team is assigned. The LED assigned to the team key indicates the team status (call, connection,...). If a call is signalled for this team, you can pick it up by pressing the team key.

Call waiting

As far as possible, you want to accept calls from every customer, even while you're already on the phone. If another call is signalled to your phone by a call-waiting tone or display notification, you can decide with which of two customers you wish to speak.

If a currently engaged subscriber is called, she gets automatic call-waiting. Call-waiting is possible for internal and external calls. The call-waiting connection is signalled to the called party visually and/or acoustically, depending on the terminal.

The called party can:

- Decline the call-waiting connection and proceed with the current call. The caller is then signalled "engaged".

- Accept the call-waiting connection and hold the current connection.

- Accept the call-waiting connection after the current connection is ended.
- Ignore the call-waiting connection. Call-waiting automatically ends after 30 seconds and the caller hears a "busy" signal.

Analogue terminals

The call-waiting option can be individually configured for every subscriber. Allowing call waiting or not can be set via configuration or via a code number in operations.

Analogue terminals get the system call waiting tone. The number of the call-waiting party can be shown in the analogue telephone display if it features the corresponding perform-ance feature (CLIP off Hook). CLIP off Hook is disabled for analogue terminals in the basic setting, but may be enabled via configuration.

Call waiting can only occur simultaneously in the system for a limited number of analogue connections. If call waiting is already operating with this maximum number of call-waiting tones on analogue connections, additional call-waiting callers will get the busy tone.

If you hear the call-waiting tone during a call, you can take that call and transfer the ongo-ing call An operating procedure allows transfer of the ongoing call and acceptance of the call waiting. The following conditions apply here:

- Every dialled number is accepted by the system.
- After the operation procedure, the subscriber and the call-waiting subscriber are immedi-ately connected to each other (no acknowledge tones).
- Transfer to one's own number is possible, then call waiting.
- Internal, external target subscribers as well as teams can be dialled.
- A return call occurs in case of invalid or engaged target number.
- If the subscriber is free, a return call is made according to the target subscriber's defined period.
- With transfer to a team number, there is no return call in case of an engaged or unreach-able team
- With transfer to a team number only return call after time is supported.

ISDN terminals

Configuration and operation of call waiting occurs as described in the users' guides of the corresponding terminals. ISDN terminals use their own tones to signal call waiting.

Note

Call waiting is not possible:

- for conference calls

- for do not disturb (analogue terminals)

- for announcements

- for room monitoring

- for terminals, for which the Data Protection performance feature is set up (e. g. fax, modem)

- in analogue subscriber's dialling status (the receiver has been picked up, but there is no connection yet)

- for current call-waiting protection

- for dialling a team number. Then there is no call waiting for analogue team subscribers.

ISDN telephones can also transfer a call waiting to another subscriber via the "Call Deflection" performance feature. An active connection is ended by replacing the receiver, for example. The call waiting connection is then signalled and can be accepted, e. g. by picking up the receiver.

The **Numbering**->**User Settings**->**Class of Services**->**Features** menu consists of the following fields:

Fields in the Feature Authorization menu.

Field	Description
Pick-up Group	Enter the number of the group in which calls may be picked up.
Call Waiting	Select whether call waiting shall be allowed for this authorisation class. The function is activated by selecting *Allowed*. The function is enabled by default.
Use global rerouting	Select whether global redirect shall be allowed for this authorisation class. The function is activated by selecting *Enabled*. The function is disabled by default.

Field	Description
	Note
	The redirect target must be in a class of service that does not allow global redirect.
Switch signalling vari-ants manually	Select whether manual switching of call options shall be allowed for this authorisation class.
	The function is activated by selecting *Allowed*.
	The function is disabled by default.
Call Through	Select whether Call Through shall be allowed for this authorisa-tion class.
	The function is activated by selecting *Allowed*.
	The function is enabled by default.

Simplex operation

The simplex operation function allows you to set up a connection from a system telephone to another system telephone without this connection having to be actively accepted by the called system telephone (pick up receiver, switch on loudspeaker/hands-free). As soon as the system telephone has accepted the simplex operation connection, the connection is set up. The caller and the called system telephone hear an attention tone at the beginning of the simplex operation. Duration of the simplex operation is limited to two minutes. If the receiver of a concerned telephone is picked up during this period, the call is translated into a normal connection.

System telephones can initiate a simplex operation call via the system telephone menu or a programmed function key. If the simplex operation is initiated via a function key, notifications appear in the system telephone display as with a normal connection and the simplex operation key LED is switched on. The simplex operation can be ended by renewed pressing of the function key or by pressing the loudspeaker key. The LED switches off again at conclusion of the simplex operation.

If a telephone or a system telephone is the destination of a simplex operation call, the caller's number is indicated in the display. The simplex operation call is signalled over the loudspeaker with an attention tone. Simplex operation can be terminated with the ESC key.

A function key can also be configured on a system telephone to deny or allow simplex operation calls.

Note

Simplex operation calls are automatically accepted by the called telephone by enabling the hands-free function, if:

• the telephone is not in use
• simplex operation is allowed and
• the "Do not disturb" function (Call Protection) is disabled.

If a simplex operation connection is not ended by both subscribers, the connection is automatically ended by the system after ca. 2 minutes.

Message

Do you wish to call your co-workers to a meeting or to a meal? You could call each of them individually, or simply use the announcement function. With just one call, you reach all the announcement-enabled telephones without subscribers having to pick up the receiver.

Caution

Although you can be heard with the announcement, you cannot hear any comments your colleagues or family members make.

The announcement function allows you to set up a connection to another telephone without this connection having to be actively accepted by the latter (pick up receiver or switch on loudspeaker/hands-free). As soon as a telephone has accepted the announcement, the connection is active. The announcer and the called subscriber initially hear a positive acknowledge tone. Announcement duration is unlimited.

Announcements are possible to ISDN and analogue telephones if these support the announcement performance feature. Please refer to the user's guide for your telephones to determine whether the performance feature is supported.

Announcements can be allowed or denied to telephones via a code number.

System telephones

Announcement to and from system telephones is possible. System telephones can initiate an announcement via the system telephone menu or using a programmed function key. If the announcement is initiated via a function key, notifications appear in your telephone display as with a normal connection and the announcement key LED is switched on. The announcement can be ended by renewed pressing of the function key or by pressing the

loudspeaker key. The LED switches off again at conclusion of the announcement.

If a system telephone is the destination for an announcement, the number of the announcer appears on the display. The announcement is signalled with a positive acknowledge tone over the loudspeaker. The announcement can be terminated with the ESC key.

A function key with associated LED can also be set up on a system telephone to deny or allow announcements.

Individual announcement

You can initiate the announcement in a selective manner by dialling an internal number. The announcement can be allowed or denied by the destination subscriber via an operating procedure. The announcement is signalled to the destination subscriber and the announcer with a positive acknowledge tone.

Team announcement

An announcement can also be made to a team by dialling a team number. The team subscribers hear the announcement simultaneously. The announcement is signalled to the destination subscribers and the announcers with a positive acknowledge tone. The announcement to a team is also possible from an inquiry. With a team announcement, it can take up to four seconds before the connection to the individual team subscribers is established. The announcement then proceeds to the team subscribers who have accepted the announcement within this period.

Note

Announcements are automatically accepted by the called telephone by enabling the loudspeaker function, if:

- the telephone is not in use
- the announcement is set up and
- the "Do not disturb" function is not active.

MWI (Message Waiting Indication)

You've got new messages in your mailbox, or new e-mails waiting at your Internet service provider. as you have no prior knowledge, you must constantly check whether you do actually have new messages. With the MWI performance feature, your system receives the information about new messages from the corresponding service provider. Now you merely need query your mailbox or e-mail POB if new messages really are present. You can also send a MWI from a voicebox connected to the system, or from a system telephone set up

as a reception telephone.

This information can be displayed or signalled on terminals (analogue terminals, ISDN terminals and system telephones) that support this performance feature. MMW information from outside is conveyed transparently by the system. When an MMI is present, the bintec elmeg telephone displays an envelope symbol and a text generated in the telephone, along with the caller's phone number.

Analogue terminals

- Switching on the MMI can only occur with receiver replaced.
- If there's a message from a voicemail system, there's a short call. Depending on the terminal, a symbol, a text generated in the telephone as well as the caller's telephone number can be displayed. If MWI information is deleted, there is no signalling.
- For the terminal, CLIP must be set up and enabled in the configuration.
- Callback to the voice mail system or reception telephone is possible; the MMI information is deleted in the process.

ISDN terminals

- Switching on the MWI is possible at all times (also during the call).
- If there's a message from a voicemail system, there's a short call. Depending on the terminal, a symbol, a text generated in the telephone as well as the caller's telephone number can be displayed. If MWI information is deleted, there is no signalling.
- Callback to the voice mail system or reception telephone is possible; the MMI information is deleted in the process.

System telephones

- Switching on the MWI is possible at all times (also during the call). The caller's number is entered in the caller list. Depending on the type of system telephone, e. g. external voicemail, Netbox Heute, the name and number of the caller are entered. In addition, the **Caller list** LED flashes.
- Callback to the voice mail system or reception telephone is possible; the MMI information is deleted in the process.

Hotel room telephone

- If a message from a voicemail system is present, a special dialling tone is heard after the receiver is picked up.

Reception telephone

- MWI information can be switched on and off from a reception telephone to a room tele-

phone via a telephone procedure. If MWI information is switched to a room telephone, the reception telephone number is entered into the caller list and the special dialling tone is enabled.

Disabling the MWI announcement

- Manual disabling via reception telephone procedure.
- Call from reception telephone to room telephone. The MWI information is automatically deleted in call status.
- Callback from room telephone to reception telephone deletes the MWI information.

Note

This performance feature must be requested for your ISDN connection from the network operator. There, you will also be informed of available services. The information can only be displayed on the internal ISDN terminal if an external MSN has been assigned to the terminal in the configuration.

All MWI data are deleted after a system reset.

Net Direct (keypad)

Some time ago, you purchased the most advanced telephone of the time. Since then, however, a number of new performance features have appeared on the public network, which cannot be used by simply pressing a key. You can use the keypad function to employ your network operator's current ISDN functions by entering a key sequence from your ISDN or analogue telephone.

The keypad function allows control of service or performance features in your operator's network by entering character and numerical sequences.

Note

You can only use the keypad performance feature if it is supported by your network operator and has been requested for your ISDN connection. If you have set up an automatic outside line for an internal subscriber, the keypad functions cannot be directly used. First disable the **Automatic Outside Line** or dial the star key, then the code for manual outside line (e. g. 0) followed by keypad dialling, beginning with the star or hash key.

Keypad functions can only operate from terminals that have been assigned an external multiple subscriber number (MSN) in configuration and possess a keypad authorisation.

Your network operator's performance features are always set up for the number (MSN) sent by your terminal.

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

Fields in the Advanced Settings menu.

Field	Description
Receive System Inter-com Call	Select whether simplex operation calls to the system telephone shall be allowed for this authorisation class. The function is activated by selecting *Allowed*. The function is enabled by default.
Receive Announce-ment Calls	Select whether this authorisation class may receive announce-ments. The function is activated by selecting *Allowed*. The function is enabled by default.
Receive MWI Informa-tion	Select whether this authorisation class may receive information about existing messages (MWI = Message Waiting Indication). The function is activated by selecting *Allowed*. The function is enabled by default.
Net Direct (Keypad)	Select whether you wish to use your network operator's current ISDN functions also from older ISDN or analogue telephones by entering a key sequence. The function is activated by selecting *Allowed*. The function is disabled by default.

10.2.2.3 Applications

Additional applications are configured in the **Numbering**->**User Settings**->**Class of Ser-vices**->**Applications** menu.

The **Numbering**->**User Settings**->**Class of Services**->**Applications** menu consists of the following fields:

Fields in the Application Authorization menu.

Field	Description
System Phonebook Authorization	Select whether this authorisation class may use entries in the system phone book and, if so, to what extent. Possible values: • *Yes, according to line access authorization* (default value): System phone book entries may be used unless located beyond the configured line access authorisation. • *Yes, without restrictions*: System phone book entries may be used in unrestricted access. • *No*: System phone book entries may not be used.
Music on Hold	Select whether and which MoH (Music on Hold) shall be used. Possible values: • *Off* (default value): A caller on hold shall hear no music-on-hold. • *<MoH-Wave file>*: A caller on hold should hear the selected Wave file as music-on-hold. • *MOH Intern 1* (default value for compact systems) • *MOH Intern 2* • *MoH Wave 1 to 8*
Doorcom Access	Select whether this authorisation class may connect to the door intercom. The function is activated by selecting *Allowed*. The function is enabled by default.
TAPI	Select whether this authorisation class may use the system's TAPI functionalities. The function is activated by selecting *Allowed*. The function is enabled by default.
Save call data records	Define whether the connection data of this authorisation class shall be saved.

Field	Description
	The function is activated by selecting *Enabled*.
	The function is enabled by default.
Transmit charge information	Select whether the transferred charge information shall be transmitted to terminals of this authorisation class.
	The function is activated by selecting *Allowed*.
	The function is enabled by default.
Relay Contact(s) Access	Within an authorisation category, you can enable or prohibit the permission to configure a relay for each contact individually.
	The function is activated by selecting *Allowed*.
	The function is disabled by default.

10.2.3 Parallel Ringing

In the **Numbering**->**User Settings**->**Parallel Ringing** you configure whether, in case of incoming calls to an internal number, there shall be parallel signalling to another external number.

10.2.3.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to create other entries.

The **Numbering**->**User Settings**->**Parallel Ringing**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Internal Number	Select the internal number for which the parallel call performance feature is to be set up.
External Number	Under **New Number** enter the external telephone number to which a call should be signalled in parallel. If a mobile number and a call number are configured for personal use under **Users**->**Basic Settings**->**External Numbers**, these are displayed in **Configured Home Number** or **Configured Mobile Number**

Field	Description
	and can be selected.
Parallel Ringing	Select whether this parallel call entry is to be enabled.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.

10.3 Groups &Teams

In this menu, you configure your system's teams.

10.3.1 Teams

In the **Numbering**->**Groups &Teams**->**Teams** menu, you configure you system's teams.

Teams are groups of people working together to realise an objective. In practice, this means that all people within a team can be reached under the same subscriber number for external and internal calls. In the PABX, each team of telephones/terminals can thus be assigned a specific subscriber number to guarantee accessibility to internal and external calls. Individual structures of companies can be mapped by teams. Thus departments such as Service, Sales or Development can be called from inside or outside in a selective manner via team numbers. Within a team, the call can, for example, be signalled simultaneously to all, or first to one telephone, then also to a second, etc. In one team, answering machines or voice systems can also be used.

Four team call options are assigned to each team. Switching between call options can occur manually or via one of the calendars.

Only for compact systems: The *Team global* is configured by default.

Choose the ⁄ icon to edit existing entries. Select the **New** button to create a new team.

10.3.1.1 General

In the **Numbering**->**Groups &Teams**->**Teams**->**General** basic conditions in the team are configured. Among these are the team name and the internal team number.

For internal team calls, a team number and team name can be assigned to the team in the configuration. If a team number is dialled, the caller sees the team name until a team subscriber accepts the call. The name of the team subscriber is then displayed.

The **Numbering**->**Groups &Teams**->**Teams**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the team.
Internal Number	Enter the internal number of the team.

Fields in the Further Settings menu.

Field	Description
Switch call signalling	Define whether the call option configured for the team shall be enabled manually over the telephone, or via the calendar. For this, calendar and switching times must first have been configured. You can create up to four call variants for each team in the menu **Numbering**->**Groups &Teams**->**Teams**->**New**->**Variant1-4** . Possible values: • *No calendar,only manually* (default value): Manual switch is enabled. • *<Calendar>*: Select one of the configured calendars.
Active Variant (Day)	Select one of the call options to be currently enabled. If a switch is set up via the calendar, this setting will be switched back again in a timely manner. The default value is *Signalling Variant 1.*
Permit Call Forwarding	Define whether call forwarding may occur for the team. The function is activated by selecting *Enabled*. The function is disabled by default.
Call Forwarding to External Numbers	Define whether there shall be call forwarding within the system itself (**Through PABX**, default value) or via an exchange (provider, **Through Exchange Office**). Please note that for call forwarding within the system two external connections are used.

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

Fields in the Timer menu.

Field	Description
Team Speed Timer	Here, enter the **Team Speed Timer** following which call for-warding after time shall be performed in the team. The default value is *15* seconds.
Simultaneous after time	With linear and rotating team calls, there is the option for all team subscribers to be simultaneously called after a defined period. The default value is *60* seconds.
Wrap-up Timer	This setting is only enabled in **Signalling** *Even Distribu-tion (Longest Free)*. For every subscriber who has ended a call, a **Post processing time** is configured, during which he receives no more calls. Calls received by the subscriber on his number rather than via the team and self-initiated calls are not included in the time cal-culation. The default value is *0* seconds; the range *0... 999* seconds.

10.3.1.2 Variant 1 - 4

In the **Numbering**->**Groups &Teams**->**Teams**->**Variant 1 - 4** you configure a team's four call variants. You can create up to four different call options for each team. For this, assign either an internal or external number to the call option, and define how an incoming call should be signalled within the team.

Internal numbers of a team

Under **Internal Assignment**, select the internal subscribers who are to belong to this team. If you wish to temporarily exclude a team subscribers from call signalling (e. g. team sub-scriber is on holiday), you can **Logout** the subscriber. Team calls are not signalled to logged out subscribers. Every team subscriber can also control login and logout himself via a system code.

For internal team calls, a team number and team name can be assigned to the team in the configuration. If a team number is dialled, the caller sees the team name until a team sub-scriber accepts the call. The name of the team subscriber is then displayed. A call to a team can be simultaneous, linear, rotating, setting up or parallel after time. With linear and rotating team calls, there is the option for all team subscribers to be simultaneously called after a defined period (1 - 99).

The **Numbering**->**Groups &Teams**->**Teams**->**Variant** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Assignment	You can assign several internal numbers to each team, or an external number to each. Define whether calls for a team shall be signalled to internal or external subscribers. Possible values: • *External*: The entered external number is called. • *Internal* (default value): The subscribers assigned to the selected number are called according to the defined signalling.
Internal Assignment	Only if **Assignment** = *Internal* Select the internal team subscribers. With **Add**, you add more internal numbers. Only for compact systems: The numbers *10*, *20*, *21*, *22* are assigned to the *Team global*.
External Assignment	Only if **Assignment** = *External* Enter the number of the external subscriber.
Route and Charge Assignment	Only if **Assignment** = *External* Charges for the call and assignment of an external connection occur via the selected internal subscriber.

Automatic call acceptance in the team

You want a caller to be accepted already at call signalling and not to hear the ringing tone. That's no problem if you're using automatic call acceptance for team calls. In this case, the caller is automatically accepted by the system and hears an announcement or system music-on-hold. During this time, the call is signalled to the entered team subscribers. If a subscriber takes the call, the connection to the caller is established.

If a team is called, it can be defined in configuration that the call is automatically accepted, and that the caller hears an announcement or music. The target subscriber(s) are called

during this time. After the receiver is picked up, the announcement or music is turned off and the subscribers are connected to each other.

Possible settings for automatic call acceptance:

- *Simultaneous*: All assigned terminals are called simultaneously. If a terminal is busy, call waiting can be used.

- *Linear*: All assigned terminals are called in the sequence of their entry in configuration. If a terminal is engaged, the next free terminal is called. The call is signalled ca. 15 seconds per subscriber. This period can be set between 1 and 99 seconds (per team) in the configuration. If subscribers are on the phone or logged out, there is not forwarding time for these.

- *Rotating*: This call is a special case of the linear call. After all terminals are called, call signalling begins again with the first entered terminal. The call is signaled until the caller replaces the receiver or the call is ended by the exchange (after ca. 2 minutes).

- *Adding*: The terminals are called in the order of their entry in the subscriber list. Every terminal that has already been called is called again, until all entered terminals are called.

- *Linear,Simultaneous after time* or *Rotating,Simultaneous after time*: Rotating or linear is set for the team call. After defined times have run out, all team sub-scribers can be called in parallel (simultaneously). Example: A precondition is that the sum of forwarding times is larger than the time **parallel after time**. There are 4 sub-scribers to a team. The forwarding time for each subscriber is 10 seconds, 40 seconds in total. The time **parallel after time** is set to 38 seconds. Every subscriber will be called. If a subscriber logs out of the team or is engaged, forwarding time is only 30 seconds, after which the **parallel after time** call is no longer made.

- *Even Distribution (Longest Free)*: Even distribution corresponds to **SignallingRotating** and insures that all team subscribers receive the same number of calls. For every subscriber who has ended a call, a **Wrap-up Time** (0...999 seconds) is set up for the team/subscriber, during which she receives no more calls. Calls received by the subscriber on his number rather than via the team and self-initiated calls are not included in the even distribution calculation. Even distribution begins with the subscriber who hasn't received calls for the longest time, on restart with the first subscriber entered in the subscriber list. A subscriber who has logged out of the team (code number or func-tion key) is no longer taken into account for the even distribution. After a system power failure, the existing **Even distribution** calculation is deleted and the process begins again. If all team subscribers are in **Post processing time**, external calls are routed to the preset redirect destination; internal calls hear the busy tone. If the same time since the last call is calculated for several team subscribers, the sequence of entries in **Internal Assignement** applies.

Fields in the Options menu.

Field	Description
Signalling	You can call team subscribers with a broadcast call. Possible values: • *Simultaneous* (default value) • *Linear* • *Rotating* • *Adding* • *Linear,Simultaneous after time* • *Rotating,Simultaneous after time* • *Even Distribution (Longest Free)*
Busy on busy	Select whether the performance feature "Busy on Busy" is to be enabled for this call option. If a team subscriber is currently engaged, you can decide whether additional calls for this team should be signalled. If "Busy on Busy" is set for a team, other callers are signalled as "engaged". The function is activated by selecting *Enabled*. The function is disabled by default.
Automatic Call Pick-up with	Select whether an incoming call should be automatically accepted, and the caller hear the desired music-on-hold or announcement. Signalling of the call to the team proceeds. The caller bears the costs for the existing connection. The function is activated by selecting *Enabled*. The function is disabled by default. Also select the desired music-on-hold or announcement. Possible values: • *<File_x>* • *MOH Intern 1* • *MOH Intern 2* • *MoH Wave 1 to 8*

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

Fields in the Rerouting Functions menu.

Field	Description
Rerouting on no re-sponse	Select whether and, if so, to which team an incoming call should be redirected on no reply. Possible values: • *None* (default value) • *<Team>* Also enter the time after which the call should be redirected.
Further Rerouting	Select whether and, if so, to which redirect option an incoming call shall be switched. Possible values: • *Off* (default value): No other redirect options are used. • *Immediately*: The incoming call is immediately rerouted to the redirect function selected in **Immediately**. • *On Busy*: The incoming call is rerouted to the redirect function selected in **On Busy**.
Immediately	Only if **Further Rerouting** = *Immediately* Select the redirect function for immediate redirect. Configure re-direct functions in **Applications**->**Rerouting**->**Rerouting Func-tions**.
On Busy	Only if **Further Rerouting** = *On Busy* Select the redirect function for redirect on engaged. Configure redirect functions in **Applications**->**Rerouting**->**Rerouting Functions**.
Busy starting with	Only if **Further Rerouting** = *On Busy* Select from which number of subscribers the team is considered engaged.

10.3.1.3 Log on / Log off

In the **Numbering**->**Groups &Teams**->**Teams**->**Log on / Log off** individual team members are logged in or out.

The **Numbering**->**Groups &Teams**->**Teams**->**Log on / Log off** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Numbers	Indicates the internal number of assigned team members.
Status	Select whether the team member is logged into the team.
	The team member is logged in by selecting *Logged on*.
	Only for compact systems: All team members are *Logged on* by default..

10.4 Call Distribution

In this menu, you configure internal forwarding of all incoming calls.

10.4.1 Incoming Distribution

In the **Numbering**->**Call Distribution**->**Incoming Distribution** menu, you configure the assignment of incoming calls to the desired internal numbers..

In Call Assignment, you assign the call numbers entered under **External Numbers**, e.g. to the teams or to an internal number.

10.4.1.1 Edit

Choose the ✎ icon to edit existing entries.

The **Numbering**->**Call Distribution**->**Incoming Distribution**-> ✎ menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
<Name of Number-Entry>	Displays the number configured.
Trunk	Displays the external connection for which call assignment is configured.
Assignment	Select the internal number or the desired function to which incoming calls shall be assigned via the line selected in **Trunk**. Possible values: • *Internal Number* (default value): The internal team number is selected for assignment to a team. • *Call Through* • *Redirect application* • *Phone Remote Access* • *ISDN Login* • *Mini Call Center*

Fields in the Internal Number and Rerouting Settings menu.

Field	Description
Internal Number	Only for **Assignment** = *Internal Number* Select the internal number to which incoming calls shall be assigned via the line selected in **Trunk**.
Rerouting Application	Only for **Assignment** = *Rerouting Application* Select the desired redirect application to be assigned to the number. You can configure redirect applications in the **Applications**->**Rerouting**->**Rerouting Applications** menu.
Active Variant (Day)	Only for redirect application = *<configured redirect application>* Select the redirect application variant to be currently enabled. If a variant switch is set up via the calendar, this setting will be switched back again at the appropriate time. Possible values:

Field	Description
	• *Variant 1*
	• *Variant 2*
	• *Variant 3*
	• *Variant 4*

Fields in the Call Through Settings menu.

Field	Description
Authorization	Only for **Assignment** = *Call Through*
	Define the authorisation for which the Call Through function shall be released.
	Possible values:
	• *Number screening*: Dialling release occurs after matching the entered number with the entry in the system phone book or with the user's call number entries (**Mobile Number** and **Home Number**).
	• *Number screening and PIN*: Dialling release occurs after matching the entered number with the entry in the system phone book or with the user's call number entries (**Mobile Number** and **Home Number**) AND PIN entry.
	• *PIN*: Dialling release occurs after PIN entry.
	• *Number screening or PIN*: Dialling release occurs after matching the entered number with the entry in the system phone book or with the user's call number entries (**Mobile Number** and **Home Number**) OR PIN entry.
PIN (6 Digit Numeric)	Only for **Authorization** = *Number screening and PIN*, *PIN*, *Number screening or PIN*
	The system checks the caller's authorisation for Call Through, then activates a simulated external dialling tone for the call. Authorisation is granted if the caller has entered the correct 6-digit PIN.
Internal Number and Rerouting Settings	Select the internal subscriber via which Call Through is to occur. One of the system's telephone numbers is defined in the configuration for Call Through. An external caller using this telephone number first hears the system's attention tone.

10.4.2 Misdial Routing

In the menu **Numbering**->**Call Distribution**->**Misdial Routing** for every external connection, you define the subscriber or the team to which the call shall go in any of the following cases:

- an incoming call has a wrong or truncated number / extension
- all members of the called team or call center are logged off.
- all members of the called c all center are in post-processing.

Only for compact systems: A predefined entry with the parameters **Trunk** = *ISDN Extern* and **Rerouting to Number** = *40 (Team global)* is displayed.

10.4.2.1 Edit

Choose the ⟋ icon to edit existing entries.

The **Numbering**->**Call Distribution**->**Misdial Routing**-> ⟋ menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Trunk	Displays the external connection for which redirect for wrong dialling is configured.
Rerouting to Number	Select the type of rerouting: • *None*: No redirect here, the caller gets a busy tone. • *Global Settings*: Redirect occurs as entered in **System Management**->**Global Settings**->**System**->**Rerouting to Number**. • *<Internal number of a user or team>*: The call is redirected to this user or team.

10.4.3 Caller number distribution

This menu allows you to specify to which internal number an incoming call is distributed to in dependence from the caller's number. This function can also be used as a blacklist when incoming calls from specific numbers are distributed neither to an internal number nor to an announcement. These calls are rejected.

10.4.3.1 Edit or New

Select the ✎ button in order to edit exiting entries, or select the **New** button to add further caller numbers.

The menu **Numbering**->**Call Distribution**->**Caller number distribution**->**New** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Caller Number	Specify the caller's number whose calls are to be distributed to a specific internal number. Possible applications are: • complete numbers (0911987654) • area codes (0911) • country codes (001) • prefixes of special numbers (0137) . Numbers from your own public network have to be specified with their area code, the local country code is ignored. **Note** Any incoming number is matched against the specified number starting with the first digit and without considering any possible groups of digits. A single *0*, therefore, matches **all** calls coming in with a leading *0*. This means that a digit sequence matches the more calls the shorter it is. If you select the option *anonymous* instead of specifying a number, all calls are filtered that come in without transmitting a caller number.
Description	Enter a description for the number settings you have just made, e.g., *Family* or *Advertising*.
Assignment	here, you specify how your device is to respond to an incoming call.

Field	Description
	Possible choices: • *None*: The incoming call is not distributed, at all, and is refused. • *Internal Number*: The call is distributed to an internal number. If you choose this option, another card **(Assignment)** is displayed that allows you to choose from the available internal numbers. • *Announcement*: The caller is played an announcement. You can choose from the available announcements in the card **Assignment**.

☞ **Note**

If you want to assign more than one internal number to an incoming number, create multiple entries for the same incoming number.

Chapter 11   Terminals

11.1   elmeg System Phones

In this menu, you perform the assignment of configured internal numbers to the terminals and manage additional functions depending on the type of terminal.

The system telephone end devices (or DECT bases, respectively) are listed alphabetically in the **Description** column. Click the column title of any other column to sort entries in ascending or descending order.

Connected telephones or DECT bases are automatically recognized and listed in the respective summary; they can, however, also be manually configured before being connected to the system.

11.1.1   System Phone

A list of system telephones is displayed in the **Terminals**->**elmeg System Phones**->**System Phone** menu; it shows manually configured telephones as well as automatically detected ones.

The basic configuration is the same for all telephones, but there are differences in the scope of service and configuration of several features (depending on the telephone type). If you cannot use a specific feature with the selected telephone, it is not offered for configuration.

Depending on its type, you can connect the system telephone to the internal ISDN, S0, UP0 or Ethernet port. The system telephone offers typical system features in connection with the PABX system. For example:

• Dialling from the system phone book

• Announcement and simplex operation with other system telephones on the system

• Function keys for control of system features (enable call options, login/logout in teams, line keys, connection keys). The status of a feature can be indicated via LED's assigned to individual function keys.

• Access to the system menu of the system. In this menu, advanced functions are offered by the PABX system.

Choose the ✎ icon to edit existing entries.

As soon as a **Description** is entered for the system telephone and an entry is selected in

the **Internal Numbers** field and copied with **OK**, the entry for that device is moved to the upper part of the overview. To continue configuration, click the ✏ symbol again.

Choose the ⧴ icon to copy existing entries. Copying an entry can prove useful if you wish to create an entry only distinguished by a few parameters from an existing entry. In this case, you copy the entry and modify the desired parameters.

Select the **New** button to create a new system telephone entry.

Note

Configuration modifications are transmitted to the system telephones at the earliest 30 seconds after confirming the modification with the **Apply** button.

11.1.1.1 General

In the **Terminals**->**elmeg System Phones**->**System Phone**->**General** menu, you perform basic settings for a system telephone.

Telephone type

Various types of telephones can be configured.

If the system telephones are first configured in the system with type and serial number, the system detects the system telephone after hook up to the connection. Then the configuration created for this system telephone is transmitted by the system to the system telephone.

Alternatively, you can create a system telephone in your PABX system, select the appropriate telephone type, and assign an MSN. If you connect a telephone with default settings to your PABX system, the telephone answers with the question for the language and the first MSN. When you enter the language into the system telephone, and the MSN that you have configured in the PABX system, the PABX system sends the configuration to the telephone.

If the system telephone is removed, the system detects this and identifies the entry into the system with a red arrow. If another system telephone of the same type is subsequently connected, the system detects this and assigns the detected system telephone the corresponding configuration. The system telephone thus receives the same configuration as its predecessor, despite a different serial number. Only the first MSN must be identically entered in the system telephone and the system.

The **Terminals**->**elmeg System Phones**->**System Phone**->**General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the telephone in the system, enter a description for the telephone.
Phone Type	Displays the type of the connected telephone. If the interface is configured, the system automatically reads out the type. The field can then no longer be edited if a telephone is connected.
	Possible values:
	• *ISDN / Upn*
	• *IP*
	For **Phone Type** = *ISDN / Upn* : Displays the system telephone product description, if it is supported by your device.
	Possible values:
	• *CS290*
	• *CS290-U*
	• *CS400xt*
	• *CS410*
	• *CS410-U*
	• *S530*
	• *S560*
	For **Phone Type** = *IP* : Displays system telephone product description.
	Possible values:
	• *IP-S290*
	• *IP-S290plus*
	• *IP-S400*
Location	Only for **Phone Type** = *IP*
	Select the location of the telephone. You define location in the **VoIP**->**Settings**->**Locations** menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selec-

Field	Description
	tion. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the subscriber is nevertheless registered. • *Not defined (No Registration)*: No location is defined. According to set default behaviour, the subscriber is not registered. • *Not defined (Registration for Private Networks Only)*: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • *<Location>*: A defined location is selected. The subscriber is only registered if at this location.
Interface	Only for **Phone Type** = *ISDN / Upn* Displays the interface to which the terminal is connected. If the interface is configured, the system automatically reads out the type. The field can then no longer be edited if a telephone is connected. Possible values: • *None* • *<interface designation>*
Serial Number	Displays the serial number of the device. If the interface is configured, the system automatically reads out the serial number. This field cannot be subsequently edited.

Fields in the menu Number Settings

Field	Description
Internal Numbers	Select the internal number for this terminal You can assign internal numbers for 10 MSN's. By default, up to 3 MSN's can be assigned for system telephones Up to 3 MSN's are available for terminals in the 290 series. Up to five MSN's are available for terminals in the S5x0 series. Up to 10 MSN's are available for terminals in the CS400 and 4xx series

Field	Description
	Please note that for proper operation of the telephone, at least the first MSN must be entered in the system. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *No number selected*: No internal number shall be assigned to this MSN. • *<Internal Number>*: Select one of the existing numbers of the configured users.

Key extensions

The T400 key extension (available for CS4xx series telephones and for IP-S400) features 20 keys with LED's usable as function keys on two levels. The LED's are assigned to the first key level. Two other LEDs are used to display additional information. You can connect up to 3 key extensions in sequence (cascading) to your telephone. A plug power supply unit must be used if using more than two key extensions.

The T400 /2 key extension (available for CS4xx series telephones and for IP-S400) features 10 keys with LED's usable as function keys on two levels. The LED's are assigned to the first key level. Two other LEDs are used to display additional information.

The T500 key extension (available for CS530 and S560 telephones) features 30 keys that can be used as function keys on two levels. To the right of each key, two LED's indicate which level is active. You can connect up to 3 key extensions in sequence (cascading) to your telephone. A plug power supply unit is required from the first key extensions.

Fields in the menu Extensions

Field	Description
Key Extension Module 1 - 3	Displays whether you're operating the system telephone with a key extension module. Possible values (each according to **Phone Type**): • *Not available* • *T400* • *T400/2* • *T500*

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

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the codec profile to be used if the connection is over a VoIP line. Codec profiles are configured in the **VoIP**->**Settings**->**Codec Profiles** menu.

Fields in the menu Further Settings

Field	Description
Emergency Phone	The system telephones of your system can be set up as emergency telephones. You can immediately begin dialling externally, whether any external connections are active or not. If all external connections are already in use, one of the active calls is terminated and the connection is used for the emergency call. If an emergency call is already being made, it is not interrupted. You can use this performance feature regardless of the performance feature priority for emergency calls. The function is activated by selecting *Enabled*. The function is disabled by default.

11.1.1.2 Settings

In the **Terminals**->**elmeg System Phones**->**System Phone**->**Settings** you can release specific performance features and functions for this system telephone.

The **Terminals**->**elmeg System Phones**->**System Phone**->**Settings** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Display Language	Select the display language for your telephone. Possibe values: • *Deutsch* • *Dutch* : Not for **S530** and **S560** • *English* • *Italian*

Field	Description
	• *Danish*: Not for **S530** and **S560**
	• *Spanish*: Not for **S530** and **S560**
	• *Swedish*: Not for **S530** and **S560**
	• *French*: Not for **S530** and **S560**
	• *Portugues*: Not for **S530** and **S560**
	• *Česko*: Not for **S530** and **S560**
	• *Norwegian*: Not for **S530** and **S560**
	• *Greek*: Not for **S530** , **S560** , **CS290** , **CS290-U** , **IP-S290** , **IP-S290plus**
	• *Icelandic*: Not for **S530** , **S560** , **CS400**, **CS410** , **CS410-U** , **IP-S400**
	• *Polish*: Not for **S530** and **S560**
	• *Hungarian*: Not for **S530** and **S560**
	• *Russian*: Not for **S530** , **S560** , **CS290** , **CS290-U** , **IP-S290** , **IP-S290plus**
Headset Support	Not for **S530** and **S560**. Select whether the headset should automatically accept calls.

> **Note**
>
> If you wish to use a headset, you must configure a headset key and a key for automatic call acceptance on your PABX system. On the system telephone, you must select a headset type and enable the key for automatic call acceptance.

Field	Description
Call Waiting	Select whether another call shall be supported for this telephone through call waiting or a display notification. The function is activated by selecting *Enabled*. The function is disabled by default. If **Call Waiting** is enabled, define for which calls you wish to allow call waiting. Possible values:

Field	Description
	• *Internal Calls* • *External Calls* • *Internal and External Calls* Under **Call Waiting Signal repeated** also decide whether the call waiting tone or the display notification should only be signalled once, or repeated for the call duration.
Do not Disturb (DND)	Only for telephones in the **CS4xx** series, the **S530** telephones and **S560** and the **IP-S400** telephone. For the **S530** and **S560** telephones, you merely configure the function here. With these telephones, enable *Do not Disturb* via the function key. Select whether you wish to use the call protection (do not disturb) performance feature. With this performance feature, you can enable call signalling to your terminal. Select for which number you wish to use the station guarding performance feature. Possible values: • *First Number only* (**CS4xx** series only): Call protection applies only to the first configured MSN. • *All Numbers* (**CS4xx** series only): Call protection applies to all configured MSN's. Select whether incoming calls shall be signalled: • *Off*: Calls are signalled. • *On* (**CS4xx** series only): Calls are not signalled. • *Acknowledgement Tone only* (**CS4xx** series only): An attention tone is heard once for a call • *Attention tone 1* (only **S530** and **S560**) • *Attention tone 2* (only **S530** and **S560**) • *Attention tone 3* (only **S530** and **S560**) • *Attention tone 4* (only **S530** and **S560**) • *No attention tone* (only **S530** and **S560**)

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

Fields in the menu Advanced Settings

Field	Description
Status LED	Select whether and, if so, which events should be signalled by the system telephone status LED. Possible values: • *Off*: The status LED function is not used. • *Caller List*: The status LED signals calls and new messages. • *Messages only*: The status LED only signals new messages (MWI). • *New Message* (**nur S5x0**) • *New Call* (**nur S5x0**) • *Active Call* (**nur S5x0**) You can use *New Message New Call* the options , *Active Call* and individually, or combine them freely.
Directory Softkey	Only for telephones in the **CS4xx** series Select whether calls shall be made with the softkey entries from the system phone book (*System*) or from the telephone phone book (*Telephone*).
Conversation Display	Not for **S5x0** Select which information shall be indicated in the system telephone display during a call. Possible values: • *Number and Charge or Duration* • *Number and Charge* • *Number and Duration* • *Number and Time* • *Number only* • *Date and Time only*
Default Signalling dur-	Select whether DTMF signals or keypad functions shall be

Field	Description
ing Calls	transmitted into the system in call status. You can use special functions during a call by entering character and numerical sequences. These entries must be made as keypad or MFV sequences, depending on the function to be used. You can define whether MFV or keypad functions are possible in the basic setting during a call. Possible values: • *DTMF* (default value) • *Keypad*
Automatic Call Pick-up	Select the period after which calls to this system telephone should be automatically accepted without you having to pick up the receiver or press the loudspeaker key. ☞ **Note** Please note that to be able to use this function at least one telephone key must be assigned to automatic call acceptance. Only for **S5x0** You switch on automatic call acceptance with *Enabled*. You can configure the corresponding duration in the **Terminals**->**elmeg System Phones**->**System Phone**->**New**->**Keys** menu. Only for **x290xx** = and **x4x0xx**. Possible values: • *Immediately* • *After 5 seconds* • *After 10 seconds*
Mute after hands-free Calling	Not for **S5x0**, **CS290**, **CS290-U** You can dial the number of a subscriber without picking up the receiver (e. g. hands-free). Here, you have the choice of whether the built-in microphone shall be switched on immediately or only after pressing of the corresponding softkey. If the micro-

Field	Description
	phone is turned off during dialling, the corresponding softkey must be pressed, even if the connection is already active. The function is activated by selecting *Enabled*. The function is disabled by default.
Receiving UUS	Select whether performance feature UUS (User to User Signalling) can be used for this telephone. With this performance feature, you can receive short text messages from other telephones. In this way, you can send written information within the system, e. g. *Meeting at 9:30 AM* or *Am on holiday until Monday*. Possible values: • *Off, UUS are blocked*:The UUS performance feature is not used. • *Internal only*: Text messages can only be received internally. • *External only*: Text messages can only be received externally. • *Internal and External* (default value): Text messages can only be received internally and externally.
Receive System Intercom Call	Only visible when a **Number / User**is selected in the **Terminals**->**elmeg System Phones**->**System Phone**->**General** menu under **Internal Numbers**. Select whether the **Receive System Intercom Call** function should be allowed. The function is disabled by default.
Receive Announcement Calls	Only visible when a **Number / User**is selected in the **Terminals**->**elmeg System Phones**->**System Phone**->**General** menu under **Internal Numbers**. Select whether the **Receive Announcement Calls** function should be allowed. The function is disabled by default.

11.1.1.3 Keys / T400 / T400/2 / T500

The menu **Terminals**->**elmeg System Phones**->**System Phone**->**Keys** displays the configuration of your system telephone's keys.

Your telephone features several function keys to which you can assign various functions on two levels The functions that can be programmed on the keys vary from telephone to telephone.

Every function key with automatic LED functions (e. g. connection keys, line keys) can only be programmed once per system (telephone and key extensions).

Values in the list Keys

Field	Description
Key	Displays the name of the key.
Label Description	Displays the configured key name. This appears on the labelling page (label strips).
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

Print allows you to print out a label sheet for the description field of your system phone or key extension.

Edit

Choose the ✎ icon to edit existing entries. In the pop-up menu, you configure the functions of your system telephone keys.

You can use the following functions with system telephones:

- *MSN Selection Key*: You can perform an internal or external call so that your system telephone transmits a specific number (MSN) to the caller. This number (MSN) has to be configured on your system telephone. If the LED is active, there is an active connection via this key.
- *Dial Key (Standard)*: You can store a number on each function key. External numbers have to be prefixed by the exchange code *0* if *no automatic outside line* has been configured for your **Class of Service** on the telephone.
- *Dial Key (DTMF)*: You can store a DTMF sequence on every function key.

- *Dial Key (Keypad sequence)*: You can store a keypad sequence on every function key.

- *Extension Key (User)*: You can set up dialling to an internal extension using a line key. After pressing the corresponding key, hands free is switched on and the internal extension entered is selected. If a call is signalled on the internal extension you have entered, you can pick this up by pressing the line key.

- *Extension Key (Team)*: You can set up dialling to a team using a line key. After pressing the corresponding key, hands-free is activated and the entered team is called according to its enabled call option. If a call is signalled for the entered team, you can pick it up by pressing this connection key.

- *Trunk Line*: An ISDN connection or a VoIP provider is set up under a connection key. If this key is pressed, automatic hands-free is enabled and the corresponding ISDN connection is assigned. You then hear the external dialling tone. If an external call is signalled on another internal telephone, you can pick it up by pressing this line key.

- *System Call (Announcement User)*: You can set up a connection to another telephone without this connection having to be actively accepted. As soon as the telephone has accepted the announcement, the connection is established and the announcement key LED is enabled. The announcement can be ended by renewed pressing of the announcement key or by pressing the loudspeaker key. The LED switches off again at conclusion of the announcement.

- *System Call (Announcement Team)*: You can configure an announcement for a team by setting up a function key. The way this works is the same as that described above.

- *Login / Log Out, Team*: If you are entered as a subscriber in the call assignments for one or more teams, you can set up a key so that you can control the call signalling of your telephone. If you're logged in, team calls are signalled to your telephone. If you are logged out, no team calls will be signalled.

  The call numbers entered in the telephone can be logged in/logged out from a team using a set function key (**MSN**-1...**MSN**-9). Before entering a team number, you must select the telephone call number index (MSN) that is entered in the corresponding team call assignments.

- *System Call (Announcement enable)*: You can also selectively deny or allow announcements using a function key. To use announcements, you must be authorised for the corresponding authorisation class.

- *Receive Intercom Calls*: You can set up a key is such a way that a connection to the specified telephone is established without this connection having to be actively accepted.

- *System Call (Intercom enable)*: You can set up a key in such a way that the simplex operation function is allowed or denied. To use simplex operation, the function must be allowed in the corresponding authorisation class.

- *Boss Key* / *Secretary Key*: You can set up a key as a special line key. The Boss telephone and Secretary telephone properties are saved in both telephones with these keys.

- *Diversion Secretary*: You can set up a key in such a way that incoming calls to the Boss telephone are automatically routed to the Secretary telephone.

- *Call Forwarding (CFNR)*: You can set up a key so that delayed call diversion is configured for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.

- *Call Forwarding (CFU)*: You can set up a key so that immediate call diversion is configured for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.

- *Call Forwarding (CFB)*: You can set up a key so that call diversion on engaged is configured for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.

- *Macro Function*: You can configure a key so that by pressing it a saved macro is executed.

  The macro function can only be programmed at the phone.

- *Headset Control* (not with the **S5x0**): If you've connected and configured a headset to your telephone over a separate headset socket, operation of the headset occurs over a function key. Press the headset key to initiate or accept calls. If you already have an active connection over the headset, you can end the call by pressing the headset key.

- *Automatic Call Pick-up*: Your telephone can accept calls automatically without you having to lift the receiver or press the loudspeaker key. Automatic call acceptance is switched on or off using the function key assigned. You can configure a separate function key for each number ("MSN-1"..."MSN-9"), or a function key for all numbers. The period after which calls are automatically accepted is configured once for all numbers of the telephone.

- *Trunk Group Access*: Several external ISDN (if supported by you device) or IP connections to bundles can be grouped in the system. With a bundle key, you can save these connections on a function key. If this key is pressed, automatic hands-free is enabled and a free B channel of the corresponding bundle is assigned. You then hear the external dialling tone.

- *Connection Key* (not with the **S5x0**): In addition to the softkeys "Connection 1..", function keys can be configured on the system telephone or the extension for operation while brokering. At least two connection keys must be configured.

- *Hotel Rooms*: You can assign a key in such a way that when pressed, the guest is checked in or out (first level), or the selected hotel room phone is called (second level). You must configure this key on the first level, then the connected key on the second level is automatically assigned and, as the case applies, its content overwritten.

- *System Parking (Open Enquiry)*: The called party is put on hold for enquiry and dials a code. The telephone is now freed for other operations, e. g. announcements. Another party can accept the call, if he lifts the receiver and dials the relevant code of the held call. The codes assigned by the PABX can also be entered in the function keys of one or more system telephones. If a call is set to open hold for enquiry by pressing the function key, this is indicated by flashing LEDs on the function keys for the system telephones set up for this. The call is transferred by pressing the corresponding function key. This performance feature is only possible if only one call is on hold.

- *Agent wrap-up Time*: You can configure a key so that when it is pressed, an agent's post-processing time is switched on or off at a team call centre (first level), or extended (second level).

- *Night Mode*: You can configure a key so that by pressing it night operation is switched on or off.

Note

To manually switch night operation off again, the authorisation class **Switch signalling variants manually** must be enabled.

- *Parallel Ringing* (only **S5x0**): If a parallel call to another telephone is configured, both connections will ring when a call comes in. The call is accepted where first picked up.

- *Shift* (only **S5x0**): With this key, you can access second level functions.

- *Do not Disturb* (only **S5x0**): With this key, you enable or disable the Do not Disturb function which you have configured under **Terminals**->**elmeg System Phones**->**System Phone**->**Settings**.

The menu **Terminals**->**elmeg System Phones**->**System Phone**->**Keys**->**Edit** consists of the following fields:

Fields in the menu Telephone

Field	Description
Key name	Enter a name for the key to be used as text for the corresponding key when the ID labels are printed.

Field	Description
Key Type	Depending on the model, the telephones feature from 5 to 15 keys on which functions may be assigned over two levels. You can reach the second layer of function keys by pressing the keys twice. This must be done quickly. With S5x0 devices, you can alternately use the *Shift* function key. With the optional key extensions, you have access to additional twice-assignable function keys.
	Possible values:
	• *Dial Key (Standard)*
	• *Dial Key (Standard)*
	• *Dial Key (DTMF)*
	• *Dial Key (Keypad sequence)*
	• *Extension Key (User)*
	• *Extension Key (Team)*
	• *Trunk Line*
	• *System Call (Announcement User)*
	• *System Call (Announcement Team)*
	• *Login / Log Out, Team*
	• *System Call (Announcement enable)*
	• *Receive Intercom Calls*
	• *System Call (Intercom enable)*
	• *Boss Key*
	• *Secretary Key*
	• *Diversion Secretary*
	• *Call Forwarding (CFNR)*
	• *Call Forwarding (CFU)*
	• *Call Forwarding (CFB)*
	• *Macro Function*
	• *Headset Control*
	• *Automatic Call Pick-up*
	• *Trunk Group Access*
	• *Connection Key*
	• *Hotel Room*

Field	Description
	• *System Parking* • *Agent wrap-up Time* • *Night Mode* • *Shift key* (**S5x0** only) • *Parallel call* (only **S5x0**) • *Station guarding (quiet)* (**S5x0** only)
Number	Only where **Key Type** = *Dial Key (Standard)*, *Dial Key (DTMF)* and *Dial Key (Keypad sequence)* You can save a number, an MFV sequence or a keypad sequence on every function key. Enter the call number or the code for the DTMF/keypad sequence.
Internal Number	For **Key Type** = *Extension Key (User)* Select the internal number of a user to be called when this key is pressed. Where **Key Type** = *System Call (Announcement User)* Select the internal number of a user on whose telephone an announcement shall be made. For **Key Type** = *Login / Log Out, Team* Select the internal number of a team to be logged into or out of when this key is pressed. For **Key Type** = *Receive Intercom Calls* Select the internal number of a user with which you wish to conduct simplex operations. For **Key Type** = *Call Forwarding (CFNR)*, *Call Forwarding (CFU)*, *Call Forwarding (CFB)* Select the internal number of a telephone MSN from which the indicated destination number can be forwarded For **Key Type** = *Automatic Call Pick-up* Select the internal number of this telephone, on which incoming calls shall be automatically accepted.

Field	Description
	For **Key Type** = *Hotel Room*
	Select the internal number of a hotel guest.
	For **Key Type** = *Agent wrap-up Time*
	Select the internal number of a user whose post-processing time shall be modified at regular intervals when this key is pressed.
	For **Key Type** = *Parallel Ringing*
	Select the internal number of a user whose phone should also ring when a call goes in to you.
	For **Key Type** = *MSN Selection Key*
	Select that number of your telephone you intend to use.
Automatic Call Pick-up	For **Key Type** = *Automatic Call Pick-up*
	Select when a call shall be automatically accepted by the entered internal subscriber.
	Possible values:
	• *Immediately*: The call is immediately and automatically accepted.
	• *After 5 seconds*: The call is automatically accepted after 5 seconds.
	• *After 10 seconds*: The call is automatically accepted after 10 seconds.
	• *After 15 seconds* (only **S5x0**): The call is automatically accepted after 15 seconds.
	• *After 20 seconds* (only **S5x0**): The call is automatically accepted after 20 seconds.
	• *Off* (only **S5x0**): The call is not automatically accepted.
Team	For **Key Type** = *Extension Key (Team)*
	Select the internal number of a team to be called when this key is pressed.
	Where **Key Type** = *System Call (Announcement Team)*

Field	Description
	Select the internal number of a team on whose telephone an announcement shall be made.
	For **Key Type** = *Login / Log Out, Team*
	Select the internal number of a team to be logged in/out when this key is pressed.
Trunk Line	Only where **Key Type** = *Trunk Line*
	Select the external connection over which an external call shall be set up when this key is pressed.
Number of Secretary Phone	Only if **Key Type** = *Boss Key*
	Select the internal number of the secretary telephone. The secretary telephone is called when this key is pressed.
Number of Boss Phone	Only if **Key Type** = *Secretary Key*
	Select the internal number of the Boss telephone. The Boss telephone is called when this key is pressed.
Target Number "On no reply"	Only if **Key Type** = *Call Forwarding (CFNR)*
	Enter the number to which incoming calls shall be forwarded on no reply .
Target Number "Immediate"	Only if **Key Type** = *Call Forwarding (CFU)*
	Enter the number to which incoming calls shall be forwarded immediately.
Target Number "On busy"	Only if **Key Type** = *Call Forwarding (CFB)*
	Enter the number to which incoming calls shall be forwarded on busy.
Trunk Group Access	Only if **Key Type** = *Trunk Group Access*
	Select the bundle via which an outside call shall be set up.
Waiting Queue	Only for **Key Type** = *Open hold*
	Select the queue in which the current call should be held.

Transfer key

Select the $\uparrow_{\downarrow}$ icon to move configured function keys.

Fields in the menu Key

Field	Description
Key name	Displays the name of the key.
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

Fields in the menu Move to

Field	Description
Phone	Select one of the connected telephones.
Module	Select *Telephone* or a key extension.
Key	Select the key to which you wish to transfer the configured function.

11.1.1.4 Device Info

In the **Terminals**->**elmeg System Phones**->**System Phone**->**Device Info** menu, the system data read out of the system telephone are displayed.

Meaning of the list entries

Description	Meaning
Description	Displays the entered description of the telephone.
Phone Type	Displays the type of telephone.
Serial Number	Displays the serial number of the telephone.
Software Version	Displays the current version of the telephone software.
Release Date and Time	Displays the date and time of the telephone software version.

Description	Meaning
Last Device Configuration	Displays the date and time of the last telephone configuration.
Answering Machine	Displays whether an answering machine module is inserted in the telephone (Yes) or not (No).

Meaning of Key Extensions

Description	Meaning
Module 1: Type / Serial Number, **Module 2: Type / Serial Number**, **Module 3: Type / Serial Number**	Displays the type and serial number of the connected key extension.
Module 1: Software Version, **Module 2: Software Version**, **Module 3: Software Version**	Displays the current software version of the connected key extension.

11.1.2 elmeg IP

The **Terminals**->**elmeg System Phones**->**elmeg IP** menu displays a list of IP telephones. The upper part of the overview displays the manually configured, the lower part displays the automatically detected devices. For an automatic discovery we recommend the use of DHCP. (Activate the option *Use this device as DHCPv4 server* in the menu **Assistants**->**First steps**.)

If you want to assign a static IP address, you must enter your PABX system as provisioning server (*http://<IP address of the provisioning server>/ eg_prov*). As soon as a **Description** for the telephone is entered and saved with **OK**, the entry for that device is moved to the upper part of the overview.

Note

Key Extension Modules are not discovered automatically, but must be manually configured using the GUI.

If a configured Key Extension Module is deleted the corresponding function keys are likewise deleted.

Choose the ✎ icon to edit existing entries.

After a short time, the icons 🖬 and ↻ are displayed for this device.

After clicking the **Apply** button it takes several seconds until the changes have been transmitted to the respective IP telephone.

Choose the ≡₊ symbol in order to copy an existing entry. This can be useful if you intend to create an entry that differs only in a few parameters from the already existing entry. In this case, copy the entry and change only the desired paramaters.

Select the 🖬 button to go to the **elmeg IP** telephone user interface administrator page. This is described in the telephone user guide.

Select the **New** button to manually set up a new IP end device.

Employ automatic provisioning in order to have your PABX system transmit basic telephony parameters to the IP telephones. When using the assistent **First steps** activate the option *elmeg IP1x/DECT* for the field **Transmit Provisioning Server for** in the **Assistants**->**First steps**->**Advanced Settings**->**Add** section. Alternatively, you can create a new entry in the menu **Local Services**->**DHCP Server**->**DHCP Configuration**->**New**->**Advanced Settings**->**DHCP Options** and set the fields **Option** = *URL (Provisioning Server)* and **Value** = *http://<IP address of the provisioning server>/eg_prov*.

To register the handsets you first set the base station to login mode. Then you perform the registering of the handsets on the handests themselves. To configure the base station in any more detail, you need to use the DECT system's web configurator.

Select the button ↻ to trigger an update of the device's provisioning. If the update is successful, the updated value displays in the **Last seen** column within 10 seconds.

> **Note**
>
> If you wish to test whether your base station is correctly configured and accessible, select the button ↻ and check whether an updated value is displayed within 10 seconds in the **Last seen** column.

11.1.2.1 General

In the menu **Terminals**->**elmeg System Phones**->**elmeg IP**->**General**, you make the basic settings for an IP telephone.

The **Terminals**->**elmeg System Phones**->**elmeg IP**->**General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the telephone in the system, enter a description for the telephone.
Phone Type	Displays the type of your IP telephone. Possible values: • *elmeg IP120* • *elmeg IP130* • *elmeg IP140* • *elmeg IP620* • *elmeg IP630* • *elmeg IP680*
Location	Select the location of the telephone. You define locations in the **VoIP**->**Settings**->**Locations** menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the subscriber is nevertheless registered. • *Not defined (No Registration)*: No location is defined. According to set default behaviour, the subscriber is not registered. • *Not defined (Registration for Private Networks Only)*: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • *<Location>*: A defined location is selected. The subscriber is only registered if at this location.
MAC Address	Shows the MAC address of the telephone.

Field	Description
IP/MAC Binding	Displays the IP address automatically assigned by DHCP.
	Here you have the option of permanently assigning the displayed IP address to the device with the displayed MAC address.
	This option should be activated to enable quick re-login after a functional fault.

Key extension modules

The key extension module **elmeg T100** (available for **elmeg IP120**, **IP130** und **IP140**) features 14 keys with LEDs, which you can configure as function keys. **elmeg IP120** can be expanded by up to two extension modules, **elmeg IP 130** and **IP140** support up to three cascaded modules. The operation of a thirs extension mosdule requires the connection of a power supply.

Fields n the menu Extensions

Fiekd	Description
Ext. Module No 1 - 3 (depends on **Phone Type**)	Displays if you are operatnig the IP telephone with an key extension module. Only the number of modules supported by the respective phone type is offered for configuration. Possible values: • **Not available** • **Available**

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

Fields in the menu Further Settings

Field	Description
Multiple SIP Connections (Sub-Exchange)	Select whether multilinks shall be allowed from this terminals. Operation as subsystem: Only in case of connection of a subsystem to a system Here, with a disabled performance feature, only a connection via the subscriber SIP registration is possible. If a second call comes in, it is accepted and the existing call is held. With an enabled performance feature, several SIP connections are possible over the same login. If the performance feature is enabled for as system without subsystem, two simultaneous calls on the phone are not connected to each other

Field	Description
	after the receiver is replaced but released, for example. Here, the performance feature should not be set. The function is activated by selecting *Enabled*. The function is disabled by default.
No Hold and Retrieve	The performance features hold a call and retrieve a held call are not available on certain telephones. The function is activated by selecting *Enabled*. The function is disabled by default.

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the Codec profile to be used. Codec profiles are configured in the **VoIP**->**Settings**->**Codec Profiles** menu.
Video	Select if calls between IP telephones are to support the transmission of video data. Video transmission can only be negotiated between the participants if both support this feature.
SRTP	Select if calls via this SIP provider may be secured with SRTP (Secure Real-Time Transport Protocol).

11.1.2.2 Numbers

In the menu **Terminals**->**elmeg System Phones**->**elmeg IP**->**Numbers** you assign an IP telephone up to twelve internal phone numbers using **Add**.

The available internal phone numbers are created under **Numbering**->**User Settings**->**Users**->**New**.

You can delete assigned numbers from the list with ▄ .

Values in the list Number Settings

Field	Description
Connections Nr.	Shows the serial number of the connection.
Internal Number	Displays the assigned internal number.
Displayed Description	Displays the description that will be displayed on the IP tele-

Field	Description
	phone's display.
User	Displays the user's name.

11.1.2.3 Keys / T100

The menu **Terminals**->**elmeg System Phones**->**elmeg IP**->**Keys** displays the configuration of your system telephone's keys.

> **Note**
>
> You can configure the key assigment either through your PABX system or on the telephone itself. We recommend using your PABX system for this, since it overwrites the telephone configuration.
>
> You can avoid the overwriting for individual keys that have already been configured on the telephone by choosing *Not configured* on the PABX system.

Your telephone is equipped with several function keys that allow the assignment of different functions. The functions available for programming are different across different types of telephones.

Values in the list Keys

Field	Description
Key	Displays the name of the key.
Label Description	Displays the configured key name. This appears on the labelling page (label strips).
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

Print allows you to print out a label sheet for the description field of your system phone or key extension.

Edit

Choose the ⟋ icon to edit existing entries. In the pop-up menu, you configure the func-

tions of your system telephone keys.

You can use the following functions with system telephones:

- *Dial Key (Standard)*: You can store a number on each function key. External numbers have to be prefixed by the exchange code *0* if *no automatic outside line* has been configured for your **Class of Service** on the telephone.

- *Dial Key (DTMF)*: You can store a DTMF sequence on every function key.

- *Extension Key (User)*: You can set up dialling to an internal extension using a line key. After pressing the corresponding key, hands free is switched on and the internal extension entered is selected. If a call is signalled on the internal extension you have entered, you can pick this up by pressing the line key.

- *MSN Selection Key*: Assigns a specific connection (i.e. a specific SIP account) to the function key. You can use this key to initiate a call via this connection, or you can accept a call coming in via this connection. The key flashes if a call is received, it is lit if the connection is busy. Select the desired connection. All configured connections are available. Configure SIP accounts exclusively on your PABX system.

- *Call Forwarding (enable)*: Assigns activating or deactivating a call forwarding that has been configured on the telephone. You can only store a single call forwarding on the device; it is applied to all calls.

- *System Parking (Open Enquiry)*: The called extension enters an enquiry and dials a code. The telephone is now open for additional operations like e.g.an announcement. A second subscriber can accept the call by picking up the receiver and dialing the code corresponding to the call. The codes are determined by the PABX, but can also be assigned to the functions keys of one or more system phones. If a call is put into open enquiry by pressing a function key, this is indicated by the flashing of the respective function key LED on all system phones with a corresponding configuration. Pressing the function key accepts the call. This function is only available if a call has been parked.

- *XML-Content* (only for IP140/130): Assigns an URL to the function key. You can, e.g., store customer-specific menus and temporarily show them on the display of your telephone. This function is currently not supported by your PABX system.

- *Next call anonymous*: For the next call the called party will no see your MSN.

- *Menu - Call Forwarding*: Assigns the menu item **Call Forwarding** in the display menu of your telephone to the function key. You can configure the call forwarding specifics.

- *Menu - Resource Directory* (only for IP140/130): Assigns the menu item **MediaPool** in the display menu of your telephone to the function key. You can manage images used as screen saver, caller icons for phone directory entries and ring tones. Moreover, you can monitor the capacity of the pool.

- *Menu - Internet Radio* (only for IP140/130): Assigns the menu item **Internet Radio** in the display menu of your telephone to the function key. You can tune in to the last se-

lected radio station or select a different one. This option has to be activated in the menu of the telephone, too.

- *Macro* (only for IP630): A macro key allows you to define an arbitrary code to be executed when the key is switched on, as well as a code that is executed when the key is switched off again. This, e.g., allows switching a call forwarding inside the phone without having to access the PBX. In the switched-on state the key LED is lit, in the switched-off state it is switched off, too.

> **Note**
>
> The status of the macro key is not synchronized with the configuration of the PBX. If a function is activated through the key which then is disabled again by a timer in the PBX, the function is inactive even though the key LED is still lit.

- *Not configured*: The function key is managed by the telephone itself and not by the PABX system.This options locks the key for the provisioning by your PABX system.

The menu **Terminals**->**elmeg System Phones**->**elmeg IP**->**Keys**->**Edit** consists of the following fields:

Fields in the menu Telephone

Field	Description
Key name	Enter a name for the key to be used as text for the corresponding key when the ID labels are printed.
Key Type	Depending on the model, telephones have seven or 14 keys that can have functions assigned to them. Optional key extension modules extend the number of available functions keys.
	Possible values:
	- *Dial Key (Standard)*
	- *Dial Key (DTMF)*
	- *Extension Key (User)*
	- *MSN Selection Key*
	- *Call Forwarding (enable)*
	- *System Parking*
	- *XML-Content*
	- *Next call anonymous*
	- *Menu - Call Forwarding*
	- *Menu - Resource Directory*

Field	Description
	• *Menu - Internet Radio* • *Not configured*
Internal MSN	Only for **Key Type** = *Dial Key (Standard)*, *Extension Key (User)*, *MSN Selection Key*, *Call Forwarding (enable)* or *System Parking* You can select one of the internal MSNs configured in the menu **Terminals**->**elmeg System Phones**->**elmeg IP**->**Numbers**.
Number	Only for **Key Type** = *Dial Key (Standard)* or *Dial Key (DTMF)* You can save a number or a DTMF sequence to any function kye. Specify the number or the characters for the DTMF sequence.
Internal Number	Only for **Key Type** = *Extension Key (User)* Select the internal number of the subscriber that is to be called when pressing this key.
Pick-Up Code	Only for **Key Type** = *Extension Key (User)* The code that is required for the busy lamp field to allow you picking up a call on an IP telephone when the LED is flashing. The default value is *#0*.
Waiting Queue	Only for **Key Type** = *System Parking (Open Enquiry)* Select the waiting queue to which the currect connection is to be added.
URL	Only for **Key Type** = *XML-Content* For this function you can store the URL to a server which hosts the desired information. This function is currently not supported by your PABX system.

Transfer key

Select the $t_↓$ icon to move configured function keys.

Fields in the menu Key

Field	Description
Key name	Displays the name of the key.
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

Fields in the menu Move to

Field	Description
Phone	Select one of the connected telephones.
Module	Select *Telephone* or a key extension.
Key	Select the key to which you wish to transfer the configured function.

11.1.2.4 Settings

In the **Terminals**->**elmeg System Phones**->**elmeg IP**->**Settings** menu you can reset the telephone's administrator password.

The **Terminals**->**elmeg System Phones**->**elmeg IP**->**Settings** menu consists of the following fields:

Fields in the menu System Phone

Field	Description
Admin Password	Select whether the administrator password should be reset. The function is activated by selecting *Enabled*. The function is disabled by default. As soon as you select the **OK** button, the password is reset to the default setting.
Display Language	Select the display language for your telephone. Possible values:

Field	Description
	• *Deutsch*
	• *Dutch*
	• *English*
	• *Italian*
	• *Spanish*
	• *French*
	• *Portugues*
	• *Česko*
	• *Greek*
	• *Polish*
	• *Romanian*
	• *Slovak*

11.1.3 elmeg DECT

The menu **Terminals**->**elmeg System Phones**->**elmeg DECT** displays the base stations of the connected DECT single-cell and multi-cell systems.

All base stations that are connected are automatically detected and listed in the lower part of the overview. For an automatic discovery we recommend the use of DHCP. (Activate the option *Use this device as DHCPv4 server* in the menu **Assistants**->**First steps**.)

If you want to assign a static IP address, you must enter your PABX system as provisioning server (*http://<IP address of the provisioning server>/ eg_prov*).

As soon as a **Description** for the base station is entered and saved with **OK**, the entry for that device is moved to the upper part of the overview.

After a short time, the icons ⬚ and ⟳ are displayed for this device.

Choose the ✎ icon to edit existing entries.

After clicking the **Apply** button it takes several seconds until the changes have been transmitted to the respective device.

Select the **New** button to manually set up a new base station.

Select the button ⬚ to go to the base station's Web configurator. This is described in the user guide for the relevant DECT system.

In order to be able to use automatic provisioning, click the ✎ icon again and add the re-spectice numbers.

Use automatic provisioning to have your PABX system transfer elementary telephony para-meters to the DECT system. If you want to use the assistant **First Steps** to do this, you ac-tivate the value *elmeg IP1x/DECT* under **Assistants**->**First steps**->**Advanced Settings**->**Add** in the field **Transmit Provisioning Server for** . Alternatively, you can create a new entry in the menu **Local Services**->**DHCP Server**->**DHCP Configuration**->**New**->**Ad-vanced Settings**->**DHCP Options** and set the fields **Option** = *URL (Provisioning Server)* and **Value** = *http://<IP address of the provisioning serv-er>/eg_prov* .

To register the handsets you first set the base station to login mode. Then you perform the registering of the handsets on the handests themselves. To configure the base station in any more detail, you need to use the DECT system's web configurator.

Select the button ↻ to trigger an update of the device's provisioning. If the update is suc-cessful, the updated value displays in the **Last seen** column within 10 seconds.

Note

If you wish to test whether your base station is correctly configured and accessible, se-lect the button ↻ and check whether an updated value is displayed within 10 seconds in the **Last seen** column.

Note

If you wish to change the language currently used with a DECT single-cell system, the system has to be connected to the provisioning server of the PABX. You require an in-stalled SD card (if supported by you device). All languages to be deployed need to be stored on the SD card. Single-cell systems load a required language from the SD card on demand.

11.1.3.1 General

In the menu **Terminals**->**elmeg System Phones**->**elmeg DECT**->**General** you make the basic settings for base stations.

The **Terminals**->**elmeg System Phones**->**elmeg DECT**->**General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the base station in the system, enter a description for the telephone.
Phone Type	Displays the type of base station. Possible values: • *elmeg DECT150* • *elmeg DECT200*
Location	Select the location of the base station. You define locations in the **VoIP**->**Settings**->**Locations** menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the subcriber is nevertheless registered. • *Not defined (No Registration)*: No location is defined. According to set default behaviour, the subscriber is not registered. • *Not defined (Registration for Private Networks Only)*: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • *Location*: A defined location is selected. The subscriber is only registered if at this location.
MAC Address	Shows the MAC address of the base station.
IP/MAC Binding	Displays the IP address automatically assigned by DHCP. Here you have the option of permanently assigning the displayed IP address to the base station with the displayed MAC address. This option should be activated to enable quick re-login after a functional fault.

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

Fields in the menu Further Settings

Field	Description
No Hold and Retrieve	The performance features hold a call and retrieve a held call are not available on certain telephones.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the Codec profile to be used. Codec profiles are configured in the **VoIP**->**Settings**->**Codec Profiles** menu.

11.1.3.2 Numbers

In the menu **Terminals**->**elmeg System Phones**->**elmeg DECT**->**Numbers** you assign **Internal Numbers** to the mobile parts. You can select from the numbers that you have created for this purpose under **Numbering**->**User Settings**->**Users**.

The system automatically assigns a serial number, the **Mobile Number**, to each mobile part so that you can identify the device. You can then use **Add** to assign a **Internal Number** to a mobile part from the list.

You can delete assigned numbers with ![trash] .

Values in the list Numbers

Field	Description
Mobile Number	Displays the serial number of the mobile part. This number is permanently assigned to the mobile part so that it can be uniquely identified.
Internal Number	Displays the assigned internal number.
Displayed Description	Displays the description entered for the internal number. In standby mode this description is shown on the mobile part's display.
User	Displays the user's name.

11.1.3.3 Settings

In the **Terminals**->**elmeg System Phones**->**elmeg DECT**->**Settings** menu you can reset the administrator password for the base station.

The **Terminals**->**elmeg System Phones**->**elmeg DECT**->**Settings** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Admin Password	Select whether the administrator password should be reset.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.
	As soon as you select the **OK** button, the password is reset to the default setting.

11.2 Other phones

In this menu, you perform assignment of configured internal numbers to the terminals and set additional functions according to terminal type.

Terminals of the corresponding category (VoIP, ISDN, or analog) are sorted alphabetically in the **Description** column. Click the column title of any other column to sort entries in ascending or descending order.

11.2.1 VoIP

In the **Terminals**->**Other phones**->**VoIP** menu, you configure the connected VoIP terminals. For example, you perform assignment of a configured internal number.

Specific instructions for configuring VoIP, see *VoIP - Configuration example (a smartphone as an internal VoIP telephone)* on page 224.

11.2.1.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to add VoIP terminals.

The **Terminals**->**Other phones**->**VoIP**->**New** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the IP telephone.
Location	Select the location of the telephone. You define locations in the **VoIP**->**Settings**->**Locations** menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection. Possible values: • *Not defined (Unrestricted Registration)*: No location is defined. According to set default behaviour, the subscriber is nevertheless registered. • *Not defined (No Registration)*: No location is defined. According to set default behaviour, the subscriber is not registered. • *Not defined (Registration for Private Networks Only)*: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • *<Location>*: A defined location is selected. The subscriber is only registered if at this location.

Fields in the menu Number Settings

Field	Description
Internal Numbers	Select the internal number for this terminal You can define several internal numbers. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

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

Fields in the menu SIP Client Settings

Field	Description
SIP Client Mode	Select whether a *dynamic* SIP client or a *static* SIP client is to be used. Possible values: • *Dynamic* (default value): Your device (e. g. a standard SIP telephone) runs a SIP registration to tell the system its (dynamic) IP address. • *Static* : The system accepts an incoming call from a (statically configured) SIP client without this client needing to have been registered beforehand, if the IP address of the client matches the IP address entered under **SIP Client IP Address**. This mode is used by, for example, the MIcrosoft Office Communications Server and other unified xommunication servers.
SIP Client IP Address	Only for **SIP Client Mode** = *Static*. Enter the static local IP address of the SIP client.
Port Number	Only for **SIP Client Mode** = *Static*. Enter the number of the port to be used for connection. A 5 digit sequence is possible. For example, port *5065* must be entered for connection to a Microsoft Exchange Communication Server.
Transport Protocol	Only for **SIP Client Mode** = *Static*. Select the transport protocol for the connection. Possible values: • *UDP* (default value) • *TCP* For example, the *TCP* protocol must be entered for connection to a Microsoft Exchange Communication Server.

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the codec profile to be used if the connection is over a

Field	Description
	VoIP line. Codec profiles are configured in the **VoIP**->**Settings**->**Codec Profiles** menu.
Video	Select if calls between IP telephones are to support the transmission of video data. Video transmission can only be negotiated between the participants if both support this feature.
SRTP	Select if calls via this SIP provider may be secured with SRTP (Secure Real-Time Transport Protocol).

Fields in the menu Further Settings

Field	Description
Multiple SIP Connections (Sub-Exchange)	Select whether multilinks shall be allowed from this terminals. Operation as subsystem: Only in case of connection of a subsystem to a system Here, with a disabled performance feature, only a connection via the subscriber SIP registration is possible. If a second call comes in, it is accepted and the existing call is held. With an enabled performance feature, several SIP connections are possible over the same login. If the performance feature is enabled for as system without subsystem, two simultaneous calls on the phone are not connected to each other after the receiver is replaced but released, for example. Here, the performance feature should not be set. The function is activated by selecting *Enabled*. The function is disabled by default.
No Hold and Retrieve	The performance features "hold a call" and "retrieve a held call" are not available on certain telephones. The function is activated by selecting *Enabled*. The function is disabled by default.
T.38 FAX support	Select if you want to transmit FAX documents via Voice over IP using the T.38 standard. *Enabled* activates T.38 support. Per default, the function is disabled. If the function is disabled, FAX documents are transmitted using G.711.

11.2.2 VoIP - Configuration example (a smartphone as an internal VoIP telephone)

Requirements

- An **be.IP**
- A configured with the Assistents **Initial operation** SIP connection *DeutschlandLAN*
- A taken with the Assistents in operation WLAN access point
- An Smartphone e.g. **iPhone 4**
- Available connection to the WLAN access poin the **be.IP**
- SIP app, Media5-fone, installed on the smartphone

> **Note**
>
> Please note that the scope of settings and supported functions may vary with different versions of smartphone operating systems (iOS, Android) and the smartphone app, Media5-fone.

Example scenario
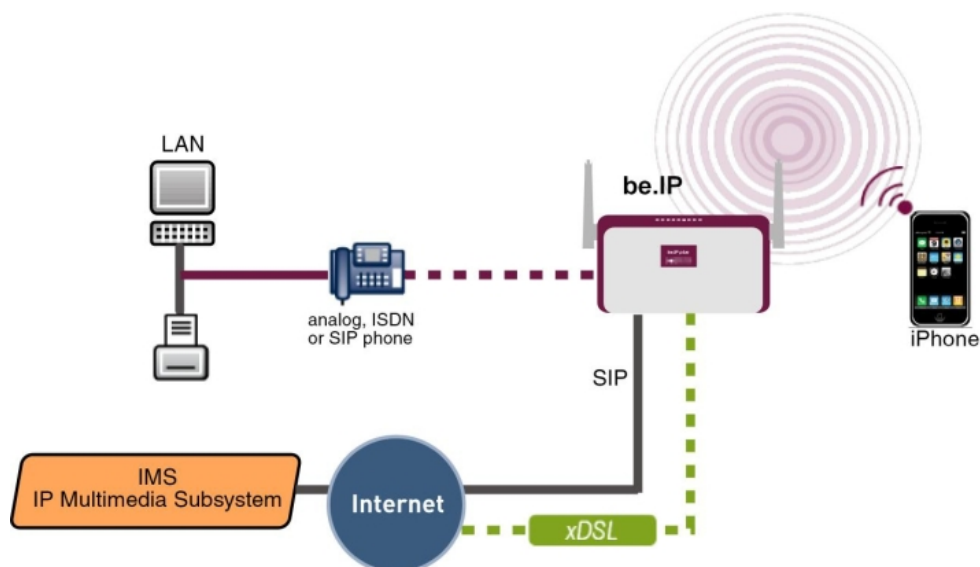
Configuration target

Integration of a smartphone as an internal VoIP phone

Overview of Configuration Steps

Creating a User and integrate Smartphone

Field	Menu	Value
Name	**N e Assistants**->**Telephony**->**Users**->**w**	e.g. *User 33 (iPhone)*
Description	**N e Assistants**->**Telephony**->**Users**->**w**	e.g. *iPhone 33*
Password	**N e Assistants**->**Telephony**->**Users**->**w**	e.g. *1234*
Displayed Description	**N e Assistants**->**Telephony**->**Users**->**w-** >**Add**	e.g. *#33 iPhone*
Internal Number	**N e Assistants**->**Telephony**->**Users**->**w-** >**Add**	e.g. *iPhone*
Description	**Terminals**->**Other phones**->**VoIP**->**New**	e.g. *33*
Internal Numbers	**Terminals**->**Other phones**->**VoIP**->**New**	*33 (#33 iPhone)*

Configuration of the smartphone app using the example Media5-fone

Field	Menu	Value
Title	**New SIP Account** -> **Manual Settings**	e.g. *be.IP*
User Name	**New SIP Account** -> **Manual Settings**	e.g. *33*
Password	**New SIP Account** -> **Manual Settings**	e.g. *1234*
Address	**New SIP Account** -> **Manual Settings**-> **Server**	e. g. *192.168.0.250*
Port	**New SIP Account** -> **Manual Set-**	*5060*

Field	Menu	Value
	tings-> **Server**	
Activating a proxy	**New SIP Account** -> **Manual Settings**-> **Server**	*Disabled*
SIP Transport	**New SIP Account** -> **Manual Settings**-> **Server**	*UDP*
Switch SRTP	**New SIP Account** -> **Manual Settings**-> **Server**	*Switched off*
Mailbox Number	**New SIP Account** -> **Manual Settings** ->**Advanced**	e.g. *50*
Write MWI	**New SIP Account** -> **Manual Settings** ->**Advanced**	*Enabled*
DTMF Method	**New SIP Account** -> **Manual Settings** ->**Advanced**	*RTP Input Signal Band*
Codecs Wi-Fi	**New SIP Account** -> **Manual Settings** ->**Advanced**	*G.711 µLaw, G.711 aLaw*

Configuration of external number

Field	Menu	Value
International Prefix / Country Code	**Assistants**->**Telephony**->**First steps**	e.g. *00* / *49*
National Prefix / City Code	**Assistants**->**Telephony**->**First steps**	e.g. *0* / *911*
Connection Type		*SIP Provider*

Field	Menu	Value
	New	
Type		*DeutschlandLAN*

Field	Menu	Value
	New	
Description		e.g. *SIP Connection*

Field	Menu	Value
	New->Next	
Single Number (MSN)		e.g. *111111*

Field	Menu	Value
	New->Next	
Description		e.g. *SIP number 1*

Field	Menu	Value
	New->Next	
Connection Type		*SIP Provider*

Field	Menu	Value
	New	
Type		*DeutschlandLAN*

Field	Menu	Value
	New	
Name		e.g. *SIP Connection*

Field	Menu	Value
	New->Next	
Single Number (MSN)		e.g. *222222*

Field	Menu	Value
	New->**Next**	
Description		e.g. *SIP number 2*

Field	Menu	Value
	New->Next	
Connection Type		*SIP Provider*

Field	Menu	Value
	New	
Type		*DeutschlandLAN*

Field	Menu	Value
	New	
Name		e.g. *SIP Connection*

Field	Menu	Value
	New->**Next**	
Single Number (MSN)		e.g. *333333*

Field	Menu	Value
	New->Next	
Description		e.g. *SIP number 3*

Field	Menu	Value
	New->**Next**	

Signalling of incoming calls

Feld	Menü	Wert
Assignment Type	**Assistants**->**Telephony**->**Call Distribution**-> **<111111>** 🖉	*Team*
Team	**Assistants**->**Telephony**->**Call Distribution**-> **<111111>** 🖉	e.g. *40 (Team global)*
Assignment Type	**Assistants**->**Telephony**->**Call Distribution**-> **<222222>** 🖉	*Extension*
Assignment	**Assistants**->**Telephony**->**Call Distribution**-> **<222222>** 🖉	e.g. *20 (Sys Tel 20)*
Assignment Type	**Assistants**->**Telephony**->**Call Distribution**-> **<333333>** 🖉	*Extension*
Assignment	**Assistants**->**Telephony**->**Call Distribution**-> **<333333>** 🖉	e.g. *33 (#33 iPhone)*

Signalling of specific number

Feld	Menü	Wert
Trunk	**Numbering**->**User Settings**->**Users**-> **<User 33> (iPhone)** 🖉 ->**Outgoing Signalisation**->**Internal Number**->**<33>** 🖉	*SIP Connection*
Outgoing Signalisation	**Numbering**->**User Settings**->**Users**-> **<User 33> (iPhone)** 🖉 ->**Outgoing Signalisation**->**Internal Number**->**<33>** 🖉	e.g. *333333*

Change registration timer in Media5-fone

Field	Menu	Value
Reg. Timer (Sec)	**More** -> **Settings** -> **Configure SIP Accounts** -> **be.IP** -> **Server** -> **Reg. Timer (Sec)**	e.g. *1200*

Configuration of codecs in Media5-fone

Field	Menu	Value
DTMF Method	**More** -> **Settings** -> **Configure SIP**	*RTP Input Signal*

Field	Menu	Value
	Accounts -> **be.IP** -> **Advanced**	*Band*
Codec Wi-Fi	**More** -> **Settings** -> **Configure SIP Accounts** -> **be.IP** -> **Advanced**	e.g. *G.711 µLaw, G.711 aLaw*

11.2.3 ISDN

In the **Terminals**->**Other phones**->**ISDN** menu, you configure the connected ISDN terminals. For example, you perform assignment of a configured internal number.

Only for compact systems. Two predefined entries are displayed:

Description	Interface	Terminal Type	Internal Numbers	License Allocation
ISDN 1	S0 1	Telephone	30	Enabled
ISDN 2	S0 2	Telephone	35	Enabled

11.2.3.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to add ISDN terminals.

The **Terminals**->**Other phones**->**ISDN**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the ISDN telephone.
Interface	Select the interface to which the ISDN telephone shall be connected.

Fields in the Basic Phone Settings menu

Field	Description
Terminal Type	Select the terminal type. Possible values: • *Telephone* (default value) • *Answering Machine* • *Voice Mail* • *Emergency Phone*

Field	Description
Internal Numbers	Select the internal number for this terminal You can define several internal numbers. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

11.2.4 analog

In the **Terminals**->**Other phones**->**Analogue** menu, you configure the connected analogue terminals. For example, you perform assignment of a configured internal number.

Only for compact systems: Two predefined entries are displayed:

Description	Interface	Terminal Type	Internal Numbers	License Allocation
a/b 1	FXS 1	Telephone	10	Enabled
a/b 2	FXS 2	Telephone	11	Enabled
a/b 3	FXS 3	Telephone	12	Enabled
a/b 4	FXS 4	Multi Function Device/Telefax	13	Enabled

11.2.4.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to add analog terminals.

Choose the ≡₊ icon to copy existing entries. Copying an entry can prove useful if you wish to create an entry only distinguished by a few parameters from an existing entry. In this case, you copy the entry and modify the desired parameters.

The **Terminals**->**Other phones**->**Analogue**->**Edit** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the analogue telephone.

Field	Description
Interface	Select the interface to which the telephone shall be connected.

Fields in the Basic Phone Settings menu

Field	Description
Terminal Type	Select the terminal type. Possible values: • *Multi Function Device/Telefax* • *Telephone* • *Modem* • *Answering Machine* • *Emergency Phone*
Internal Number	Select the internal number for this terminal. Possible values: • *No free Extension Available*: The configured internal number is already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

Fields in the Phone Settings menu

Field	Description
Call Waiting	Select whether call waiting shall be allowed for this device. The function is activated by selecting *Enabled*. The function is enabled by default.
Do not Disturb	Select whether you wish to use the call protection (do not disturb) performance feature. With this performance feature, you can enable call signalling to your terminal. Analogue terminals use system code numbers for this. Possible values:

Field	Description
	• *Internal Calls not signaled* • *External Calls not signaled* • *No Calls signaled*

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

Fields in the CLIP Settings menu

Field	Description
Show incoming Number (CLIP)	Select whether the subscriber's number shall be transmitted. The function is activated by selecting *Enabled*. The function is enabled by default.
Show Date and Time	Only for **Show incoming Number (CLIP)** *Enabled* Select whether the time and date should be taken from your PABX system and displayed on the telephone. The function is activated by selecting *Enabled*. The function is enabled by default.
Show incoming Name (CNIP)	Only for **Show incoming Number (CLIP)** *Enabled* Select whether the caller's number shall be displayed. The caller's number can be displayed if an entry exists in the system telephone book. The function is activated by selecting *Enabled*. The function is enabled by default.
Show incoming waiting Number (CLIP off Hook)	Only for **Show incoming Number (CLIP)** *Enabled* Select whether the number of a caller waiting during an existing call shall be displayed. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the Further Settings menu

Field	Description
Show new Messages (MWI)	Only for **Show incoming Number (CLIP)** *Enabled* Select whether new messages shall be signalled on a voice mail system. The function is activated by selecting *Enabled*. The function is enabled by default.
Transmit Charges Pulses	Select whether the system shall generate charge pulses for the terminal from the ISDN network charge information. For this purpose, you can define the charge impulse at 12 kHz or 16 kHz. Possible values: • *Off*: Charge information from the ISDN network is not transmitted. • *12 kHz* • *16 kHz* The default value is *16 kHz*
FXS Ringing Frequency	Call signalling in analogue terminals occurs by configuring a call switching voltage at the called analogue connections. This call switching voltage is converted into a specific ring tone by the analogue terminal. In the system, for the analogue connections you can set a call switching voltage with a frequency of *25 Hz* or *50 Hz*. The default value is *50* Hz.
Flash Time for DTMF Dialling	When operating analogue terminals with the multifrequency code dialling method, you can set the flashtime that the system detects as maximum flash length. If the terminal flash is longer than the defined period, "replaced receiver" is detected. Values from *100 ms* to *1000 ms* are possible. The default value is *400 ms*.

11.2.5 CAPI

If your device supports CAPI, you configure the connected CAPI terminals in the menu **Terminals**->**Other phones**->**CAPI**. For example, you perform assignment of a configured internal number.

11.2.5.1 Edit or New

Choose the ⟋ icon to edit existing entries. Select the **New** button to add CAPI terminals.

The **Terminals**->**Other phones**->**CAPI**->**New** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the CAPI telephone.

Fields in the menu Basic Phone Settings

Field	Description
Internal Numbers	Use **Add** to select the internal number for this terminal. You can define several internal numbers. Possible values: • *No free Extension Available*: All configured internal numbers are already in use. First configure another user with additional numbers. • *<Internal Number>*: Select one of the existing numbers of the configured users.

11.3 Overview

11.3.1 Overview

In the **Terminals**->**Overview**->**Overview** menu, you get an overview of all configured terminals.

Values in the Overview list

Field	Description
Description	Displays the terminal description.
Phone Type	Displays the telephone type.
Interface / Location	For ISDN, system and analogue terminals, displays the interface at which you're connected to the system. The configured location is displayed for IP terminals.
Internal Numbers	Displays the configured internal number.

Chapter 12   Call Routing

The functions for external calls and automatic route selections for external calls are defined in call routing.

12.1   Outgoing Services

In the **Call Routing**->**Outgoing Services** menu, you can configure the performance features **Direct Call**, **Call Forwarding**, **Dial Control** and **Priority Numbers**.

12.1.1   Direct Call

In the **Call Routing**->**Outgoing Services**->**Direct Call** menu you configure numbers that are dialled directly without the subscriber needing to dial a number themselves on the phone.

You wish to configure a telephone for which a call to a specific number is set up even without entry of the number (e.g. emergency telephone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone, if required (e.g. children or grandparents). If you have set up the "Direct Call" function for one or more telephones, the receiver of the corresponding telephone only needs to be lifted. After a period without further entries set in configuration, the system automatically dials the configured direct call number.

If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated.

The time for Direct Call is set under **System Management**->**Global Settings**->**Timer**->**Direct Call**.

> **Note**
>
> In the system, up to 10 direct call destinations with names and telephone numbers can be set up by the administrator. These destinations should then only be assigned to the terminals by the user via the user configuration interface. In the configuration, system direct call, or a direct call specifically configured for the terminal, can then be set by the user.

12.1.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing**->**Outgoing Services**->**Direct Call**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Direct Call Number	Enter the number to be automatically dialled if no number is to be dialled for a certain time after the receiver has been picked up.

12.1.2 Call Forwarding

In the **Call Routing**->**Outgoing Services**->**Call Forwarding** menu, you configure call forwarding of external calls for an internal subscriber.

You are temporarily away from your office, but don't want to miss a call. With call forwarding to another number, e.g. your mobile, you can receive your calls even when you are not at your desk. You can forward calls on your number to any call number. It can occur *Immediately*, *On no reply* or *On Busy*. Call forwarding *On no reply* and *On Busy* can exist concurrently. If you are not near your telephone, for example, the call is forwarded to another number (e.g. your mobile phone) after a short period. If you are making a call at your desk, other caller may receive the busy signal. You can forward these callers e.g. to a colleague or the secretary by using call forwarding on busy.

Every internal subscriber to the system can forward her calls to another number. Calls can be forwarded to internal subscriber numbers, internal team numbers or external numbers When the number to which calls shall be forwarded is entered, the system automatically checks whether it's an internal or external number.

In a team, call forwarding can be set up for one subscriber in the team. This call continues to be signalled to the other team subscribers. Call forwarding to an internal or external subscriber is performed in the system.

Call forwarding to an internal number is performed in the system. If an internal call to an external number is to be forwarded, forwarding also occurs in the system. Here, the connection is on the bundle cleared for the subscriber doing the setup. If call forwarding occurs via an ISDN connection, one B channels remains in use; in case of forwarding from external to

external, it's both B channels. Two possibilities exist for call forwarding of an external call to an external number:

* Call forwarding in the exchange: Call forwarding is conducted at the exchange if only one subscriber is entered in the call allocation for an external call. For call forwarding in the exchange, the performance features Call Deflection (point-to-multipoint connection) or Partial Rerouting (point-to-point connection) must be enabled with the network operator for the relevant ISDN connections.

* Call forwarding in the system: Call forwarding occurs in the system if the required performance features for call forwarding at the exchange are not available for the relevant ISDN connections. If several telephones (e. g. a team), some of which have set up call forwarding, receive an external call, the corresponding call forwarding is performed in the system. Here, the external connection is set up over a bundle's B channel, cleared for the subscriber initiating the setup. This B-channel remains assigned for the duration of active call forwarding.

> **Note**
>
> If the system is connected to the external ISDN (if supported by you device), for external-to-external connections, the system systematically attempts to initiate call forwarding via the exchange For teams, there can be manual definition of whether call forwarding shall occur via the exchange or the system. If the system possesses no ISDN connections, or if Call Deflection (point-to-multipoint connection) or Partial Rerouting (point-to-point connection) has not been ordered from the network operator, call forwarding occurs solely in the system.

12.1.2.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing**->**Outgoing Services**->**Call Forwarding**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Internal Number	Select the internal number to which the incoming calls shall be forwarded.
Type of Call Forwarding	Select when incoming calls shall be forwarded to the specified internal number.

Field	Description
	Possible values: • *Immediately* • *On Busy* • *On no reply* (default value) • *On busy / On no reply*
Target Number "On no reply"	Enter the number to which incoming calls shall be forwarded after time.
Target Number "On busy"	Enter the number to which incoming calls shall be forwarded on busy.
Target Number "Immediate"	Enter the number to which incoming calls shall be forwarded immediately.

12.1.3 Dial Control

In the **Call Routing**->**Outgoing Services**->**Dial Control** menu, you block specific numbers/partial numbers, or release these .

You wish to prevent dialling of specific numbers in the system, e. g. the numbers of expensive value-added services. Enter these numbers or partial numbers into the dial ranges list of blocked numbers. All subscribers subject to dial ranges cannot dial these numbers. However, if you should need specific numbers from a blocked sector, you can clear these via the dial ranges list of cleared numbers.

You can block specific numbers or prefixes with the blocked numbers list. You can clear the blocked numbers or prefixes with the cleared numbers list. If a number entered as a cleared number is longer than one entered as a blocked number, this number can be dialled. When you dial a number, dialling after the blocked digit is terminated and you hear the busy tone. You can assign each user individually to the dial ranges in the user settings.

Example: Blocked number *01*, all external numbers that begin with *01* are blocked. Cleared number *012345*, dialling can proceed. All external numbers that begin with *012345* can be dialled. If two identical numbers (same number sequence and same number of digits, e. g. *01234* and *01234*) are entered in the list of cleared numbers as well as the list of blocked numbers, dialling of the number is prevented.

> **Note**
>
> Subscribers who enjoy full or partial dialling access (no outside line access) are authorised for dialling of cleared numbers via the list of cleared numbers.
>
> Please ensure that the area code is entered in the configuration, otherwise, the block can be circumvented in the local network by prefixing the area code.

12.1.3.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing**->**Outgoing Services**->**Dial Control**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Inhibited number	Enter the number that cannot be dialled.
Enabled number	Enter the number for which dialling is explicitly permitted.

12.1.4 Priority Numbers

In the **Call Routing**->**Outgoing Services**->**Priority Numbers** menu you configure numbers with particular special functions, e. g. emergency functions.

In your system configuration, you can enter numbers that must be accessible in an emergency. If you now dial one of these priority numbers, it is detected by the system and an ISDN B channel is automatically cleared. If the external ISDN B channels are already in use, one of the ISDN B channels is freed up and the calling subscribers hear the busy tone. An ongoing priority call is not interrupted.

12.1.4.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing**->**Outgoing Services**->**Priority Numbers**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.
Priority Number	Enter the number which can even be dialled if all B channels are occupied. In this case, an external B channel is released for this connection and reassigned for the priority call. An ongoing priority call is not interrupted.

12.1.5 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.

12.1.5.1 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.

12.2 Automatic Route Selection

In the **Call Routing**->**Automatic Route Selection** menu, you can set up routes for external calls in addition to configured line occupancy. Here, bundles released for users can be selectively assigned to ongoing calls according to the dialled number, or new providers entered along with their network access prefixes. You then specifically define the routing for individually created zones for every weekday.

12.2.1 General

In the **Call Routing**->**Automatic Route Selection**->**General** menu, you enable the ARS - Automatic Route Selection - function and select the desired route level.

The menu **Call Routing**->**Automatic Route Selection**->**General** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
ARS	Select whether to enable the ARS performance feature (Automatic Route Selection). The function is activated by selecting *Enabled*. The function is disabled by default.
Routing Stage	Select whether additional routes shall be used if an entered provider or bundle cannot be accessed. Possible values: • *1 (No Fallback)*: If the entered provider or selected bundle is (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 1**) not available, connection setup is terminated. • *2*: If the entered provider or selected bundle (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 1**) is not available, there is an attempt to initiate the connection over the additional entered routing variant (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 2**). • *3* (default value): If neither of the two entered providers or bundles (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add** -> **Mo-Su** ->**Routing Stage 1** and **Routing Stage 2**) is available, dialling occurs via the provider entered as the default for the user (**Numbering**->**Class of Service**->**Add**->**Basic Settings**->**Trunk Line Selection with Line Access Number**).

12.2.2 Interfaces / Provider

In the **Call Routing**->**Automatic Route Selection**->**Interfaces / Provider** menu, enter the
routes or providers along with their network access profiles.

12.2.2.1 Edit or New

Choose the ⁄ icon to edit existing entries. Select the **New** button to create new entries.

The **Call Routing**->**Automatic Route Selection**->**Interfaces / Provider**->**New** menu con-
sists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.
Routing Mode	Select how dialling shall be externally routed. Possible values: • *Default* (default value): The default procedure provides that when dialling externally, the prefix entered under **Call-prefix** is placed first. • *Route*: External dialling is set up via the bundle selected in **Route**.
Call-prefix	Enter the number to be placed as a prefix when making an external call, e.g. to set up a connection via a call-by-call provider.
Route	Only if **Routing Mode** = *Route* Select a bundle via which the external call shall proceed.

12.2.3 Zones &Routing

In the menu **Call Routing**->**Automatic Route Selection**->**Zones &Routing** you define the
zones via which dialling shall proceed using specific routes or providers.

Configuration of the routing tables for the defined zones occurs individually for each week-
day. For 2 routing tables, routing level 1 and routing level 2 can be created as fallback.

Choose the ⁄ icon to edit existing entries. Select the **New** button to create new entries.

12.2.3.1 Trunk Numbers

In the **Trunk Numbers** area, enter the number or partial number of the zones for which you wish to configure the routing tables.

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the entry.
Zones	Configure the desired external zones which should be dialled via the desired entered provider/routes. Possible values: • *Number/Partial Number*: Enter the number or part of a number identifying a zone. • *Name*: Enter a name for this zone.

12.2.3.2 Mon - Sun

In the **Mon** - **Sun** area, select the desired times for each routing level, and the desired route or provider via which outgoing calls shall be routed from the entered time.

Fields in the <Weekday> menu

Field	Description
Routing Stage 1	Configure the switching times for routing level 1. For this, first select the **Start Time** from which routing shall occur over a specific interface or a specific network provider, and select the latter under **Interface / Provider**.
Routing Stage 2	Configure the switching times for routing level 2. For this, first select the **Start Time** from which routing shall occur over a specific interface or a specific network provider, and select the latter under **Interface / Provider**.

Chapter 13 Applications

Internal telephone performance features of the system are set up under **Applications**.

13.1 Calendar

In the **Applications**->**Calendar** menu, you can decide whether to make new entries or modifications in the calendar.

Every company has fixed business hours. You can enter these in the system's internal calendar. For example, all calls outside of business hours can be signalled to a exchange or an answering machine. During this period, your employees can perform other tasks, without being interrupted by telephone calls. The individual call options of a team are automatically switched through the calendars.

You wish to modify the external calling authorisations after business hours for specific subscribers. In the system configuration, you can set individually for each user whether the authorisation for external calls is automatically switched. The switch occurs according to the data in the assigned calendar.

You can set up five types of calendars in the system. The "Authorisation Class" and "Night Operation" calendars are intended for central switching and can only be set up once. The "Team Signalling", "Intercom Signalling" and "Redirect to internal/external number" calendars can be set up repeatedly. Several different switching times can be selected for each weekday.

In the configuration, a calendar can be assigned to all performance features for which several options can be defined (e.g. teams) Switching between the individual call options then occurs at the switching times of the assigned calendar.

13.1.1 Calendar

In the menu **Applications**->**Calendar**->**Calendar** you can view, modify or copy a previously set calendar as well as create new calendars.

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

13.1.1.1 General

In the **General** area you define the name of the calendar to be created.

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

Fields in the menu Basic Settings

Field	Description
Description	Enter a description for the calendar.
Application	Select the application for which the calendar shall be used.
	Please note that this field cannot be edited with pre-existing entries. If another application is to be configured, you must create another entry and delete the existing one.
	Possible values:
	• *Team Signalling* (default value): Here, several calendars can be set up.
	• *Doorline Signalling*: Here, several calendars can be set up.
	• *Night Mode*: Here, only one calendar can be set up.
	• *Class of Service*: Here, only one calendar can be set up.
	• *Rerouting for internal/external Number*: Here, several calendars can be set up.
	• *Voice Mail System*: Here, several calendars can be set up.
	• *Alarm Input*: Here, several calendars can be set up.

13.1.1.2 Mon - Sun / Exception

Mon - Sun

In the **Mon** - **Sun** area you set up the switching days and times for this calendar.

The **Applications**->**Calendar**->**Calendar**->**Mon - Sun** menu consists of the following fields:

Fields in the <Weekday> menu

Field	Description
Switching Points	Enter the desired switching times.
	For this, under **Time**, for each weekday select the desired

Field	Description
	switching points to which switching shall occur from any divergent active switching option in the desired switching options selected under **Action**. Depending on the application, the following switching options are available: • *Team Signalling*: Call option 1 to call option 4 • *Doorcom Signalling*: Door Intercom call option 1 and door intercom call option 2 • *Night Mode*: Night operation on and night operation off • *Class of Service*: Authorisation class by default and authorisation class optional • *Rerouting for internal/external Number*: Redirect option 1 to redirect option 4 • *Voice Mail System*: Action *In the Office* and *Out of Office* • *Alarm Input*: Night operation on and night operation off
Use settings from	Only if settings have already been performed for a weekday. Select from which weekday the settings should be imported. If you require specific settings for this day, select the option *Individual*.

Exception

In the **Exception** area, select whether holidays shall be taken into account and, if so, how.

The menu **Applications**->**Calendar**->**Calendar**->**Exception** consists of the following fields:

Fields in the   Settings holidays   menu

Field	Description
Consider public holidays	Select whether appointments entered in the **Applications**->**Calendar**->**Public Holiday** menu shall also be considered in this calendar. The function is activated by selecting *Enabled*.

Field	Description
	The function is disabled by default.
Use settings from	Only if **Consider public holidays** is enabled.
	Select from which weekday the settings for holidays should be imported. Configure weekdays in menu **Applications**->**Calendar**->**Calendar**-> **Mon - Sun**
	If you require specific settings for holidays, select the option *Individual*.
Switching Points	Only for **Use settings from** = *Individual*
	Enter the desired switching times.
	For this, under **Time**, select the desired switching points to which switching shall occur from any divergent active switching option in the desired switching options selected under **Action**.
	Depending on the application, the following switching options are available:
	• *Team Signalling*: Call option 1 to call option 4
	• *Doorcom Signalling*: Door Intercom call option 1 and door intercom call option 2
	• *Night Mode*: Night operation on and night operation off
	• *Class of Service*: Authorisation class by default and authorisation class optional
	• *Rerouting for internal/external Number*: Redirect option 1 to redirect option 4
	• *Voice Mail System*: Action *In the Office* and *Out of Office*
	• *Alarm Input*: Night operation on and night operation off

13.1.2 Public Holiday

In the **Applications**->**Calendar**->**Public Holiday** menu, you can enter holidays or any special days for which divergent settings should be made via the calendar. The holiday entries are sorted by date!

13.1.2.1 Edit or New

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

The menu **Applications**->**Calendar**->**Public Holiday**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for a holiday.
Date (DD - MM)	Enter the date with day and month in two-digit form. Incorrect entries, e. g. 31.02 are accepted and saved but not executed by the system.

13.2 Rerouting

In the **Applications**->**Rerouting** menu, you configure how incoming calls should be handled by default in the system.

13.2.1 Rerouting Functions

In the **Applications**->**Rerouting**->**Rerouting Functions** menu you can set up various redirect options for *Immediately*, *On Busy*, *On No Reply* or *On Busy and On No Reply*. You then assign these redirect options to the external connections in the **Numbering**->**Call Distribution**->**Incoming Distribution** menu.

13.2.1.1 Edit or New

Choose the icon to edit existing entries. Select the **New** button to create new redirect options.

The **Applications**->**Rerouting**->**Rerouting Functions**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the redirect function.

Field	Description
Type of Rerouting Function	Select the desired exchange function. Possible values: • *Immediately* (default value) • *On Busy* • *On No Reply* • *On Busy and On No Reply*

Fields in the On Busy Settings menu.

Field	Description
Size of Queue	Only for **Type of Rerouting Function** = *On Busy* or *On Busy and On No Reply* In this field, you can configure the maximum number of subscribers on hold. The queue may include up to 10 subscribers. Additional callers get a "busy" tone. Possible values are *0* (no queue) to *10*. The default value is *0*.
Take Waiting Calls with	Only for **Type of Rerouting Function** = *On Busy* or *On Busy and On No Reply* Define what callers on hold shall hear (internal or configured music-on-hold, announcement). Possible values: • *MoH Wave 1* to *MoH Wave 8* • *MoH internal 1* (default value) • *MOH internal 2* • *Off*
Max waiting time in the queue	Only for **Type of Rerouting Function** = *On Busy* or *On Busy and On No Reply* Define maximum time a caller can remain on hold. After expiration of this time, the caller shall be transferred to the defined redirect destination. Leave *Endless* for an unlimited queue (corresponds to value 0). Disable *Endless*, to enter the desired value.

Fields in the On No Reply Settings menu.

Field	Description
Time for Rerouting on No Reply	Define maximum time a caller can remain on hold if she cannot reach the destination number. After expiration of this time, the caller shall be transferred to the defined redirect destination. The default value is *30* seconds.

Fields in the Further Settings menu.

Field	Description
Announcement	Select whether the incoming call shall be redirected to an announcement. Possible values: • *Off* (default value): The incoming call is not redirected to an announcement. • *MoH Wave 1* to *MoH Wave 8*
Target Number	Select the internal number to which the incoming call shall be redirected. Possible values: • *No Number (Disconnect)*: The call is terminated, the connection ended. • *<Extension number>*: If a destination number is entered, the call is forwarded.
Transfer with	The caller hears the defined announcement or music while her call is being transferred. Possible values: • *Ring tone* • *MoH Wave 1* to *MoH Wave 8* • *MOH internal 1* • *MOH internal 2* • *<Wave file>*

Announcement before query

You have set up a general information call number which customers with various problems or requests ring up. Naturally, no single employee or team can provide information in every subject areas. So the caller would need to be transferred to the individual departments. If you knew beforehand which requests (subject area) a caller had, you could immediately transfer him to the competent department. Thus, your callers don't have to be initially accepted and transferred by an exchange. Every caller decides for him/herself with which employee he/she wishes to be connected.

With the performance feature **Auto Attendant with DISA** calls are automatically accepted by the system. The caller then hears an announcement with information about which entries are possible during or after the announcement. Once the entry is made, the announcement ends and the caller is transferred to an internal subscriber or team. If the caller provides a false or no entry, he/she is transferred to the defined redirect destination (internal subscriber or team). While being transferred, the caller hears a ring tone or the system's music-on-hold.

> **Note**
>
> DISA - Direct Inward System Access Once a call is received by the system, the caller is automatically transferred after a code number is entered. This code is assigned to an internal number in the system. Entry of a number or code must occur during the announcement. Once the announcement (Wave file) ends, no more entries are accepted. There follows redirect to a defined redirect destination. The performance feature **Auto Attendant with DISA** is an integral part of the system and can accept up to 28 calls simultaneously.

Fields in the Announcement/Auto Attendant Settings menu.

Field	Description
Call Switching	Select how incoming calls are to be transferred. Possible values: • *Announcement without DISA* (default value): The configured announcement is played. There follows either transfer to the configured internal number, or the connection is interrupted and the caller hears the busy tone. • *DISA, dial internal numbers*: The caller is prompted to enter an internal number. The call is forwarded to the number. • *DISA, dial code numbers*: The caller is prompted to enter a code number from 0 to 9. The desired internal numbers are assigned to the codes. The caller is then transferred

Field	Description
	to the configured internal number.
Number of playbacks	Select how many times the announcement shall be continuously repeated. At conclusion, the caller hears the busy tone.
Auto Attendant with DISA	Only if **Call Switching** = *DISA, dial code numbers* For ever desired DISA code number, select the desired internal number to which the caller shall be transferred.

13.2.2 Rerouting Applications

In the **Applications**->**Rerouting**->**Rerouting Applications** menu, you can configure when which redirect option is to be enabled. You can switch the various options either via calendar or manually.

Choose the ✎ icon to edit existing entries. Select the **New** button to create new redirect applications.

13.2.2.1 General

In the **General** area, you perform basic settings for a redirect application.

The **Applications**->**Rerouting**->**Rerouting Applications**->**New** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the redirect application.
Type of Rerouting Application	Select the destination to which an incoming call shall be redirected. Possible values: • *Trunk Number* (default value) • *Extension* • *Global*
Switch call signalling	Select how to switch between options

Field	Description
	Possible values: • *No calendar,only manually* • *<Calendar>*

13.2.2.2 Variant 1 - 4

In the **Variant** area, you configure the redirect options. You can define up to 4 options.

The menu **Applications**->**Rerouting**->**Rerouting Applications**->**Variant** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Assignment	Choose the redirect function to which you wish to assign the selected option.

13.3 Voice Applications

In the **Applications**->**Voice Applications** menu, you configure you system's wave files.

A professional greeting, especially on the telephone, constitutes a company's visiting card. Voice applications make this possible for every business. Indeed, while being transferred, the caller receives information that's individually tailored, e. g. according to department, or is simply entertained with pleasant music-on-hold.

You wish to employ special music as music-on-hold, or specific announcements for your clients. You can load your self-produced Wave files to the system.

User-specific voice and music files can be saved in the system. Storage space for 2 MoH melodies is available in the system basic settings. The available storage space can be extended with an SD card (if supported by you device). The length of the language and music files that can be saved is based upon the SD card used. Voice and music data is saved in Wave format.

The following voice applications can be defined in the system:

- Announcement before query
- Announcement without query/Infobox
- Wake-up call

• Music on hold

You can find additional information on function, configuration and operation in the description of the individual performance features.

Basic settings of voice applications

The voice applications can be assigned to individual performance features in two different ways.

Every user employing a voice application with this connection always hears the corresponding voice announcement or music from the start. A newly-arrived user hears the voice announcement or music from the start. The number of users who can simultaneously use such a voice application is limited to 28.

Please note that externally played music or voice application music are free of third-party copyrights (GEMA free). Files in other formats must be converted into the company-specific Wave format before being saved in the system.

Note

Please note that Wave files must be available in the following format:

• Bit rate: 128 kbps
• Sampling size: 16 bits
• Channels 1 (mono)
• Sampling rate: 8 kHz
• Audio format: PCM

13.3.1 Wave Files

In the **Applications**->**Voice Applications**->**Wave Files** menu, you can configure your announcement/melody files and volume. You also have the option to play back voicemail messages or download these to your PC. To save a message, click on the ▯ icon. The download dialog then opens. To listen to a message, click on the ▶ icon.

13.3.1.1 Edit

Choose the ✎ icon to edit existing entries. Select 🗑 to change the entry.

MoH internal 1 and *MoH internal 2* are files specified in the system and can thus not be deleted.

The **Applications**->**Voice Applications**->**Wave Files**->**Edit** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the Wave file.
Select file	Click **Browse...** and select the Wave file to be loaded into the system through the Explorer window.
Volume	Select the volume at which the Wave file shall be played by default. Select *0* to play the file at a predefined default volume. You can gradually diminish the volume using the negative values, and increase it with the positive ones. Possible values: • *−5* • *−4* • *−3* • *−2* • *−1* • *0* (default value) • *+1* • *+2* • *+3*

13.4 System Phonebook

In the **Applications**->**System Phonebook** menu, you can enter and administer numbers in the system phone book.

The employees in your company must phone many customers. This is where the system phone book comes in. You need not enter the customer's number but can extract the name via the system telephone display, and dial. Customer names and telephone numbers can be centrally administered by an employee. If a customer whose number has been entered in the phone book calls, his/her name appears in the system telephone display. The system features an integrated phone book in which you can save phone book entries of up to 24-digits (numbers) and up to 20-character names (text).

When creating a telephone book entry, a **Speed Dial Number** code is assigned to each entry. Authorised telephones can initiate speed dial from the phone book via these speed dial numbers.

System telephones

System telephones can dial from the system phone book via a special menu. To search for a telephone entry, enter the first letters (max. 8) of the desired name and confirm the entry. The system always provides 8 phone book entries, which you can view successively. Select the desired entry and confirm with **OK**. You must now begin to dial within 5 seconds. The system telephone redialling list displays the name of the dialled subscriber instead of her number. If a system telephone receives a call whose number and name are saved in the system phone book, the caller's name is indicated in the system telephone display.

Note

The user's other numbers (**Mobile Number** and **Home Number**) are only displayed in the system telephone phone book menu. They are not displayed in the **System Phonebook** menu of the user interface. Entries in the system telephone phone book menu with the (M) mark refer to an entered **Mobile Number** of a user; those with the (H) mark to **Home Number**.

Note

Your PABX system supports LDAP (Lightweight Directory Access Protocol) for providing the entries of the system phonebook to other devices. Name, Number as well as mobile and private numbers can be transferred this way.

13.4.1 Entries

In the **Applications**->**System Phonebook**->**Entries** menu, all configured telephone book entries are displayed with the corresponding speeddial index. The entries in the **Description** column are sorted alphabetically. Click the column title of any column to sort entries in ascending or descending order.

13.4.1.1 Edit or New

Choose the ⁄ icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications**->**System Phonebook**->**Entries**->**New** consists of the following

fields:

Fields in the Phonebook Entry menu.

Field	Description
Description	Enter a description for the entry. Subsequent sorting in the phone book follows the initial letters of the entry.
Phone Number	Enter the telephone number (internal or external).
Speed Dial Number	Enter a speed dial code. If a speed dial code is entered, counting is automatic; i.e. speed dial is automatically assigned. Numbers from *0* to *999* are possible.
Call Through	Select whether the telephone number for the **Call Through** function has been activated. If a telephone number is approved for this, and the caller uses this number for the **Call Through** functions, the caller's authorisation to use the function is checked against the phonebook record. The function is activated by selecting *Enabled*. The function is disabled by default.

13.4.2 Import / Export

You can import and export phone book data in the **Applications**->**System Phonebook**->**Import / Export** menu. You can import data exported from Microsoft Outlook, for example. The phone book data stored in your device is exported to a text file.

The **Applications**->**System Phonebook**->**Import / Export** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Action	Select the desired action. Possible values: • *Export* (default value): You can export the names saved in **Applications**->**System Phonebook**->**Entries** into a text file (specifying phone number, speed dial, call through).

Field	Description
	• *Import*: You can import a text file in the following format: The file imported must consist of individual rows in the following format: name, phone number, speed dial, call through (1 = enabled, 2 = disabled). Example: Name,Phone Number,Speeddial Number,Call Through Hans,123456,1,1 Klaus,234567,2,2 Max,345678,3,1
Separator	Only for **Action** = *Import* and Default File Format not enabled Enter the separator type in the import file. Possible values: • *Comma* (default value) • *Semicolon* • *Space* • *Tabulator*
Select file	Only for **Action** = *Import* select the file to be imported.

You also have the option to import a CSV file.

If the data record consists of more than one column, you have the option to generate two address book entries from the data record for the import (e.g. one for business and one private entry.) To do this, specify the data to be used as the name and phone number in an additional import step. If you want to generate only one phonebook entry, select the blank option in all selection fields for the second record **Phonebook Import**.

Fields in the Phonebook Import menu.

Field	Description
Phone Number	Select which data is to be used from a data record as the phonenumber.
Name	Select which columns are to be used from a data record as the

Field	Description
	name. You have the option to use two elements here (e.g. forename and surname). The middle input field can be used to place a character string between the two elements here. The default separator used is a comma.

Speed dial is automatically assigned. By default, call through is disabled.

13.4.3 General

In the menu **Applications**->**System Phonebook**->**General** you define the user name and password for system phone book administration. In the phone book area, the administrator can view and modify the phone book, as well as import and export data.

The **Applications**->**System Phonebook**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the system telephone book administrator.
Web Access Password	Enter a password for the system telephone book administrator.
Delete Phonebook	If you wish to remove the existing system phone book with all of its entries, enable the option **Delete**. You will then be asked for confirmation **Do you really want to delete all entries of the phonebook?**. Confirm your entry by clicking **OK**. The option **Delete** is disabled by default.

13.5 Call Data Records

In the **Applications**->**Call Data Records** menu, you configure the recording of incoming and outgoing calls.

The capture of call data records provides an overview of the telephone usage in your company.

All external calls can be saved in the device in the form of call data records. These data records contain important information about the individual calls.

You must enable recording of connection data in the **Numbering**->**User Settings**->**Class**

of Services->**Applications** menu. The function is not activated in the ex works state.

13.5.1 Outgoing

The **Applications**->**Call Data Records**->**Outgoing** menu contains information that permits the monitoring of outgoing activities.

The **Applications**->**Call Data Records**->**Outgoing** menu consists of the following fields:

Fields in the Outgoing menu.

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who called.
Int. No.	Displays the user's internal number.
Called Name	Displays the name that called.
Called Number	Displays the dialled number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the external connection was routed.
Costs	Displays the connection charge, but only if the provider transmits the corresponding data.

13.5.2 Incoming

The **Applications**->**Call Data Records**->**Incoming** menu contains information that permits the monitoring of incoming activities.

The **Applications**->**Call Data Records**->**Incoming** menu consists of the following fields:

Fields in the Incoming menu.

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Caller Name	Displays the name of the caller.
External Number	Displays the caller's number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the connection from outside was routed.

13.5.3 General

In the **Applications**->**Call Data Records**->**General** menu, you can define how connection data are saved in the system.

The **Applications**->**Call Data Records**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the call data administrator.
Web Access Password	Enter a password for the call data administrator.
Save outgoing calls	Select which outgoing connections should be saved. Possible values: • *None* (default value) • *All* • *With Project Code only*

Field	Description
Save incoming calls	Select which incoming connections should be saved. Possible values: • *None* (default value) • *All* • *With Project Code only*
Privacy Number Truncation	Select whether to save the number in abbreviated form. If, for data privacy reasons, the number is to be only partially displayed, you can select the number of positions not to be displayed here. For **Outgoing Calls** and for **Incoming Calls** you can separately enter the number of hidden digits. The hiding of digits occurs from right to left. Possible values: • *No* (default value) • *All* • *1* to *9*
Transfer call data records via Serial 2	For modular PABX systems only Select whether to export call data records over the serial interface (Serial 2) after each call which enables you to connect an external charge metering software solution (hotel application). The function is activated by selecting *Enabled*. The function is disabled by default.

Fields in the Actions menu.

Field	Description
Export call data records	If you wish to save the current connection data record in an external file, click **Export** and save the file under the desired storage location and file name.
Delete call data records	If you wish to delete the current connection data record from the system storage, click **Delete**.

13.6 Call List

The menu **Applications**->**Call List** lists details of incoming and outgoing calls. Which kind of calls and how many of them are included can be spcified in the submenu **General**.

13.6.1 Incoming

The **Applications**->**Call List**->**Incoming** menu contains information that permits the monitoring of incoming activities.

The **Applications**->**Call List**->**Incoming** menu consists of the following fields:

Fields in the Incoming menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Caller Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

13.6.2 Outgoing

The **Applications**->**Call List**->**Outgoing** menu contains information that permits the monitoring of outgoing activities.

The **Applications**->**Call List**->**Outgoing** menu consists of the following fields:

Fields in the Outgoing menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Called Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

13.6.3 General

In the **Applications**->**Call List**->**General** menu, you can define how the connection data is saved in the system.

The **Applications**->**Call List**->**General** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Record calls	Select which kind of calls are to be included. Possible values: • *None* • *Incoming only* (default value) • *All*

Field	Description
Record connected calls	Select if accepted calls are to be included, too. This can significantly increase the number of included calls and decrease the amount of time the list can cover until the maximum number of calls is reached and the first calls are deleted from the list.
Max Call List entries for System Calls	Specify the maximum amount of system calls that are included in the list. The maximum number is *1000*. System calls include, e.g., call transfers to extern, calls being accepted by an announcement, team calls that are not accepted by a single user.
Max Call List entries per User	Specify the maximum amount of user calls (calls initiated of accepted by a configured user) that are included in the list. The maximum number is *200*.

13.7 Mini Call Center

The mini call centre is an integrated call centre solution for up to 16 agents. It provides the ideal solution for small groups with high dynamic telecommunication volumes (e. g insides sales, support, order acceptance/processing, customer service). Here, a specific solution with its own administrator has been integrated. The mini call centre is characterised by:

- Flexible allocation of agents and lines
- Dynamic adaptation according to call volume
- Call allocation with off-time for the agent
- Statistical data for agents and lines.

13.7.1 Status

In the **Applications**->**Mini Call Center**->**Status** menu, you can view the current status of lines and logged-in agents in a block, along with the subscribers assigned to lines.

The menu **Applications**->**Mini Call Center**->**Status** consists of the following fields:

Values in the Status list

Field	Description
View	**View** allows you to select which call centre to display.
Line	Displays the mini call centre line.
Agents assigned	Displays the number of agents assigned to this line.

Field	Description
Agents logged on	Displays the number of agents logged-in on this line.
Agents in Wrap-up	Displays the number of agents in post-processing time.
Active Calls	Displays the number of active connections.
Waiting Calls	Displays the number of waiting incoming calls.
Answered of Calls Today	Displays the current number of accepted calls for this day.
Lost Calls Today	Displays the current number of missed calls for this day.

13.7.2 Lines

In the **Applications**->**Mini Call Center**->**Lines** menu, lines are assigned to external and internal numbers, and the name of the call centre to which the line belongs is displayed.

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

13.7.2.1 General

In the **General** area, you perform basic settings for a line.

The menu **Applications**->**Mini Call Center**->**Lines**->**General** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Enter a description for the line.
External Number	Select a number configured as mini call centre for the external connection of this call centre line.
Internal Number	Enter the desired internal number for this line.
Call Center Description	Select *New* and enter a name for the new mini call centre. Or select the name of a mini call centre which has already been generated.

Fields in the Further Settings menu.

Field	Description
Switch call signalling	Select whether the call options for this line shall be switched over a configured calendar and, if so, over which. Possible values: • *No calendar,only manually* • *<Calendar>*
Active Variant	Select which call option shall be enabled by default after configuration for this line.

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

Fields in the Advanced Settings menu.

Field	Description
Team Speed Timer	Enter the time after which call forwarding to the next free agent assigned to this line shall occur.

13.7.2.2 Variant 1 - 4

In the area **Variant**, you set up call options for the mini call centre.

The menu **Applications**->**Mini Call Center**->**Lines**->**Variant** consists of the following fields:

Fields in the Settings menu.

Field	Description
Automatic Call Pick-up with	Select whether an incoming call shall be automatically accepted and, if so, with which announcement or melody. The function is activated by selecting *Enabled*. The function is disabled by default. Select the Wave file to be used for the call acceptance. All preset and additionally-loaded Wave files in the system can be selected.

Fields in the Rerouting Functions menu.

Field	Description
Rerouting on no re-sponse	Select whether and, if so, with which option an incoming call shall be redirected after the entered time. Possible values: • *None*: There shall be no redirect on no-reply. • *<Team>*: The incoming call is forwarded to the selected team after the time specified in **Time until rerouting:**.
Further Rerouting	Select additional redirect functions. You must first configure these in **Applications**->**Rerouting**->**Rerouting Functions**. Then, the following values may be selected: • *Off*: No additional redirect functions. • *Immediately*: Immediately transfers the call according to a configured redirect function . • *On Busy*: Transfers the call according to a configured redirect function on engaged.
Rerouting Function	Only for **Further Rerouting** = *Immediately* or **Further Rerouting** = *On Busy* Select a configured redirect option for immediate redirect, or on busy.
Busy when	Only for **Further Rerouting** = *On Busy* Select from how many busy agents the lines shall be considered busy.

13.7.2.3 Log on / Log off

In the **Log on / Log off** area, select which of the assigned agents shall be logged into the line.

The menu **Applications**->**Mini Call Center**->**Lines**->**Log on / Log off** consists of the following fields:

Fields in the Log on / Log off menu.

Field	Description
Numbers	Displays the internal number and description of the assigned

Field	Description
	agent.
Status	Select whether the agent is logged into the line.
	The agent is logged in by selecting *Logged on*.

13.7.3 Agents

In the **Applications**->**Mini Call Center**->**Agents** menu, lines are assigned to agents. An agent can operate one or more mini call centre lines.

13.7.3.1 Edit or New

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

The menu **Applications**->**Mini Call Center**->**Agents**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
User	Select the configured user who shall serve as a call centre agent. You configure required users in the **Numbering**->**User Settings**->**User** menu.
	The following users are already created:
	• *User 1 to User 4 analog phones*
	• *User 5 and User 6 Sys Tel*
	• *User 7 DECT*
	• *User 8 and User 9 ISDN*
Internal Number	Select the user's internal number to be used for the call centre.

Fields in the Assigned Lines menu.

Field	Description
Select lines	Select the lines for which the agent shall be responsible. The name of the corresponding call centre is displayed again when lines are selected in order to improve the overview.
	Under **Assign** select whether the entry should be enabled.

Fields in the Wrap-up Settings menu.

Field	Description
Wrap-up Time	Enter the time available to this agent for post-processing after concluding a call. No further call can be assigned to this agent during this period. The agent has the option of temporarily extending the period with a telephone procedure.

13.7.4 General

In the **Applications**->**Mini Call Center**->**General** menu, you can set up an HTML web interface access for the mini call centre manager. The latter can then monitor the status of lines and agents, and modify the settings for lines and agents.

The **Applications**->**Mini Call Center**->**General** menu consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Web Access Username	Enter a user name for the mini call centre administrator. When a user logs into the user interface under this name, he/she has access to the user interface with selected parameters for administration of the call centre.
Web Access Password	Enter a password for the mini call centre administrator.

13.8 Doorcom Units

You can connect a door intercom as an intercom adapter to an analogue connection of your system.

If a door intercom adapter is connected to your system, you can speak with a visitor at the door from every authorised telephone. You can assign particular telephones to each ring button. These phones then ring if the ring button is pressed. On analogue telephones, the signal on the telephone matches the intercom call. In place of the internal telephones, an external telephone can also be configured as the call destination for the ring button. Your door intercom can have up to 4 ring buttons. The door opener can be pressed during an intercom call. It is not possible activate the door opener if an intercom call is not taking place.

Note

All functions of the door intercom (intercom adapter) are controlled via the code numbers indicated in the intercom user's manual. The system does not support the intercom with specific codes.

13.8.1 Doorcom Units

In the **Applications**->**Doorcom Units**->**Doorcom Units** menu, select the internal analogue connection (FXS) to which an intercom adapter shall be connected. Then dial the internal number for the connection, and optionally the codes for call acceptance.

13.8.1.1 Edit or New

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

If you intend to add **Doorcom Units**, you may first have to free an interface in the menu **Terminals**->**Other phones**->**Analogue**, i.e. delete one of the preconfigured entries with the button.

The menu **Applications**->**Doorcom Units**->**Doorcom Units**->**New** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Interface	Select the interface to which an intercom adapter shall be connected. All free FXS interfaces are available.
Internal Number	Select the configured internal number to be assigned to the intercom adapter. The number is created in the **Numbering**->**User Settings**->**User** menu.
Code for Doorcom Call Acceptance	Pressing a bell button on the intercom sets off a call in the system. To establish a connection between a called subscriber and the intercom adapter, that subscriber must pick up the receiver and dial the code number for call acceptance. Enter this code for call acceptance. If a subscriber accepts a call from the intercom adapter, the PABX automatically dials the code number required to set up the connection. The subscriber need not make any more entries.

13.8.2 Doorcom Signalling

In the **Applications**->**Doorcom Units**->**Doorcom Signalling** you configure the signalling variant for call acceptance via a intercom adapter. Two intercom call options are available.

The code number for the bell button is the number the intercom adapter dials into the system when the bell button is pressed. You can perform an internal call allocation for each bell button. Please note that guidelines for connecting the intercom adapter depend on the respective manufacturer. For this, read the operating instructions provided by the manufacturer of the intercom adapter.

13.8.2.1 General

In the **General** area you set up the basic features of intercom signalling.

The menu **Applications**->**Doorcom Units**->**Doorcom Signalling**->**General** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Description	Select one of the configured intercom settings previously created in the **Applications**->**Doorcom Units**->**Doorcom Units** menu.
Bell ID	Enter an unambiguous four-digit code for the bell. Pressing a bell button on the intercom adapter initiates a call to the terminals entered in the assigned intercom call option.
Bell Name	Enter a name for the bell.
Switch signalling	Select whether the intercom call options for this bell shall be switched over a configured calendar and, if so, over which. For every ring, you can create up to two intercom call variants in the **Applications**->**Doorcom Units**->**Doorcom Signalling**->**New**->**Variant** menu. Possible values: • *No calendar,only manually* • *<Calendar>*
Active Doorcom Vari-	Select which intercom call option shall be enabled by default for

Field	Description
ant	this bell after configuration.

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

Fields in the Advanced Settings menu.

Field	Description
Call Signalisation Timer	Enter the time in seconds for which the door intercom call shall be signalled. The default value is 40 seconds.
Team Speed Timer	Here, enter the **Team Speed Timer** following which call forwarding after time shall be performed. The default value is 15 seconds.
Simultaneous after time	It is possible for all numbers assigned to this door intercom signalling to be called simultaneously after a specified time. The default value is 60 seconds.

13.8.2.2 Doorcom Signalling Variant 1 and 2

In the **Doorcom Signalling Variant** area, you configure both intercom call options for this signalling profile.

The **Applications**->**Doorcom Units**->**Doorcom Signalling**->**Intercom call variant** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Assignment	Select where pressing of the bell button shall be signalled. Possible values: • *Internal*: Signalling occurs on an internal number. • *External*: Signalling occurs to an external number.
Internal Assignment	Select the internal numbers on which pressing of the door bell shall be signalled. With **Add** you add an internal number.
External Assignment	Enter the external telephone number to which pressing the door bell shall be signalled.

Field	Description
Signalling	You can call the internal number with a broadcast call. Possible values: • *Simultaneous* (default value): All assigned terminals are called simultaneously. If a telephone is busy, call waiting can be used. • *Linear*: All assigned terminals are called in the sequence of their entry in configuration. If a terminal is engaged, the next free terminal is called. The call is signalled ca. 15 seconds per subscriber. The period can be set between 1 and 99 seconds (per bell) in the configuration. If subscribers are on the phone or logged out, there is not forwarding time for these. • *Rotating*: This call is a special case of the linear call. After all terminals are called, call signalling begins again with the first entered terminal. The call is signalled until the caller replaces the receiver or the call is ended by the intercom adapter (after ca. 2 minutes). • *Adding*: The terminals are called in the sequence of their entry in the configuration subscriber list. Every terminal that has already been called is called again, until all entered terminals are called. In the configuration, you can define when each next terminal is called. • *Linear, simultaneous after time*: You have set linear for the door intercom call. After the defined time has run out, you can also set in the configuration that all team subscribers are then called in parallel (simultaneously). • *Rotating, simultaneous after time*: You have set rotating for the door intercom call. After the defined time has run out, you can also set in the configuration that all intercom subscribers are then called in parallel (simultaneously).

13.9 Alarm Calls

The PABX systems' FXS interface can be configured as an alarm input. E. g. an alarm button can be connected to one of these interfaces. When the button is pressed, an alarm call is triggered to either up to eight internal numbers or one of two external numbers. Provided your device is equipped with switch contacts, one of them can be activated during an alarm call. The function can, optionally, be switched on using a calendar or you can switch between the two possible signalling variants.

Note

If you intend to add **Alarm input**, you may first have to free an interface in the menu
Terminals->**Other phones**->**Analogue**, i.e. delete one of the preconfigured entries
with the 🗑 button.

13.9.1 Alarm Calls

Choose the ✎ icon to edit existing entries. Select the **New** button to create new alarm
calls.

13.9.1.1 General

In the **General** area you set up the alarm calls' basic features.

The **Applications**+**Alarm Calls**+**Alarm Calls**->**General** menu consists of the following
fields:

Fields in the menu Basic Settings

Field	Description
Status	Enable or disable the alarm calls function.
	The function is enabled with *Enabled*.
	The function is enabled by default.
Description	Enter a unique name for the alarm.
Interface	Select the interface to be used for alarm.
Internal Number	Select an internal number to be used for the alarm.
Switch signalling	Specify how the alarm that has been set up is to be switched on.
	Possible values:
	• *No calendar,only manually*: Manual switch is enabled.
	• *<calendar entry>*: Select one of the calendar entries that has been configured for the alarm.
Active Variant	Select the call options that are to be enabled. You can configure the options as soon as you have confirmed the entry in the **General** tab with **OK**.

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

Fields in the menu Advanced Settings

Field	Description
Alarm Signalling Peri-od	Enter the length of time for which an alarm is to be signalled, in seconds. The default value is *30* seconds.
Repeat after	Specify the time between the alarm repeats, in seconds. A value of between *1* and *600* seconds is possible. The default value is *10* seconds. Call repeats are not possible via an FXO interface (if an FXO interface is available).
Number of repeats	Specify the number of repeats if the alarm is not taken. A value of between 1 and 10 repeats is possible. The default value is *2*. Call repeats are not possible via an FXO interface (if an FXO interface is available).
External Connection Timer	Specify the maximum duration of an external call once it has been accepted (in seconds). A value of between *1* and *600* seconds is possible. The default value is *60* seconds.
Info Message (UUS1)	Optionally, a message (max. 32 characters) can be sent to ISDN terminals.
Relay Contact	Only applicable if your device is equipped with a relais! If a relay is to be switched on during the alarm: Select the relay that is to be used. Configuration of the Relay is done in the menu **Physical Interfaces**->**Relay**.
Wave-File	Select whether and which saved WAV file is to be played when the alarm call is taken. Possible values:

Field	Description
	• *Off* (default value): A caller on hold shall hear no music-on-hold. • *<WAV file>*: The subscriber called will hear the selected WAV file.
Number of playbacks	Select how many times in a row the announcement is to be played. Possible values: • *Endlessly (default value)* • *1* to *10*

13.9.1.2 Variant 1 and 2

You can configure two versions of the alarm call. One version will normally use the option to call internal extensions, while the other will use the option to call external subscribers.

Fields in the menu Basic Settings

Field	Description
Assignment	You can assign up to eight internal numbers or two external numbers to each alarm. Define whether an alarm's calls are to be signalled to the internal or external subscribers. Possible values: • *External*: The external number that was entered is called. Alternatively, two external numbers can be called for an alarm. • *Internal* (default value): The subscribers assigned to the selected numbers are called based on the signalling defined. For one alarm, eight internal subscribers can be called simultaneously.
First External Number	Only for **Assignment** = *External*Enter the first number of the external subscriber.
Second External Number	Only for **Assignment** = *External*Enter the second number of the external subscriber.
Internal Assignment	Only for **Assignment** = *Internal*Select the internal subscribers.

Field	Description
	Use **Add** to add more internal numbers.

13.10 Voice Mail System

The voicemail system is an intelligent answering machine for those who use your PABX.
An individual voicemail box can be configured for each extension. All subscribers can hear,
save or delete their messages from any telephone using a personal PIN code.

Subscribers can have themselves informed of incoming e-mails. Recorded messages can
be automatically transferred to any e-mail address.

General settings of the voicemail system are performed on your PABX. Operation of the in-
dividual voicemail boxes occurs via telephone.

Every subscriber can use her individual voicemail box by transferring calls to her voicemail
box.

Note

If you wish to use a voicemail box, you'll need an installed SD card (if supportted by
you device). You may need load the required folder structure with the announcement
texts on the SD card. Choose in the **Maintenance**->**Software &Configuration** menu
the option `Import Voice Mail Wave Files`.

Caution

Do not remove the SD card during any read or write access to avoid losing data or
damaging the card. Watch the relevant LED on the top of the device: it will flicker dur-
ing any read or write access.

13.10.1 Voice Mail Boxes

In the **Applications**->**Voice Mail System**->**Voice Mail Boxes** menu, a list of the individual
voicemail boxes for specific subscribers is displayed.

Only for compact systems.

Two predefined voicemail boxes are displayed:

Internal Number	User	License Allocation
10	User 1 analog phone	Enabled
20	User 5 Sys Tel	Enabled

Values in the list Voice Mail Boxes

Field	Description
Internal Number	Displays the number of the individual subscriber for which the voicemail box is configured.
User	Displays the name of the individual subscriber for which the voicemail box is configured.
Language	Displays the language of the announcement text on the voice-mail box. $Default$ means that the centrally-set language, defined for the entire voicemail system in the **Applications**->**Voice Mail System**->**General** menu, is used.
Notification	Indicates whether the subscriber is informed of missed calls.
Active Variant	Indicates the current status of the voicemail box ($In\ the\ Of$- $fice$ or $Out\ of\ Office$).
License Allocation	Indicates whether a licence is currently assigned to a voicemail box.
	Note The number of configured voicemail boxes may exceed the number of existing licences. However, you must make sure that the number of currently used voicemail boxes is covered by the number of licences.

13.10.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create new entries.

The menu **Applications**->**Voice Mail System**->**Voice Mail Boxes**->**New** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Internal Number	Select the internal number of the subscriber for which you wish to set up a voicemail box. You may choose among the numbers configured in the **Numbering**->**User Settings**->**User** menu.
Voice Mail Language	Select the desired language for the voicemail box announcements. Possible values: • _Deutsch_: The voicemail box uses German texts. • _Dutch_: The voicemail box uses Dutch texts. • _English_: The voicemail boxe uses English texts. • _Italian_: The voicemail box uses Italian texts. • _Spanish_: The voicemail box uses Spanish texts. • _French_: The voicemail box uses French texts. • _Portugues_: The voicemail box uses Portugues texts. • _Default_ (default value): The voicemail box uses the language centrally defined for the entire voicemail system in the **Applications**->**Voice Mail System**->**General** menu.

> **Note**
>
> You'll only require a setting that departs from _Default_ if you wish to operate voicemail boxes with various languages within your voicemail system.

Field	Description
E-Mail Address (from User Settings)	Here is displayed the user e-mail address to which a notification shall be sent if a message has been left on the voicemail box. The e-mail address in saved in the **Numbering**->**User Settings**->**User**->**Basic Settings** menu.
E-Mail Notification	Once a message has been left on the voicemail box, the subscriber can be notified. Possible values: • _None_ (default value): The subscriber is not notified. • _E-Mail_: The subscriber is informed of a present message via e-mail.

Field	Description
	• *E-Mail with Attachment*: Once a caller has left a message, the subscriber receives an e-mail with a recording of the message in the attachment. • *User defined*: If the administrator activates the *User defined* function, the e-mail alert settings can be changed by the user in the **User Access**. If the administrator sets a different value, a block is placed on changes from the user.

> **Note**
>
> Once a subscriber has received notification of a new message in an e-mail, the **Status** of the notification is changed according to the settings in the **User Access**. You can configure the status behaviour in the **User Access**->**Voice Mail System**->**Settings** menu under **E-Mail forwarding behavior**.

Field	Description
Max Recording Time	Enter the maximum recording time per message. The possible values are *5* to *300* seconds, the default value is *180* seconds.
Calendar for status "Out of Office"	When the subscriber is out, the voicemail box can be switched over a calendar. If a calendar is to be used, it needs to be configured with the setting **Application** = *Voice Mail System* in the menu **Applications**->**Calendar**. Possible values: • *No calendar,only manually* (default value): The subscriber can manually switch the voicemail box on and off. • <Calendar>: Using the selected calendar, the voicemail box can be switched on or off at the times defined there.

Fields in the menu User Settings

Field	Description
Status of Mail Box Owner	Define in which mode the mailbox shall be used when starting the voicemail system. Possible values: • *In the Office* (default value): Select this setting if the sub-

Field	Description
	scriber is in the office when the voicemail system is started. • *Out of Office*: Select this setting if the subscriber is out of office when the voicemail system is started.
Check PIN	Select whether the currently configured voicemail box should be protected with a PIN. The function is enabled with *Enabled*. The function is disabled by default. You can change the PIN for the personal voice box in the **Numbering**->**User Settings**->**Users**->**Authorizations** under **PIN for Phone Access**.
Mode for status "In the Office"	The voicemail box can be operated with two different settings during office hours. Possible values: • *Announcement and Record* (default value): A caller hears an announcement and can leave a message. • *Announcement only*: A caller hears an announcement, but cannot leave a message.
Mode for status "Out of Office"	The voicemail box can be operated with two different settings outside of office hours. Possible values: • *Announcement only* (default value): A caller hears an announcement, but cannot leave a message. • *Announcement and Record*: A caller hears an announcement and can leave a message.

Select the icon to set up your own voice announcements for the selected voice mail box in addition to the settings above.

The **Applications**->**Voice Mail System** ->**Voice Mail Boxes** -> menu consists of the following fields:

Fields in the menu Voice Announcement

Feld	Beschreibung
In the Office	You can upload your own announcement for the **In the Office** state. Use the WAV file format for this annoncement. Click **New Message** to upload the file. The window **Annouacement Options** opens. If an announcement has been stored, use the ▶ icon to play the announcement, the 🗑 icon to delete it.
Out of Office	You can upload your own announcement for the **Out of Office** state. Use the WAV file format for this annoncement. Click **New Message** to upload the file. The window **Annouacement Options** opens. If an announcement has been stored, use the ▶ icon to play the announcement, the 🗑 icon to delete it.

Fields in the menu Annoucement Options

Feld	Beschreibung
Action	Displays *Update announcement* .
Source Location	For **Action** = *Update annoncement* Select the WAV file to be used for the announcement and click **Start** to upload.

13.10.2 Status

In the **Applications**->**Voice Mail System**->**Status** menu, the status of the individual voice-mail boxes for specific subscribers is indicated. You can see how many calls have gone in-to which voicemail box, and how many "old" calls are already present.

Values in the System Messages list

Field	Description
Internal Number	Displays the number of the individual subscriber for which the voicemail box is configured.
User	Displays the name of the individual subscriber for which the

Field	Description
	voicemail box is configured.
New Calls	Displays the calls which have not yet been listened to by the subscriber.
Old Calls	Displays the calls which have already been listened to or stored by the subscriber.

> **Note**
>
> By default, the system can record a maximum of 59 calls per voicemail box. You cannot change this value in the GUI.

13.10.3 General

In this menu, you can configure the general settings for your voicemail system.

The menu **Applications**->**Voice Mail System** ->**General** consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Voice Mail System	Select whether to activate your voicemail system. The function is enabled with *Enabled*. The function is enabled by default.
Description	Only for **Voice Mail System** enabled. Enter a description for your voicemail system. This description is displayed on the telephone when a call goes in to the voice mail system. The default value is *Voice Mail*.
Internal Number	Only for **Voice Mail System** enabled. Enter the internal number under which to access your voicemail system.

Field	Description
	The default value is *50*.
Language	Select the language for the entire voicemail system. Possible values: • *Deutsch* (default value) • *Dutch* • *English* • *Italian* • *Spanish* • *French* • *Portugues* Diverging from the language set here, a language can be individually set for each voice mail box in the **Applications**+**Voice Mail System**->**Voice Mail Boxes**->**New** menu.

Fields in the menu Mail Settings

Field	Description
SMTP Server	Enter the address (IP address or valid DNS name) of the e-mail server to be used for sending the e-mails.
SMTP Server Port	Enter the port to be used for sending e-mails. The default value is *25*.
Return Address	Enter any address to be used as sender when sending e-mails. This address merely serves to identify e-mails in the inbox.
SMTP User Name	Enter the user name for the SMTP server.
SMTP Password	Enter the password for the SNMP server user.

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

Fields in the menu Advanced Settings

Field	Description
Lifetime	Voicemail messages are deleted after an adjustable period of

Field	Description
	time.
	Possible values are *10* to *60* days. The default value is *60*.

Chapter 14   LAN

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

14.1   IP Configuration

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

14.1.1   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*.

14.1.1.1   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 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 al-

Field	Description
	locate 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* (default value): 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 501 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.
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* .

Field	Description
	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 501 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. 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)*

Field	Description
	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)*, **Transmit Router Advertisement** = *Enabled* 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 selected 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

Field	Description
	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 Ad-vertisement)*
	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*
	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

Field	Description
	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.

Field	Description
	• 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. 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.
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.

Field	Description
	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:

Field	Description
	• *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.

Field	Description
	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. 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

Field	Description
	• 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.

14.2 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**.

14.2.1 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.

14.2.1.1 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).

14.2.2 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 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.

Field	Description
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.

14.2.3 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 15   Wireless LAN Controller

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

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

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

With the **WLAN controller** you can

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

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

15.1   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.

15.1.1   Wireless LAN Controller Wizard

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

15.1.1.1 Basic Settings

The wireless LAN controller uses the following settings:

Region

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

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

Interface

Select the interface to be used for the wireless controller.

DHCP Server

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

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

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

If you wish to use a bintec elmegbintec 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.

15.1.1.2 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.

15.1.1.3 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.

15.1.1.3.1 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 oder WPA 2 or both.

Preshared Key

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

Enter an ASCII string with 8 - 63 characters.

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

Radius Server

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

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

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

EAP 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.

15.1.1.4 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 are being set up.

Channel

Displays the channel that is assigned. You can select an alternative channel.

The number of channels you can select depends on the country setting. Please consult the data sheet for your device.

Note

Configuring the network name (SSID) in Access Point mode means that wireless networks can be logically separated from each other, but they can still physically interfere with each other if they are operating on the same or closely adjacent wireless channels. So if you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart, as a network also partially occupies the adjacent channels.

In the case of manual channel selection, please make sure first that the APs actually support these channels.

Transmit Power

Displays the transmission power in dBm. You can select another transmission power.

With **OK** you apply the settings.

Select the access points that your WLAN controller shall manage. In the **Manage** column, click on the desired entries or click on **Select all** in order to select all entries. Click the **Deselect all** button to disable all entries and to then select individual entries if required (e.g. for large lists).

Click on **Start** in order to install the WLAN and automatically assign the frequencies.

Note

If there are not enough licences available, the message "The maximum number of slave access points that can be supported has been exceeded". Please check your licences. If this message is displayed then you should obtain additional licences if appropriate.

During the installation of the WLAN and the allocation of frequencies, on the messages dis-

played you will see how far the installation has progressed. The display is continuously updated.

Provided that non-overlapping wireless channels are located for all access points, the configuration that is set in the Wizard is transferred to the access points.

When the installation is complete, you will see a list of the **Managed** access points.

Under **Configure the Alert Service for WLAN surveillance**, click **Start** to monitor your managed APs. You are taken to the **External Reporting**->**Alert Service**->**Alert Recipient** menu with the default setting **Event** = *Managed AP offline*. You can specify that you wish to be notified by e-mail if the *Managed AP offline* event occurs.

Click under **New Neighborscan** on **Start**, to rescan adjacent AP's. You will receive a warning that the wireless modules of the access points must also be disabled for a certain period of time. When you start the process with **OK**, a progress bar is displayed. The located AP display is updated every ten seconds.

15.1.2 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.

15.1.2.1 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	Dsecription
VLAN ID	Select an existing VLAN from the pull down menu. Only those 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. Possiblöe values: • *External or static*: Select this option if you are already operating a DHCP server in you netweork, 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 the the menu **Local Services**->**DHCP Server**->**DHCP Configuration**.

15.2 Controller Configuration

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

15.2.1 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.
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 master and slaves. Please note: Make sure that option 138 is active when using an external DHCP server. If you wish to use a bintec elmegbintec 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. 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**

Field	Description
	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.
Slave 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.
Slave AP LED mode	Select the lighting scheme of the slave AP LEDs. Possible values: • *State* (default value): All LEDs show their standard behavior. • *Flashing*: Only the status LED flashes once per second. • *Off*: All LEDs are deactivated.

15.2.2 Slave AP Autoprofile

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

15.2.2.1 Edit or New

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

Fields in the Access Point Filter menu

Field	Description
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	Wählen Sie aus, ob der Betriebsmodus vom verwendeten Funkmodulprofil bestimmt werden soll. The function is activated by selecting *Enabled*. The function is enabled by default.
Active Radio Profile	Only for **Operating Mode** = *Enabled* Select a radio profile.

Field	Description
	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**.

15.3 Slave AP configuration

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

15.3.1 Slave Access Points

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

You will see an entry with a parameter set for each access point (**Location**, **Name**, **IP Address**, **LAN MAC Address**, **Channel**, **Search Channel**, **Status**, **Action**). Choose whether the selected Access Pont is to be managed by the WLAN Controller by clicking the ∧ button or the ∨ button in the **Action** column.

You can disconnect the Access Point from the WLAN Controller and therefore remove it from your WLAN infrastructure by click on the ∨ button. The Access Point then receives the *Discovered* status, but is no longer *Managed*.

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

Possible values for Status

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

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.

15.3.1.1 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**->**Slave AP configuration**->**Slave Access Points**-> ✎ menu if the corresponding device has two wireless modules. With devices featuring a single wireless module, the data for wireless module 1 are displayed.

The menu consists of the following fields:

Fields in the Access Point Settings menu.

Field	Description
Device	Displays the type of device for the AP.
Location	Displays the locality of the AP. The locations are given numbers if no location has been entered. You can enter another locality.
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 master and slaves 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 are 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 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* Possible values are *36*, *40*, *44*, *48* and *Auto* (default value)

Field	Description
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 Network (VSS)	Displays the wireless networks that are currently assigned.

15.3.2 Radio Profiles

An overview of all created wireless module profiles is displayed in the **Wireless LAN Controller**->**Slave AP configuration**->**Radio Profiles** menu. A profile with 2.4 GHz and a profile with 5 GHz are created by default; the 2.4 GHz profile cannot be deleted.

For each wireless module profile you will see an entry with a parameter set (**Radio Profiles**, **Configured Radio Modules**, **Operation Band**, **Wireless Mode**).

15.3.2.1 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**->**Slave AP configuration**->**Radio Profiles**-> ⟋ **/ New** menu consists of the following fields:

Fields in the menu Radio Profile Definition

Field	Description
Description	Enter the desired description of the wireless module profile.
Operation Mode	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 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 the access point is to use. For **Operation Band** = *2.4 GHz In/Outdoor* Possible values: • *802.11g*: The device operates only in accordance with 802.11g. 802.11b clients have no access. • *802.11b*: Your device operates only in accordance with

Field	Description
	802.11b and forces all clients to adapt to it.
	• *802.11 mixed (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g.
	• *802.11 mixed long (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. Only a data rate of 1 and 2 mbps needs to be supported by all clients (basic rates). This mode is also needed for Centrino clients if connection problems occur.
	• *802.11 mixed short (b/g)*: Your device adapts to the client technology and operates according to either 802.11b or 802.11g. The following applies for mixed-short: The data rates 5.5 and 11 mbps must be supported by all clients (basic rates).
	• *802.11b/g/n*: Your device operates according to either 802.11b, 802.11g or 802.11n.
	• *802.11g/n*: Your device operates according to either 802.11g or 802.11n.
	• *802.11n*: Your device operates only according to 802.11n.
	For **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* or *5.8 GHz Outdoor*
	Possible values:
	• *802.11a*: The device operates only in accordance with 802.11a.
	• *802.11n*: Your device operates only according to 802.11n.
	• *802.11a/n*: Your device operates according to either 802.11a or 802.11n.
	• *802.11a/n*: Your device operates according to 802.11ac, 802.11a or 802.11n.
	• *802.11a/n*: Your device operates according to either 802.11ac or 802.11n.
Bandwidth	Not for **Operation Band** = *2.4 GHz In/Outdoor*
	Select how many channels are to be used.
	Possible values:

Field	Description
	• *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.
Number of Spatial Streams	Not for **Operation Band** = *2,4 GHz In/Outdoor* and **Wireless Mode** = *802.11g*, *802.11b*, *802.11 mixed (b/g)*, *802.11 mixed long (b/g)*, *802.11 mixed short (b/g)* and for **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/Outdoor* or *5,8 GHz Outdoor* and **Wireless Mode**= *802.11a* Select how many traffic flows are to be used in parallel. Possible values: • *3* (default value): Three traffic flows are used. • *2*: Two traffic flows are used. • *1*: One traffic flow is used.
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. a 802.11n client) cannot achieve only a poor flow level, because a less powerful client (e. g. a 802.11a client) is treated in the same way when apportioning. The function is enabled with *Enabled*. The function is disabled by default. This fuction is only applied to unprioritized frames of the WMM Classe "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 neighbouring or rogue access points in the network. This search is run without negatively impacting the function as an access point.

Field	Description
	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 channel plan makes a preselection when a channel is selected. This ensures that no channels overlap, i.e. a distance of four channels is maintained between the channels used. This is useful if more access points are used with overlapping radio cells.
	Possible values:
	• *All*: All channels can be dialled when a channel is selected.
	• *Auto*: Depending on the region, operation band, wireless mode and bandwidth, the channels that have a distance of 4 channels are provided.
	• *User defined*: You can select the desired channels yourself.
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.
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*.

Field	Description
	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.
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.
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**.

Field	Description
	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*.

15.3.3 Wireless Networks (VSS)

An overview of all created wireless networks is displayed in the **Wireless LAN Controller**->**Slave AP configuration**->**Wireless Networks (VSS)** menu. A wireless network is created by default.

For every wireless network (VSS), you see an entry with a parameter set (**VSS Description**, **Network Name (SSID)**, **Number of associated radio modules**, **Security**, **Status**, **Action**).

Under **Assign unassigned VSS to all radio modules** click on the **Start** button to assign a newly-created VSS to all wireless modules.

15.3.3.1 Edit or New

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

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

Fields in the menu Service Set Parameters

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

Field	Description
	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.
ARP Processing	Select whether the ARP processing function should be enabled. The ARP data traffic is reduced in the network by the fact that ARP broadcasts that have been converted to ARP unicasts are forwarded to IP addresses that are known internally. Unicasts are quicker and clients with an enabled power save function are not addressed. The function is activated by selecting *Enabled*. The function is disabled by default. Make sure that ARP processing cannot be applied together with the MAC bridge function.
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: • *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	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. 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	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* Select whether you want to use WPA (with TKIP encryption) or WPA 2 (with AES encryption), or both. Possible values: • *WPA and WPA 2* (default value): WPA and WPA 2 can be used. • *WPA*: Only WPA is used. • *WPA 2*: Only WPA2 is used.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA* and *WPA and WPA 2*

Field	Description
	Select the type of encryption you want to apply to WPA. Possible values: • *TKIP* (default value): TKIP is used. • *AES*: AES is used. • *AES and TKIP*: AES or TKIP is used.
WPA2 Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA 2* and *WPA and WPA 2* Select the type of encryption you want to apply to WPA2. Possible values: • *AES* (default value): AES is used. • *TKIP*: TKIP is used. • *AES and TKIP*: AES or TKIP is used.
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 unauthorised 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.

Field	Description
	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 distrubuted 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 utilised, you can set a "soft" restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the **Max. number of clients - hard limit** is reached.
	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	Not all devices support this function.
	This function requires a dual radio setup where the same wire-

Field	Description
	less networkis configured on both radio modules, but in different frequency bands. The **Client Band select** option enables clients to be moved from the frequency band originally selected to a less busy one, providing the client supports this. To achieve a changeover, the connection attempt of a client is initially refused so that the client repeats the attempt in a different frequency band. Possible values: • *Disabled - optimized for fast roaming* (default value): The function is not used for this VSS. This is useful if clients are to switch between different radio cells with as little delay as possible, e. g. with Voice over WLAN. • *2,4 GHz band preferred*: Preference is given to accepting clients in the 2.4 GHz band. • *5 GHz band preferred*: Preference is given to accepting clients in the 5 GHz band.

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 unauthorised access to the network and block them for a certain length of time. A client is blocked if the number of unsuccessful login attempts with a specified time exceeds a certain number. This threshold value and the duration of the block can be configured. A blocked client is blocked at all the APs that are managed by the wireless LAN controller for the VSS concerned, so neither are they able to log into a different radio cell in that VSS. If a client needs to be blocked permanently, this can be done in the **Wireless LAN**

Field	Description
	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*, *40 Mbit/s* and *50 Mbit/s*.
Tx Shaping	Select a bandwidth limitation in the transmit direction.

Field	Description
	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 (keine 802.11b-Geräte)* - see above, for clients with a minimum supported rate of 12 Mbit/s • *Min. 24 MBit/s (keine 802.11b-Geräte)* - 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. • *Ab 12 MBit/s* - see above, for clients with a minimum supported rate of 12 Mbit/s • *Ab 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

Field	Description
	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.

15.4 Monitoring

This menu is used to monitor your WLAN infrastructure.

Note

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

15.4.1 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
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.

15.4.2 Slave Access Points

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

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

15.4.2.1 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.

15.4.2.2 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

Status	Meaning
	time.

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

Possible values for Status

Status	Meaning
None	The client is no longer in a valid status.
Logon	The client is currently logging on with the WLAN.
Associated	The client is logged on with the WLAN.
Authenticate	The client is in the process of being authenticated.
Authenticated	The client is authenticated.

Via the Q 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.

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

15.4.5 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.

15.5 Neighbor Monitoring

This menu serves the monitoring of remote access points.

15.5.1 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.

15.5.2 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.

15.5.3 Rogue Clients

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

Possible values for Rogue Clients

Status	Meaning
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.

Status	Meaning
Last seen	Displays the time of the last registered attempted access.
Static Blacklist	You can categorise a rogue client as untrustworthy by selecting the checkbox in the **Static Blacklist** column. The block on the client does not then end automatically, rather you need to lift it manually.
Delete	You can delete entries with the ▮ symbol.

15.5.3.1 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.

15.6 Maintenance

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

15.6.1 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.
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 16   Networking

16.1   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**.

16.1.1   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.

16.1.1.1   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. 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 restarted, 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".

16.1.2 IPv6 Route Configuration

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

16.1.2.1 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*.

16.1.3 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.

16.1.4 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.

16.1.5 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.

16.2 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 301 and the menu **LAN**->**IP Configuration**->**Interfaces** for the IPv6-relevant parameters.

16.2.1 General Prefix Configuration

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

16.2.1.1 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* .

16.3 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 364).

Specific instructions for configuring NAT, see the end of the chapter *NAT - Configuration example* on page 370.

16.3.1 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**.

16.3.2 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.

16.3.2.1 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 ex-

Field	Description
	ternally valid source port. 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/net-

Field	Description
	mask, etc.) are excluded by NAT.
	• *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*

Field	Description
	• *PUP*
	• *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.

Field	Description
	If you select $Specify\ port$ you can specify a single port, if you select $Specify\ port\ range$ you can specify a continuous 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, $TCP/$

Field	Description
	UDP
	Leave the destination port as it appears or enter the destination 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.

16.3.3 NAT - Configuration example

Requirements

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

Example scenario
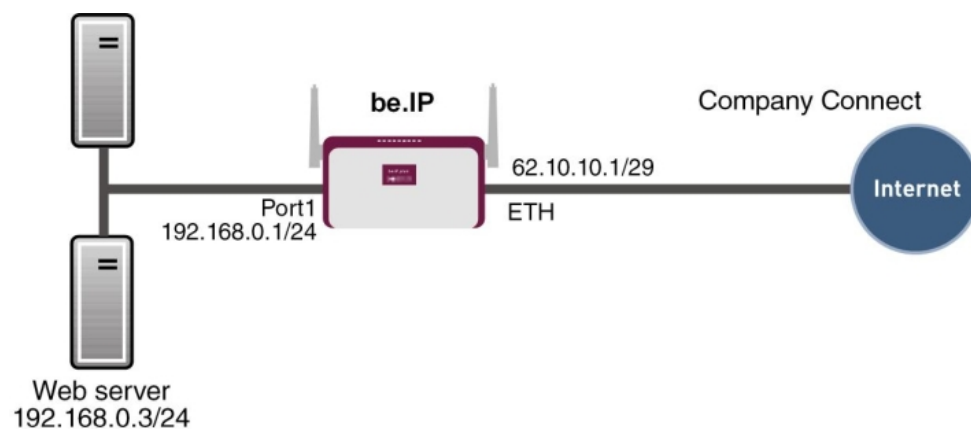
Configuration target

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

Overview of Configuration Steps

Enable NAT

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

Configured NAT enables

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

Web server

Field	Menu	Value
Description	**Network**->**NAT**->**NAT Configuration**->**New**	e.g. *Webserver*
Interface	**Network**->**NAT**->**NAT Configuration**->**New**	*LAN_EN5-0*
Type of traffic	**Network**->**NAT**->**NAT Configuration**->**New**	*incoming (Destination NAT)*
Service	**Network**->**NAT**->**NAT Configuration**->**New**	*http*
Protocol	**Network**->**NAT**->**NAT Configuration**->**New**	*Host*, e.g. *62.10.10.3*
Original Destination IP Address/Netmask	**Network**->**NAT**->**NAT Configuration**->**New**	*Host*, e.g. *192.168.0.3*
New Destination Port	**Network**->**NAT**->**NAT Configuration**->**New**	*Original*

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*
Original Destination IP Address/Netmask	**Network**->**NAT**->**NAT Configuration**->**New**	*96*
Original Destination Port/Range	**Network**->**NAT**->**NAT Configuration**->**New**	*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*

16.4 QoS

QoS (Quality of Service) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them. This is an advantage, especially for time-critical applications such as VoIP.

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data

16.4.1 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.

16.4.1.1 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 unreach-able*, *Source quench*, *Redirect*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. See RFC 792. The default value is *Any*.

Field	Description
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 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.

Field	Description
	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 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).

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

16.4.2 QoS Classification

The data traffic is classified in the **Networking**->**QoS**->**QoS Classification** menu, i.e. the data traffic is associated using class IDs of various classes. To do this, create class plans for classifying IP packets based on pre-defined IP filters. Each class plan is associated to at least one interface via its first filter.

16.4.2.1 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.

Field	Description
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.
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*.

Field	Description
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 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.

16.4.3 QoS Interfaces/Policies

In the **Networking**->**QoS**->**QoS Interfaces/Policies** menu, you set prioritisation of data.

Note

Data can only be prioritized in the outgoing direction.

Packets in the high-priority class always take priority over data with class IDs 1 - 254.

It is possible to assign or guarantee each queue and thus each data class a certain part of the total bandwidth of the interface. In addition, you can optimise the transmission of voice data (real time data).

Depending on the respective interface, a queue is created automatically for each class, but only for data traffic classified as outgoing and for data traffic classified in both directions. A priority is assigned to these automatic queues. The value of the priority is equal to the value of the class ID. You can change the default priority of a queue. If you add new queues, you can also use classes in other class plans via the class ID.

16.4.3.1 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 pos-

Field	Description
	sible 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 Speed	Only for **Traffic shaping** = enabled. 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:

Field	Description
	• *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: • *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

Field	Description
	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 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.

Field	Description
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* 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	Only for **Traffic Shaping** = enabled.

Field	Description
Speed	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 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.

Field	Description
	• *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.
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*.

16.5 Access Rules

Accesses to data and functions are restricted with access lists (which user gets to use which services and files).

You define filters for IP packets in order to allow or block access from or to the various hosts in connected networks. This enables you to prevent undesired connections being set up via the gateway. Access lists define the type of IP traffic the gateway is to accept or deny. The access decision is based on information contained in the IP packets, e.g.:

• source and/or destination IP address
• packet protocol
• source and/or destination port (port ranges are supported)

Access lists are an effective means if, for example, sites with LANs interconnected over a bintec elmeg gateway wish to deny all incoming FTP requests or only allow Telnet sessions between certain hosts.

Access filters in the gateway are based on the combination of filters and actions for filter rules (= rules) and the linking of these rules to form rule chains. They act on the incoming data packets to allow or deny access to the gateway for certain data.

A filter describes a certain part of the IP data traffic based on the source and/or destination IP address, netmask, protocol and source and/or destination port.

You use the rules that you set up in the access lists to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

There are various approaches for the definition of rules and rule chains:

Allow all packets that are not explicitly denied, i.e.:

- Deny all packets that match Filter 1.
- Deny all packets that match Filter 2.
- ...
- Allow the rest.

or

Allow all packets that are explicitly allowed, i.e.:

- Allow all packets that match Filter 1.
- Allow all packets that match Filter 2.
- ...
- Deny the rest.

or

Combination of the two possibilities described above.

A number of separate rule chains can be created. The same filter can also be used in different rule chains.

You can also assign a rule chain individually to each interface.

Caution

Make sure you don't lock yourself out when configuring filters.

> If possible, access your gateway for filter configuration over the serial console (not
> available for all devices) interface or ISDN Login.

16.5.1 Access Filter

This menu is for configuration of access filter Each filter describes a certain part of the IP
traffic and defines, for example, the IP addresses, the protocol, the source port or the des-
tination port.

A list of all access filters is displayed in the **Networking**->**Access Rules**->**Access Filter**
menu.

16.5.1.1 Edit or New

Choose the ✎ icon to edit existing entries. To configure access fitters, select the **New** but-
ton.

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.

Field	Description
	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*
	• *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 Ad-	Enter the destination IPv6 address of the data packets and the

Field	Description
dress/Length	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. 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

Field	Description
	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: • *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*.

16.5.2 Rule Chains

Rules for IP filters are configured in the **Rule Chains** menu. These can be created separately or incorporated in rule chains.

In the **Networking**->**Access Rules**->**Rule Chains** menu, all created filter rules are listed.

16.5.2.1 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.

Field	Description
	• *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 $t_↓$ 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.

16.5.3 Interface Assignment

In this menu, the configured rule chains are assigned to the individual interfaces and the gateway's behavior is defined for denying IP packets.

A list of all configured interface assignments is displayed in the **Networking**->**Access Rules**->**Interface Assignment** menu.

16.5.3.1 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.

Field	Description
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.

16.6 Drop In

"Drop-in mode" allows you to split a network into smaller segments without having to divide the IP network into subnets. Several interfaces can be combined in a drop-in group and assigned to a network to do this. All of the interfaces are then configured with the same IP address.

Within a segment, network components which are connected to a connection can then be grouped and, for example, be protected by firewall. Data traffic from network components between individual segments which are assigned to different ports are then controlled according to the configured firewall rules.

16.6.1 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.

16.6.1.1 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

Field	Description
	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:
	• *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.

Field	Description
	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 17 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.

17.1   General

17.1.1 General

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

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

Fields in the Basic Settings menu.

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

17.2 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.

17.2.1 IGMP

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

17.2.1.1 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**.

17.2.2 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.

17.3 Forwarding

17.3.1 Forwarding

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

17.3.1.1 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**.

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

Chapter 18 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.

18.1 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.

18.1.1 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.

18.1.1.1 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 501 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 501 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.

18.1.2 PPTP

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

In this menu, you configure an Internet connection that uses the Point Tunnelling Protocol (PPTP) to set up a connection. This is required in Austria, for example.

18.1.2.1 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 Interfaces**->**ATM**->**Profiles**->**New**, e.g. $ethoa50-0$.
User Name	Enter the user name.

Field	Description
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 501 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:

Field	Description
	• *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*.

Field	Description
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). The function is enabled with *Enabled*. The function is disabled by default.

Field	Description
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.

18.1.3 PPPoA

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

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

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

18.1.3.1 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. Possible values:

Field	Description
	• *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 501 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 network.
	• *Netmask*: Netmask for **Remote IP Address** If no entry is

Field	Description
	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 501 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. The function is activated by selecting *Enabled* .

Field	Description
	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.
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* - *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.

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 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. |

Field	Description
	• *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.

18.1.4 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

18.1.4.1 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.
	Only activate this option if you have Internet access with a flat-rate charge.

Field	Description
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* Assign the IP address from your LAN to the ISDN interface which is to be used as your device's internal source address.

Field	Description
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. • $Multi-User\ (Dialin\ only)$: The interface is defined as multi-user connection partner, i.e. several clients dial in with

Field	Description
	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:
	• *None* (default value): Your device does not call back.

Field	Description
	• *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 dialup connections. Only one B-channel is initially opened when

Field	Description
	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.

18.1.5 IP Pools

The **IP Pools** menu displays a list of all IP pools.

Your device can operate as a dynamic IP address server for PPP connections. You can use this function by providing one or more pools of IP addresses. These IP addresses can be assigned to dialling-in connection partners for the duration of the connection.

Any host routes entered always have priority over IP addresses from the address pools. This means that, if an incoming call has been authenticated, your device first checks whether a host route is entered in the routing table for this caller. If not, your device can allocate an IP address from an address pool (if available). If address pools have more than one IP address, you cannot specify which connection partner receives which address. The addresses are initially assigned in order. If a new dial-in takes place within an interval of one hour, an attempt is made to allocate the same IP address that was assigned to this partner the previous time.

18.1.5.1 Edit or New

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

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool.
	Secondary: Optionally, enter the IP address of an alternative DNS server.

18.2 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 sec-

tions 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.

18.2.1 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*).

18.2.1.1 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). • `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 iden-

Field	Description
	tification number of the virtual channel. A virtual channel is the logical connection for the transport of ATM cells between two or more points. Note your provider's instructions. 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. • *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

Field	Description
	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*.
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.

Field	Description
	The maximum length of the entry is 45 characters.

Fields in menu Routed Protocols over ATM Settings (appears only for Type = Routed Protocols over ATM)

Field	Description
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 demand, e.g. for Internet access. You'll find additional information on PPP over ATM under *PPPoA* on page 419.

18.2.2 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.

![warning triangle icon] **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.

18.2.2.1 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). 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

Field	Description
	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*.
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*.

18.2.3 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.

18.2.3.1 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

Field	Description
	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 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.

Field	Description
	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 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.
	• $Passive$: The function is disabled.
	Also select whether the test cells of the OAM CC are to be sent or received.

Field	Description
	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.

18.3 Real Time Jitter Control

When telephoning over the Internet, voice data packets normally have the highest priority. Nevertheless, if the upstream bandwidth is low, noticeable delays in voice transmission can occur when other packets are routed at the same time.

The real time jitter control function solves this problem. So that the "line" is not blocked for

too long for the voice data packets, the size of the other packets can be reduced, if required, during a telephone call.

18.3.1 Controlled Interfaces

In the **WAN**->**Real Time Jitter Control**->**Controlled Interfaces** a list of functions is displayed for which the Real Time Jitter Control function is configured.

18.3.1.1 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 19   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.

19.1   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 101). IPSec implementation achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

Additional IPv4 Traffic Filter

bintec elmeg gateways support two different methods of setting up IPSec connections:

• a method based on policies and

• a method based on routing.

The policy-based method uses data traffic filters to negotiate the IPSec phase 2 SAs. This allows for a very "fine-grained" filter to be applied to the IP packet, even at the level of the protocol and the port.

The routing-based method offers various advantages over the policy-based method, e.g., NAT/PAT within a tunnel, IPSec in combination with routing protocols and the creation of VPN backup scenarios. With the routing-based method, the configured or dynamically learned routes are used to negotiate the IPSec phase 2 SAs. Although this method does simplify many configurations, problems may also be caused by competing routes or the "coarser" filtering of data traffic.

The **Additional IPv4 Traffic Filter** parameter fixes this problem. You can apply a "finer" filter, i.e. you can enter the source IP address or the source port. If a **Additional IPv4 Traffic Filter** is configured, this is used to negotiate the IPSec phase 2 SAs; the route now only determines which data traffic is to be routed.

If an IP packet does not match the defined **Additional IPv4 Traffic Filter**, it is rejected.

If an IP packet meets the requirements in an **Additional IPv4 Traffic Filter**, IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

Note

The parameter **Additional IPv4 Traffic Filter** is exclusively relevant for the initiator of the IPSec connection, it is only used for outgoing traffic.

Note

Please note that the phase 2 policies must be configured identically on both of the IPSec tunnel endpoints.

19.1.1 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 622.

19.1.1.1 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. 手 **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

Field	Description
	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.
	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:

Field	Description
	• *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *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 first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used. Note: If you use certificates for authentication and your certificate contains alternative subject names (see *Certificates* on page 101), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.
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 501 menu.
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*

Field	Description
	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 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. 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 501 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 meth-

od 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

Field	Description
	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* 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, pre-defined 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, pre-defined 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 Blow-

Field	Description
	fish/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.
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 dynamic peer configuration on the gateway must not specify a peer ID or a peer IP address. Clients connecting to the gateway, however, must have a peer ID specified in the client peer configuration, since the ID is still used to differentiate the tunnels created via the dynamic peer. The resulting gateway peer would match all incoming tunnel requests. It is, therefore, essential to put it at the end of the IPSec peer list on the gateway. Otherwise all peers that follow the dynamic peer in the peer list would be inactive.
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	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

Field	Description
	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 soon as its connection is available again. |

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. |

Field	Description
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 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

Field	Description
	status of the connection to the IPSec peer is Up (active), i.e. a connection already exists to the IPSec peer.
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 imple-
> mented is activated first by the IPSec Daemon. If IPSec with DynDNS is configured on
> the local device, the own IP address is propagated first and then the ISDN call is sent
> to the remote device. This ensures that the remote device can actually reach the local
> device if it initiates the tunnel setup.

Transfer of IP Address over ISDN

Transferring the IP address of a device over ISDN (in the D channel and/or B channel)
opens up new possibilities for the configuration of IPSec VPNs. This enables restrictions
that occur in IPSec configuration with dynamic IP addresses to be avoided.

> **Note**
>
> To use the IP address transfer over ISDN function, you must obtain a free-of-charge
> extra licence.
>
> You can obtain the licence data for extra licences via the online licensing pages in the
> support section at *www.bintec-elmeg.com* . Please follow the online licensing instruc-
> tions.

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 Pro-
tect 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 462. 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 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.

Field	Description
	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 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".

19.1.2 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.

19.1.2.1 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 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 |

Field	Description
	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 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:

Field	Description
	• *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. 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.

Field	Description
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. 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*

Field	Description
Local ID Value	Only for **Phase-1 (IKE) Parameters** Enter the ID of your device. For **Authentication Method** = *DSA Signature*, *RSA Signature* or *RSA Encryption* the **Use Subject Name from certificate** option is displayed. When you enable the **Use Subject Name from certificate** option, the first alternative subject name indicated in the certificate is used, or, if none is specified, the subject name of the certificate is used. Note: If you use certificates for authentication and your certificate contains alternative subject names (see *Certificates* on page 101), you must make sure your device selects the first alternative subject name by default. Make sure you and your peer both use the same name, i.e. that your local ID and the peer ID your partner configures for you are identical.

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

Field	Description
	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 option is used to carry out a check at certain intervals depending on forthcoming data transfers.
	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

Field	Description
	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*
	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.

19.1.3 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.

19.1.3.1 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.
	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

Field	Description
	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.
	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.

Field	Description
	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	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 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.
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.

19.1.4 XAUTH Profiles

In the **XAUTH Profiles** menu a list of all XAUTH profiles is displayed.

Extended Authentication for IPSec (XAuth) is an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or as a client:

- As a server the gateway requires a proof of authorisation.
- As a client the gateway provides proof of authorisation.

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server. If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

19.1.4.1 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.
Role	Select the role of the gateway for XAuth authentication. Possible values:

Field	Description
	• *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 authentication password (**Password**). Add new members with **Add**.

19.1.5 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.

19.1.5.1 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.

19.1.6 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*. 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 ac-

Field	Description
	tivated.
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	Select whether IKE Initial Contact messages are to be sent dur-

Field	Description
Message	ing 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*. 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.

Field	Description
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.

19.2 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.

19.2.1 Tunnel Profiles

A list of all configured tunnel profiles is displayed in the **VPN**->**L2TP**->**Tunnel Profiles** menu.

19.2.1.1 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 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.

Field	Description
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. 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 resend 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.

19.2.2 Users

A list of all configured interface L2TP partners is displayed in the **VPN**->**L2TP**->**Users** menu.

19.2.2.1 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.
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.

Field	Description
	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*
	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*

Field	Description
	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. 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.

Field	Description
	• *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 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.

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

19.2.3 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.

19.3 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).

19.3.1 PPTP Tunnels

A list of all PPTP tunnels is displayed in the **PPTP Tunnels** menu.

19.3.1.1 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*. 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.
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**

Field	Description
	• *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); 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.)

Field	Description
	• *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 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.

Field	Description
	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 partner 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

Field	Description
	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**.

19.3.2 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.

19.3.3 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.

19.3.3.1 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.

19.4 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.

19.4.1 GRE Tunnels

A list of all configured GRE tunnels is displayed in the **VPN**->**GRE**->**GRE Tunnels** menu.

19.4.1.1 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*.
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 connec-

Field	Description
	tions 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 20   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 515.

20.1 Policies

20.1.1 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.

20.1.1.1 New

> **Note**
>
> Informationen on the selection of Trusted Interfaces can be found here: *IPv4 Filter Rules* on page 503.

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.

20.1.2 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 $\equiv_+$ button to insert another policy above the list entry. The configuration menu for creating a new policy opens.

You can use the $\uparrow_\downarrow$ 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.

20.1.2.1 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*

Field	Description
	Additional services are created in **Firewall**->**Services**->**Service List**.
	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.

20.1.3 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:

Field	Description
	• *All* (default value): All firewall activities are displayed.
	• *Deny*: Only reject and deny events are shown, see "Action".
	• *Accept*: Only accept events are shown.
	• *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. 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 data traffic of this connection will be blocked because the session is interpreted as "incomplete" by the SIF. This will happen even if there is a rule that allows the same kind data traffic in a complete session.
	In order to allow the data traffic of "incomplete" sessions you have to disable **IPv4 Full Filtering**.
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 re-

Field	Description
	garded as expired (in seconds).
	Possible values are *30* to *86400*.
	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.

20.2 Interfaces

20.2.1 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.

20.2.1.1 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.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Selection** column.

20.2.2 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.

20.2.2.1 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.

20.3 Addresses

20.3.1 Address List

A list of all configured addresses is displayed in the **Firewall**->**Addresses**->**Address List** menu.

20.3.1.1 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.

20.3.2 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.

20.3.2.1 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.

20.4 Services

20.4.1 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.

20.4.1.1 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*

Field	Description
	• *Destination unreachable*
	• *Source Quench*
	• *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*

20.4.2 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.

20.4.2.1 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.

20.5 Configuration

20.5.1 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
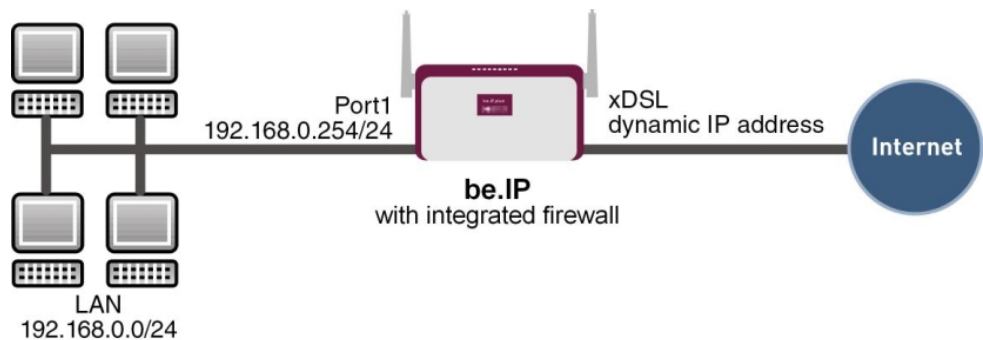
Configuration target

• Only certain Internet services are to be available for the staff of a company (HTTP, HT-

TPS, 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** ->**Ad-**	*Address / Subnet*

Field	Menu	Value
	dress List ->**New**	
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*
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*
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 Filter Rules**-> **New**	*Director*
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 21 Local Services

This menu offers services for the following application areas:

* Name resolution (DNS)
* Configuration via web browser (HTTPS)
* Locating of dynamic IP addresses using a DynDNS provider
* Configuration of gateway as a DHCP server (assignment of IP addresses)
* Automation of tasks according to schedule (scheduling)
* Alive checks for hosts or interfaces, ping tests
* Realtime video/audio conferences (Messenger services, universal plug & play)
* Provision of public Internet accesses (hotspot).
* Start network devices that are switched off via an integrated network card (Wake-On-LAN)

21.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

* DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
* DNS cache, for saving the positive and negative results of DNS requests.
* Static entries (static hosts), to manually define or prevent assignments of IP addresses to names.
* DNS monitoring (statistics), to provide an overview of DNS requests on your device.

Name server

Under **Local Services**->**DNS**->**DNS Servers**->**New** you enter the IP addresses of name servers that are queried if your device cannot answer requests itself or by forwarding entries. Global name servers and name servers that are attached to an interface can both be entered.

Your device can also receive the global name servers dynamically via PPP or DHCP and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

(1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.

(2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(3) Otherwise, if name servers have been entered, taking into account the priority configured and if the relevant interface status is "up", the primary DNS server is queried and then the secondary DNS server. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(5) Otherwise, if overwriting the addresses of the global name servers is allowed in the **WAN**->**Internet + Dialup** menu (**Interface Mode** = *Dynamic*), a connection is set up – if necessary at extra cost – to the first Internet or dialin connection configured to enable DNS server addresses to be requested from DNS servers (**DNS Negotiation** = *Enabled*), if this has not been already attempted. When the name servers have been negotiated successfully, these name servers are then available for more queries.

(6) Otherwise the initial request is answered with a server error.

If one of the DNS servers answers with non-existent domain, the initial request is immediately answered accordingly and a corresponding negative entry is made in the DNS cache of your device.

21.1.1 Global Settings

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*. 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**.

Field	Description
	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 as the name server address. • *DNS Setting* (default value): The addresses of the global name servers entered on your device are sent.

21.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services**->**DNS**->**DNS Servers** menu.

21.1.2.1 Edit or New

Choose the ⌖ icon to edit existing entries. Select the **New** button to set up additional DNS servers.

Here you can configure both global DNS servers and DNS servers that are to be assigned to a particular interface.

Configuring a DNS server for a particular interface can be useful, for example, if accounts with different providers have been set up via different interfaces and load balancing is being used.

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). The pair with the highest priority is used if the interface is "up". Possible values from *0* (highest priority) to *9* (lowest priority). 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

Field	Description
	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. For **Interface Mode** = *Dynamic* A global DNS server is created with the setting *None*. 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 Server	Only if **Interface Mode** = *Static* Enter the IPv6 address of the first name server for Internet address name resolution.
Secondary IPv6 DNS Server	Only if **Interface Mode** = *Static*

Field	Description
	Optionally, enter the IPv6 address of an alternative name server.

21.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services**->**DNS**->**Static Hosts** menu.

21.1.3.1 New

Choose the **New** button to set up new static hosts.

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.
	Possible values:
	• *Negative*: A DNS request for **DNS Hostname** gets a negat-

Field	Description
	ive 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**.

21.1.4 Domain Forwarding

In the **Local Services**->**DNS**->**Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

21.1.4.1 New

Choose the **New** button to set up additional forwardings.

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. If you enter a name without a ".", the entry is supplemented with

Field	Description
	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**.
Interface	Only for **Forward to** = *Interface* Select the interface that has the DNS server assinged which is to receive the DNS requests.
Primary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the primary DNS server.
Secondary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the secondary DNS server.

21.1.5 Dynamic Hosts

In the menu **Local Services**->**DNS**->**Dynamic Hosts**, you can find relevant information on dynamic DNS entries.

21.1.6 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.

21.1.7 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.
Cache Hitrate (%)	Indicates the number of **Cache Hits** pro DNS request in percentage.
Successfully Answered Queries	Shows the number of successfully answered requests (positive and negative).
Server Failures	Shows the number of requests that were not answered by any name server (either positively or negatively).

21.2 HTTPS

You can operate the user interface of your device from any PC with an up-to-date Web browser via an HTTPS connection.

HTTPS (HyperText Transfer Protocol Secure) is the procedure used to establish an encrypted and authenticated connection by SSL between the browser used for configuration and the device.

21.2.1 HTTPS Server

In the **Local Services**->**HTTPS**->**HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

The **Local Services**->**HTTPS**->**HTTPS Server** 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.

21.3 DynDNS Client

The use of dynamic IP addresses has the disadvantage that a host in the network can no longer be found once its IP address has changed. DynDNS ensures that your device can still be reached after a change to the IP address.

The following configuration steps are necessary:

- Registration of a host name at a DynDNS provider
- Configuration of your device

Registration

The registration of a host name means that you define an individual user name for the DynDNS service, e.g. *dyn_client*. The service providers offer various domain names for this, so that a unique host name results for your device , e.g. *dyn_client.provider.com*. The DynDNS provider relieves you of the task of answering all DNS requests concerning the host *dyn_client.provider.com* with the dynamic IP address of your device.

To ensure that the provider always knows the current IP address of your device, your device contacts the provider when setting up a new connection and propagates its present IP address.

21.3.1 DynDNS Update

In the **Local Services**->**DynDNS Client**->**DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed

21.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

The menu **Local Services**->**DynDNS Client**->**DynDNS Update**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host Name	Enter the complete host name as registered with the DynDNS provider.
Interface	Select the WAN interface whose IP address is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.

Field	Description
Provider	Select the DynDNS provider with which the above data is registered. A choice of DynDNS providers is already available in the unconfigured state and their protocols 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. The function is activated by selecting *Enabled*. The function is disabled by default.

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

Fields in the Advanced Settings menu.

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether forwarding of all subdomains of the **Host Name** is to be enabled for the current IP address of the **Interface** (advanced name resolution). The function is activated by selecting *Enabled*. The function is disabled by default.

21.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu.

21.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

The menu **Local Services**->**DynDNS Client**->**DynDNS Provider**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is *80*.
Protocol	Select one of the protocols implemented. Possible values: • *DynDNS* (default value) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit*
Update Interval	Enter the minimum time (in seconds) that your device must wait

Field	Description
	before it is allowed to propagate its current IP address to the DynDNS provider again.

The default value is *300* seconds. |

21.4 DHCP Server

You can configure your device as a DHCP (Dynamic Host Configuration Protocol) server.

Your device and each PC in your LAN requires its own IP address. One option for allocating IP addresses in your LAN is the Dynamic Host Configuration Protocol (DHCP). If you configure your device as a DHCP server, the device automatically assigns IP addresses to requesting PCs in the LAN from a predefined IP address pool.

If a client requires an IP address for the first time, it sends a DHCP request (with its MAC address) to the available DHCP server as a network broadcast.* The client then receives its IP address from bintec elmeg (as part of a brief exchange).

You therefore do not need to allocate fixed IP addresses to PCs, which reduces the amount of configuration work in your network. To do this, you set up a pool of IP addresses, from which your device assigns IP addresses to hosts in the LAN for a defined period of time. A DHCP server also transfers the addresses of the domain name server entered statically or by PPP negotiation (DNS), NetBIOS name server (WINS) and default gateway.

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 541.

21.4.1 IP Pool Configuration

The **Local Services**->**DHCP Server**->**IP Pool Configuration** menu displays a list of all the configured IP pools. This list is global and also displays pools configured in other menus.

21.4.1.1 Edit or New

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

Fields in the menu Basic Parameters

Field	Description
IP Pool Name	Enter any description to uniquely identify the IP pool.
IP Address Range	Enter the first (first field) and last (second field) IP address of the IP address pool.
DNS Server	**Primary**: Enter the IP address of the DNS server that is to be used, preferably, by clients who draw an address from this pool. **Secondary**: Optionally, enter the IP address of an alternative DNS server.

21.4.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured 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.

21.4.2.1 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.

Field	Description
	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. • *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

Field	Description
	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 transmit-

ted.

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.
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.

21.4.3 IP/MAC Binding

The **Local Services**->**DHCP Server**->**IP/MAC Binding** menu displays a list of all clients that received an IP address from your device via DHCP.

You can allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.

Note

You can only create new static IP/MAC bindings if IP address ranges were configured in **Local Services**->**DHCP Server**->**DHCP Pool**, and in the **Local Services**->**DHCP Server**->**IP Pool Configuration** menu is assigned a valid IP Pool.

21.4.3.1 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.

21.4.4 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

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 re-

Field	Description
	quests 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*.

21.4.5 DHCP - Configuration example

Requirements

• An optional DHCP server

Example scenaria

Example scenario as DHCP Server
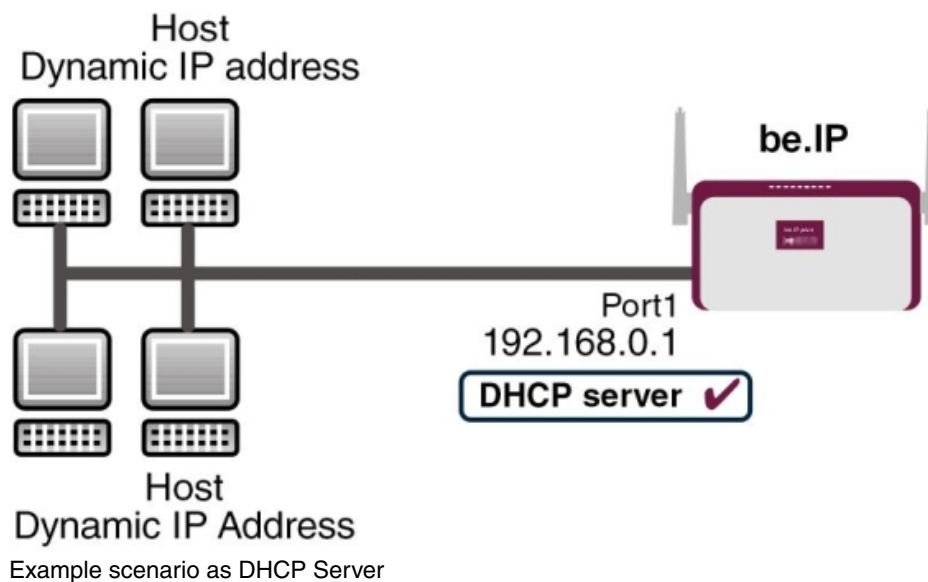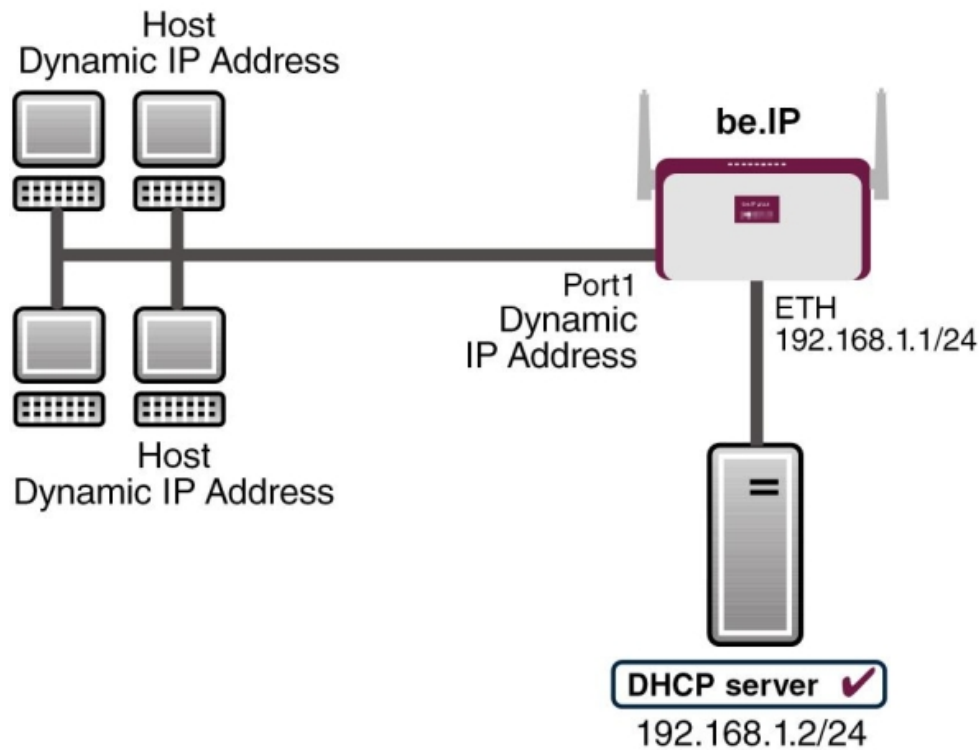
Example scenario as DHCP Client
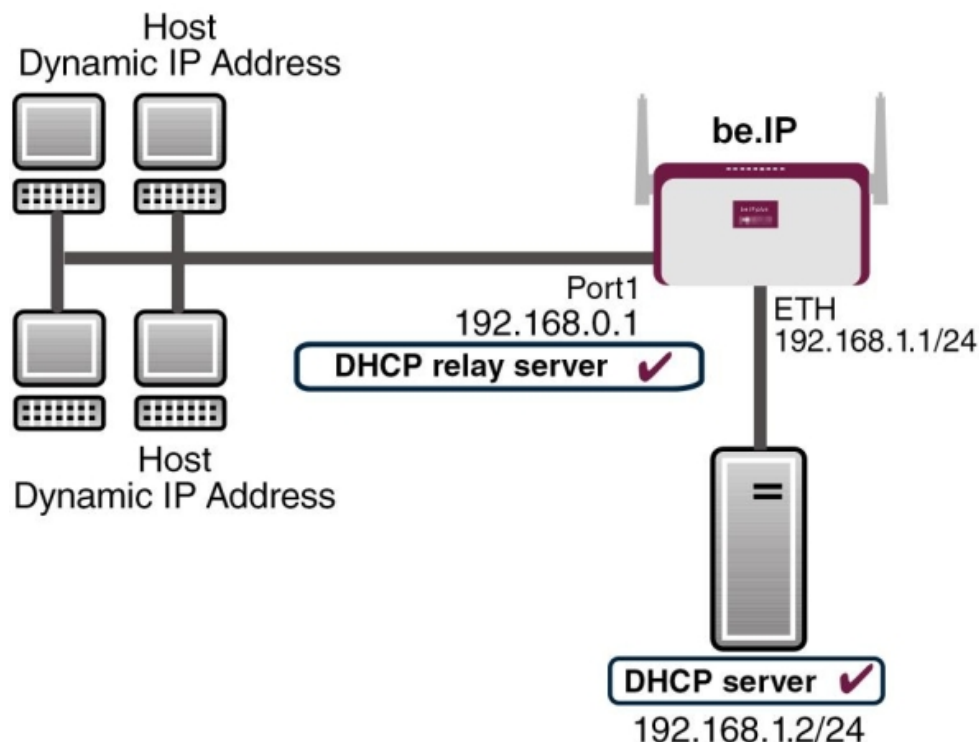
Example scenario as DHCP Relay Server

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

21.5 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**

21.5.1 DHCPv6 Server

Here you can create interface-related address pools and define DHCP options inside of an DHCP Option Set.

21.5.1.1 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.

21.5.2 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

Field	Description
	Search List"). Domain names will be transmitted to the clients in the order defined by the list. The domain name (e.g. dev.bintec.de.) mast end with a dot (.).

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

Fields in the menu Server preference

Field	Description
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

Field	Description
	Server"). Use **Add** to create the desired time server entries.

21.5.3 Stateful Clients

Here you see an entry for each Stateful Client that has contacted the server and has been assigned an IPv6 address.

21.5.4 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.

21.5.4.1 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

Field	Description
	IPv6 address, i.e., the last 64 Bit of the IP address. This prefix must start with ::.

21.6 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.

21.6.1 User

A list of all configured CAPI users is displayed in the **Local Services**->**CAPI Server**->**User** menu.

21.6.1.1 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

Field	Description
	be allowed or denied.
Password	Enter the password which the user **User Name** shall use for identification to gain access to the CAPI service.
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.

21.6.2 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*.

21.7 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 licences. 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 569.

> ⚠️ **Caution**
>
> The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of bintec elmeg gateways. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

> **Note**
>
> To run the event scheduler, the date configured on your device must be 1.1.2000 or later.

21.7.1 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.

21.7.1.1 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. 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 as-

Field	Description
	signed 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 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*

Field	Description
	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. • *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.

Field	Description
	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 operation.
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 until **Destination IP Address** as *Unreacheable* applies. 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

Field	Description
	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 particular 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. De-

Field	Description
	activation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set a **Stop Time** = **Start Time**, the initiator is activated, and deactivated after 10 seconds.

21.7.2 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**.

21.7.2.1 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

Field	Description
	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**.
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:

Field	Description
	• *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**. 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**.

Field	Description
	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: • *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*.

Field	Description
	• *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* 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:

Field	Description
	• *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: • *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*

Field	Description
	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.

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**. |

Field	Description
	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*
	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 until **Destination IP Address** is considered unreachable.
	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.

Field	Description
Local Certificate De-scription	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 protec-ted Certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* 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 certi-ficate	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 con-figuration	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 De-scription	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. *ht-*

Field	Description
	tp://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* 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.

Field	Description
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. • 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.

21.7.3 Options

You configure the schedule interval in the **Local Services**->**Scheduling**->**Options** menu.

The **Local Services**->**Scheduling**->**Options** 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*.
	The value *300* is recommended (5 minute accuracy).

21.7.4 Configuration example - Time-controlled Tasks (Scheduling)

Requirements

• Basic configuration of the gateway.

Example scenario
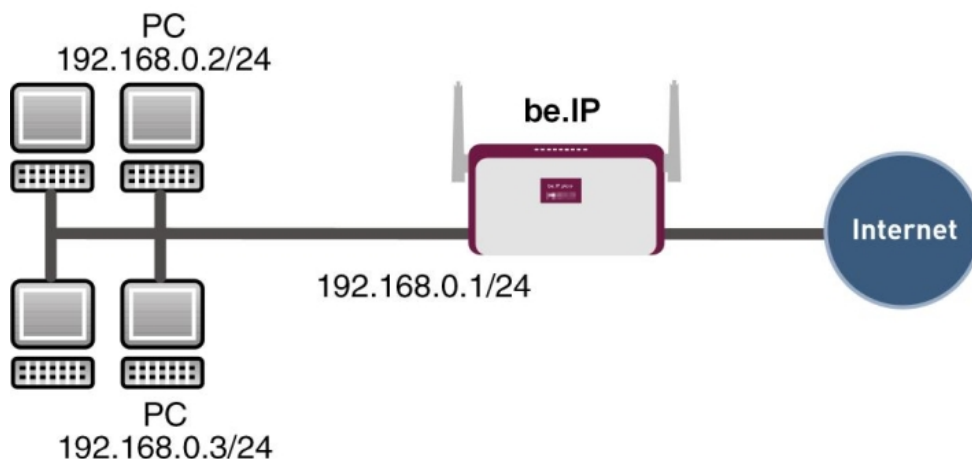
Example scenario Time-controlled Tasks

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*

Field	Menu	Value
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*
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** ->	*Down*

Field	Menu	Value
	Actions -> **New**	
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 config-uration 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 Manage-ment
Event List	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Trigger configuration backup
Event List Condition	**Local Services** -> **Scheduling** -> **Actions** -> **New**	All
Action	**Local Services** -> **Scheduling** -> **Actions** -> **New**	Export configuration
Server URL	**Local Services** -> **Scheduling** -> **Actions** -> **New**	e.g. *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*

Field	Menu	Value
Schedule Interval	**Local Services** -> **Scheduling** -> **Options**	*Enabled*, *55* sec

21.8 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.

21.8.1 Hosts

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Hosts** menu.

21.8.1.1 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.

Field	Description
	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*. 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*.

Field	Description
	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 execute, 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** used in IP Load Balancing.

21.8.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Interfaces** menu.

21.8.2.1 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_.

21.8.3 Ping Generator

In the **Local Services**->**Surveillance**->**Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

21.8.3.1 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 follow-

ing 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 until **Destination IP Address** as *Unreacheable* applies. The default value is *3*.

21.9 UPnP

Universal Plug and Play (UPnP) makes it possible to use current messenger services (e.g. real time video/audio conferencing) as peer-to-peer communication where one of the peers lies behind a NAT-enabled gateway.

UPnP enables (mostly) Windows-based operating systems to take control of other devices with UPnP functionality on the local network. These include gateways, access points and print servers. No special device drivers are needed as known common protocols are used, such as TCP/IP, HTTP and XML.

Your gateway makes it possible to use the subsystem of the Internet Gateway Device (IGD) from the UPnP function range.

In a network behind a NAT-enabled gateway, the UPnP-configured computers act as LAN UPnP clients. To do this, the UPnP function on the PC must be enabled.

The pre-configured port used for UPnP communication between LAN UPnP clients and the gateway is *5678*. The LAN UPnP client acts as a so-called service control point, i.e. it recognizes and controls the UPnP devices on the network.

The ports assigned dynamically by, for example, MSN Messenger, lie in the range from *5004* to *65535*. The ports are released internally to the gateway on demand, i.e. when an audio/video transfer is started in Messenger. When the application is closed, the ports are immediately closed again.

The peer-to-peer-communication is initiated via public SIP servers with only the information from the two clients being forwarded. The clients then communicate directly with one another.

For further information about UPnP, see *www.upnp.org* .

21.9.1 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*. The function is disabled by default.

21.9.2 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*.

21.10 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

21.10.1 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.

21.10.1.1 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** / **Netmask**, 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.

Field	Description
	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: • *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.

Field	Description
	Possible values: • *All*: All clients are approved. • *DHCP Client*: Prevents users who have not received an IP address from DHCP from logging in.
Max. Sessions per User	Enter the maximum number of sessions per user.
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.

21.10.2 Options

In the **Local Services**->**HotSpot Gateway**->**Options** menu, general settings are performed for the hotspot.

The **Local Services**->**HotSpot Gateway**->**Options** menu consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host for multiple loca-tions	If several locations (branches) are set up on the Hotspot server, enter the value of the NAS identifier (RADIUS server parameter) that has been registered for this location on the Hotspot server.

21.11 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**.

21.11.1 Wake-On-LAN Filter

The menu **Local Services**->**Wake-On-LAN**->**Wake-On-LAN Filter** displays a list of all the WOL filters that have been configured.

21.11.1.1 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 of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1*

Field	Description
	• *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 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:

Field	Description
	• *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 pre-fix 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 cor-responding 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 corres-ponding netmask.
Source IPv6 Address/ Length	Enter the source IPv6 address of the data packets and the pre-fix 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 for **Protocol** = *TCP*, *UDP* or *TCP/UDP* Enter a source port number or a range of source port numbers. Possible values:

Field	Description
	• $-All-$ (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. The default value is $Ignore$.

21.11.2 WOL Rules

The menu **Local Services**->**Wake-On-LAN**->**WOL Rules** displays a list of all the WOL rules that have been configured.

21.11.2.1 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.
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.

Field	Description
	• *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.

21.11.3 Interface Assignment

In this menu, the configured rule chains are assigned to individual interfaces which are then monitored for these rule chains.

A list of all configured interface assignments is displayed in the **Local Services**->**Wake-On-LAN**->**Interface Assignment** menu.

21.11.3.1 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.

21.12 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.

21.12.1 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.

21.12.2 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 22 Maintenance

This menu provides you with numerous functions for maintaining your device. It firstly provides a menu for testing availability within the network. You can manage your system configuration files. If more recent system software is available, you can use this menu to install it. If you need other languages for the configuration interface, you can import these. You can also trigger a system reboot in this menu.

22.1 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.

22.1.1 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**.

22.1.1.1 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.

22.2 Diagnostics

In the **Maintenance**->**Diagnostics** menu, you can test the availability of individual hosts, the resolution of domain names and certain routes.

22.2.1 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.

22.2.2 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.

22.2.3 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.

22.3   Software &Configuration

You can use this menu to manage the software version of your device, your configuration files and the language of the **GUI**.

22.3.1   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**. • *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.

Field	Description
	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* 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.

Field	Description
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* 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**.

Field	Description
	• *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.

22.4 Update System Phones

In the **Maintenance**->**Update System Phones** menu, you can update your system telephone software.

> **Note**
>
> Before beginning with the software update of your system telephone, you must load the software in the **Maintenance**->**Update System Phones**->**Firmware Files** menu on your SD card (if supported by you device) or in your system.

22.4.1 elmeg System Phones

In the **Maintenance**->**Update System Phones**->**elmeg System Phones** menu, you will see a list of the connected elmeg system telephones. You can select telephones for immediate updating of the software, or you can have the software updated on a scheduled basis.

In the case of immediate updating, there is no version control.

With time-controlled updating, a check is performed to determine whether a newer version of the system software is saved on the SD card or in your system than on the telephone. It's only in that case that an update takes place. The **Update by time** setting remains after the update has been received, i.e. within the configured period a daily check is performed to determine whether a newer version of the system software is available on the SD card or in your system.

Values in the list elmeg System Phones

Field	Description
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
Serial Number	Displays the system telephone serial number.
Systel Version	Displays the system telephone software version.
Internal Storage Vers.	Displays the inserted SD card version (if supported by you device) or the version stored in internal storage.
Status/Update Status	Displays the system telephone status, or a progress bar during the update progress. ✓ identifies a connected system telephone whose system software is supported by your PABX. ✗ identifies a system telephone that is either not connected, or whose system software is not supported by your PABX. ⏱ identifies an update currently not performed because the maximum number of possible simultaneous updating processes is momentarily exceeded. As soon as another updating process is complete, the telephone is updated in the ⏱ status. For IP telephone, there is no restriction on simultaneous updating of system software. With ISDN telephones, the number of simultaneous updates is dependent on system upgrades. Per digital module, two telephones can be simultaneously updated. If the system telephone system software is not supported by your PABX, there is still a way to update the system software. During system software updating, you see a progress bar.
Update by time	Displays whether, at a certain point, the system telephone software should be updated. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the

Field	Description
	devices displayed.
Update immediately	Displays whether the system telephone software should be updated immediately.
	This function is enabled on an individual device by setting a checkmark. The function is disabled by default.
	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

22.4.2 elmeg OEM

In the **Maintenance**->**Update System Phones**->**elmeg OEM** menu, you will see a list of the connected elmeg OEM telephones or base stations. This view displays both elmeg IP1x telephones and elmeg DECT base stations, if there are any. You can select devices to have their software updated immediately or allow them to download completely new software from the system.

In the case of immediate updating, there is no version control.

> **Note**
>
> Note that immediate software updates for DECT multi-cell systems are only available via the system's web configurator and that they cannot be initiated by the PABX GUI.

Values in the list Update from internal Server

Field	Description
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
MAC Address	Shows the system telephone's MAC address.
Phone Version	Displays the software version of the telephone.
Internal Storage Vers.	Displays the inserted SD card version (if supported by you device) or the version stored in internal storage .
Status/Update Status	Displays the system telephone status, or a progress bar during

Field	Description
	the update progress.
	✅ identifies a connected system telephone whose system software is supported by your PABX.
	❌ identifies a system telephone that is either not connected, or whose system software is not supported by your PABX.
	For IP telephone, there is no restriction on simultaneous updating of system software.
	If the system telephone system software is not supported by your PABX, there is still a way to update the system software.
	During system software updating, you see a progress bar.
Update enabled	Shows whether connected telephones can independently download new software from the system.
	You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button or the **Deselect all** button.
Update by time	Displays whether, at a certain point, the system telephone software should be updated.
	This function is enabled on an individual device by setting a checkmark. The function is disabled by default.
	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.
Update immediately	Displays whether the system telephone software should be updated immediately.
	This function is enabled on an individual device by setting a checkmark. The function is disabled by default.
	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

Values in the list Update from external Server

Field	Description
Automatic Update from external Server	Enable or disable the automatic update from external server function. The function is enabled with *Enabled*. The function is enabled by default.
Description	Displays the description entered for the system telephone.
Phone Type	Displays the system telephone type.
MAC Address	Shows the system telephone's MAC address.
Phone Version	Displays the software version of the telephone.
Status	Displays the system telephone status, or a progress bar during the update progress. identifies a connected system telephone whose system software is supported by your PABX. identifies a system telephone that is either not connected, or whose system software is not supported by your PABX.
Update immediately	Displays whether the system telephone software should be updated immediately. This function is enabled on an individual device by setting a checkmark. The function is disabled by default. You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

22.4.3 Firmware Files

In the **Maintenance**->**Update System Phones**->**Firmware Files** menu, you see the system software files that are currently available on your SD card (if supported by you device) or into the internal storage. You can load additional files on the SD card or into the internal storage.

> **Note**
>
> You will find current system software files in the download area, at
> *www.bintec-elmeg.com* .
>
> For DECT systems there is a ZIP file available which contains the system software
> files and, for **elmeg DECT150**, language files too.

> **Note**
>
> One version of the system software file per telephone type can be saved on the SD
> card or into the internal storage.

Values in the list Firmware Files

Field	Description
Load firmware	Save the system software files on your SD card (if supported by you device) or into the internal storage.
No.	Displays the serial number of the system software file.
Phone Type	Displays the system telephone type.
Version	Displays the version of the system software.
Status	● indicates that a system software file is saved in the correct directory.

22.4.4 Settings

In the **Maintenance**->**Update System Phones**->**Settings** menu, you can set a period for
the time-dependent updating of the system software. You can save a telephone number
that may be used in case a system software update has failed. You can dial this number
with the telephone in order to update the system software once the telephone is in boot
mode following a failed update.

The **Maintenance**->**Update System Phones**->**Settings** menu consists of the following
fields:

Fields in the menu Time Settings for System Phone Firmware Update

Field	Description
Internal Number	For ISDN system telephones only
	Enter the number of the PABX update server that you wish to call from the telephone if the system software update fails. In this case, you can perform the update from the telephone.
	This number is automatically sent to the system telephone when the telephone logs into the PABX.
	When it has been sent, the number is displayed on the telephone under **Menu**->**Service**->**Software Update**. If you press the **OK** button, the number is available in redial.
Firmware Update	Set a period for updating the system software. To do this, select the **Start Time** and the **Stop Time**.
ISDN Remote Access	Select whether a ISDN remote access shall be permitted on your system.
	The function is enabled with *Enabled*
	The function is disabled by default.

22.5 Reboot

22.5.1 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.

22.6 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 23 External Reporting

In this system menu, you define what system protocol messages are saved on which computers, and whether the system administrator should receive an e-mail for certain events. Information on IP data traffic can also be saved--depending on the individual interfaces. In addition, SNMP traps can be sent to specific hosts in case of error.

23.1 Syslog

Events in various subsystems of your device (e.g. PPP) are logged in the form of syslog messages (system logging messages). The number of messages visible depends on the level set (eight steps from *Emergency* over *Information* to *Debug*).

In addition to the data logged internally on your device, all information can and should be transmitted to one or more external PCs for storage and processing, e.g. to the system administrator's PC. The syslog messages saved internally on your device are lost when you reboot.

> ⚠️ **Warning**
>
> Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon

All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Demon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (can be called in the download area at *www.bintec-elmeg.com*).

23.1.1 Syslog Servers

Configure your device as a syslog server so that defined system messages can be sent to suitable hosts in the LAN.

In this menu, you define which messages are sent to which hosts and with which conditions.

A list of all configured system log servers displayed in the **External Reporting**->**Syslog**->**Syslog Servers** menu.

23.1.1.1 New

Select the **New** button to set up additional syslog servers.

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*

23.2 IP Accounting

In modern networks, information about the type and number of data packets sent and received over the network connections is often collected for commercial reasons. This information is extremely important for Internet Service Providers that bill their customers by data volume.

However, there are also non-commercial reasons for detailed network accounting. If, for example, you manage a server that provides different kinds of network services, it is useful for you to know how much data is generated by the individual services.

Your device contains the IP Accounting function, which enables you to collect a lot of useful information about the IP network traffic (each individual IP session).

23.2.1 Interfaces

In this menu, you can configure the IP Accounting function individually for each interface.

In the **External Reporting**->**IP Accounting**->**Interfaces** menu, a list of all interfaces configured on your device is shown. For each entry, you can activate IP Accounting by setting the checkmark. In the **IP Accounting** column, you do not need to click each entry individually. Using the options **Select all** or **Deselect all** you can enable or disable the IP accounting function for all interfaces simultaneously.

23.2.2 Options

In this menu, you configure general settings for IP Accounting.

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
%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]*

23.3 Alert Service

It was previously possible to send syslog messages from the router to any syslog host. Depending on the configuration, e-mail alerts are sent to the administrator as soon as relevant syslog messages appear.

23.3.1 Alert Recipient

A list of Syslog messages is displayed in the **Alert Recipient** menu.

23.3.1.1 New

Select the **New** to create additional alert recipients.

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. 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.

Field	Description
	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 Slave 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. 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*.

Field	Description
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.

23.3.2 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.
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.

Field	Description
	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. 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*.

23.4 SNMP

SNMP (Simple Network Management Protocol) is a protocol from the IP protocol family for transporting management information about network components.

Every SNMP management system contains an MIB. SNMP can be used to configure, control and administrate various network components from one system. Such an SNMP tool is included on your device: the Configuration Manager. As SNMP is a standard protocol, you can use any other SNMP managers, e.g. HPOpenView.

For more information on the SNMP versions, see the relevant RFCs and drafts:

- SNMP V. 1: RFC 1157
- SNMP V. 2c: RFC 1901 - 1908
- SNMP V. 3: RFC 3410 - 3418

23.4.1 SNMP Trap Options

In the event of errors, a message - known as a trap packet - is sent unrequested to monitor the system.

In the **External Reporting**->**SNMP**->**SNMP Trap Options** menu, you can configure the sending of traps.

The menu **External Reporting**->**SNMP**->**SNMP Trap Options** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
SNMP Trap Broadcast-ing	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*. 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.

Field	Description
	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*.

23.4.2 SNMP Trap Hosts

In this menu, you specify the IP addresses to which your device is to send the SNMP traps.

In the **External Reporting**->**SNMP**->**SNMP Trap Hosts** menu, a list of all configured SNMP trap hosts is displayed.

23.4.2.1 New

Select the **New** button to create additional SNMP trap hosts.

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.

23.5 SIA

23.5.1 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 24 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.

24.1 Status Information

This menu displays current settings for terminals and team subscribers. This data is continuously read out.

24.1.1 Users

In the **Monitoring**->**Status Information**->**Users** menu, current settings for a user's internal number (MSN) are displayed.

24.1.1.1 Users - Details

By pressing the Q button, you display detailed statistics on the respective user.

Values in the Extension Status list

Field	Description
Number	Displays the user's internal number.
Name	Displays the name assigned to the user. If a voicemail system is active, *Voice Mail System* is displayed.
Current Class of Service	Displays the all of the authorisation classes assigned to the user. The currently enabled authorisation class is marked appropriately with a green arrow ( ).
Terminal	Displays the interface assigned to this subscriber.
Charges	Displays calculated charges for accrued connection units.
Status	Displays the status of the interface to which the subscriber is connected.

Values in the System Settings list

Field	Description
Parallel Ringing	Displays whether parallel call is set up for the user.

Field	Description
Call Forwarding	Displays current call forwarding for this user.
Do not Disturb	Displays whether call waiting protection is set up for the user. (Only for system telephones)
Call Waiting	Displays whether call waiting is allowed for internal and/or external calls.
Direct Call	Displays whether direct call on receiver pickup is configured for the user.
Room Monitoring	Displays whether room monitoring is enabled for the user.
Receive Announcement Calls	Displays whether the announcement is allowed for the user.
Receive Intercom Calls	Displays whether simplex operation is allowed for the user.
Automatic Call Pick-up	Displays whether automatic call acceptance is configured for the user.

24.1.2 Teams

In the **Monitoring**->**Status Information**->**Teams** menu, current team settings are displayed.

24.1.2.1 Teams - Details

By pressing the $_Q$ button, you display detailed statistics for the respective team.

Values in the Team Status list

Field	Description
Name	Displays the name assigned to the team.
Number	Displays the team's internal number.
Users assigned/Users logged on	Displays the users assigned to the team, and how many of these users are logged in.
Call Forwarding	Displays current call forwarding for this team.

Values in the System Settings list

Field	Description
Active Variant (Day)	Displays the currently enabled call option for this team.
Switch call signalling	Displays whether the call option can be switched manually, over the calendar or manually and over the calendar.
Signalling	Displays the type of call signalling in the team.

Field	Description
Busy on busy	Displays whether busy on busy is configured for the team.
Automatic Call Pick-up	Displays whether automatic call acceptance is configured, and which melody is played.
Rerouting on no response	Displays whether redirect on no reply is enabled and, if so, the time period after which it occurs and the destination team.
Further Rerouting	Displays which of the redirect functions are enabled and which subscriber is the redirect destination.

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

Values in the Advanced Settings list

Field	Description
Assigned Users	Displays all logged-in and logged-out subscribers in the team.

24.2 Internal Log

24.2.1 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.

24.3 IPSec

24.3.1 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.
Remote Networks	Displays the currently negotiated subnets of the remote terminal.
Security Algorithm	Displays the encryption algorithm of the IPSec tunnel.
Status	Displays the operating status of the IPSec tunnel.
Action	Enables you to change the status of the IPSec tunnel as displayed.
Details	Opens a detailed statistics window.

You change the status of the IPSec tunnel by clicking the ∧ button or the ∨ button in the
Action column.

By clicking the ⚲ button, you display detailed statistics on the IPSec connection.

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.

Field	Description
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** / **Life-time remaining** / **Status**	The parameters of the IKE (Phase 1) SAs are displayed here.
IPSec (Phase-2) SAs (x) **Role** / **Algorithm** / **Life-time remaining** / **Status**	Shows the parameters of the IPSec (Phase 2) SAs.
Messages	The system messages for this IPSec tunnel are displayed here.

24.3.2 IPSec Statistics

In the **Monitoring**->**IPSec**->**IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

The **Monitoring**->**IPSec**->**IPSec Statistics** menu consists of the following fields:

Fields in the Licences menu

Field	Description
IPSec Tunnels	Shows the IPSec licences currently in use (**In Use**) and the maximum number of licenses usable (**Maximum**).

Fields in the Peers menu

Field	Description
Status	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.
Passed	Shows the number of incoming (**In**) or outgoing (**Out**) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (**In**) or outgoing (**Out**) packets.
Encrypted	Shows the number of all incoming (**In**) or outgoing (**Out**) packets protected by IPSec.
Errors	Shows the number of incoming (**In**) or outgoing (**Out**) packets for which processing led to errors.

24.4 Interfaces

24.4.1 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 ∨ 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.

Field	Description
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Click the Q 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.

24.4.2 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.

24.5 Bridges

24.5.1 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.

24.6 HotSpot Gateway

24.6.1 HotSpot Gateway

A list of all linked hotspot users is displayed in the **Monitoring**->**HotSpot Gateway**->**HotSpot Gateway** menu.

Values in the HotSpot Gateway list

Field	Description
User Name	Displays the user's name.
IP Address	Shows the IP address of the user.
Physical Address	Shows the physical address of the user.
Logon	Displays the time of the notification.
Interface	Shows the interface used.

24.7 QoS

In the **Monitoring**->**QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

24.7.1 QoS

A list of all interfaces for which QoS was configured is displayed in the **Monitoring**->**QoS**->**QoS** menu.

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.

Chapter 25   User Access

The system administrator can set up an individual configuration access interface for the users. You, the user, can thus display your most important personal settings and individually customise some of these.

To log in to the configuration interface with your assigned access data, enter your **User Name** and **Password** in the login window.

After successful login, the **Status** page is displayed. It includes an overview of your most important settings.

In the **Phonebook** menu, you can access the **System Phonebook** and create, edit as well as delete entries in a user-specific telephone book.

In the **Call Data Records** menu, you get a detailed overview of the calls you have conducted and accepted.

The **Settings** menu contains an overview of current settings of performance features **Direct Call**, **Call Forwarding** and **Parallel Ringing**. You can individually customise these here. In addition, you can view general settings and customise access and contact data.

You can also view the settings of the **elmeg System Phones** assigned to you, and modify these to your needs.

In the **Voice Mail System**->**Settings** menu, you'll see the current configuration of your individual voicemail box, as well as the number of messages present. You can modify several frequently used voicemail box parameters here. The **Voice Mail System**->**Messages** menu displays a detailed overview of all received calls.

25.1   Status

The **User Access**->**Status** menu displays the most important settings performed for you by the system administrator.

The **User Access**->**Status** menu consists of the following fields:

Values in the User Data list

Field	Description
Name, First Name	Displays the configured surname and name, if applicable, of your user.

Field	Description
Description	Displays the configured additional description for your user.

Values in the Internal Numbers &Communication Cost list

Field	Description
<Internal Number>	Displays the connection charges for the internal numbers assigned to your user.

Values in the Further Settings list

Field	Description
Current Class of Service	Displays the name of the authorisation class to which your user is assigned.
Dialling Authorization	Displays the dial permission for your telephones. This derives from the setting for the corresponding user class. Possible values: • *International*: The telephones have unrestricted dialling authorisations and can initiate all connections. • *National*: The telephones can initiate all calls except international calls. If a number starts with the code for international dialling, the number cannot be dialled. • *Incoming*: The telephones can receive incoming external calls, but cannot initiate any external calls. Internal calls are possible. • *Region*: The telephones cannot make any national or international calls. For this dial permission, 10 exception numbers allowing national or international dialling can be configured. An exception number can consist of complete call numbers or sections thereof (e. g. the first numerals). • *Local*: The telephones can make local calls. National and international calls are not possible. • *Internal*: The telephones do not have authorisation for incoming or outgoing external calls. Only internal telephone calls are possible.
Allow manual trunk group selection	Indicates whether your user is assigned to an authorisation class for which manual bundle assignment is allowed. If so, authorised bundles or external connections are displayed.

Field	Description
	Besides general exchange access, a telephone can also select-ively use a bundle. Here an external connection is initiated with the corresponding code for the target assignment of the bundle and not by dialling the dialling code.
	To be able to perform a selective bundle assignment, the au-thorisation class must possess the appropriate authorisation. The authorisation can also include bundles that the authorisa-tion class can otherwise not assign. If a telephone does not pos-sess the authorisation for selective bundle assignment, or if the selected bundle is in use, the busy tone is heard after dialling the code. If **Automatic Outside Line** is set up for an authorisa-tion class, users of this authorisation class must press the star key before selective bundle assignment, then initiate external di-alling with the code for bundle assignment.
Pick-up Group	Displays the number of the group in which calls may be picked up.

25.2 Phonebook

In the **Phonebook** menu, telephone book entries are displayed separately according to **System Phonebook** and **User Phonebook**. In **User Phonebook** the user can create, modify or delete up to 50 own entries. These entries can only be viewed by the respective user. These entries are updated via the **GUI**.

25.2.1 System Phonebook

In the **System Phonebook**, entries of the overall system created by the administrators are displayed You cannot modify these.

Values in the System telephone book list

Field	Description
Description	Displays the subscriber's description. The **System Phonebook** is sorted according to these entries.
Phone Number	Displays the telephone number.
Speed Dial Number	Displays the speed-dial number.

Field	Description
Call Through	Indicates whether the telephone number for the **Call Through** function is activated.

25.2.2 User Phonebook

In the **User Phonebook**, your user entries are displayed. You can add, edit or delete entries.

25.2.2.1 Edit or New

Choose the ✏ icon to edit existing entries. Select the **New** button to create new entries.

The menu **User Access**->**Phonebook**->**User Phonebook**->**New** consists of the following fields:

Fields in the Phonebook Entry menu.

Field	Description
Description	Enter a description for the entry. Sorting in **User Phonebook** follows the initial letters of the entry.
Phone Number	Enter the telephone number (internal or external).

25.3 Call Data Records

The **Call Data Records** menu displays your user's incoming and outgoing connections recorded to date.

25.3.1 Outgoing

The **Call Data Records**->**Outgoing**menu consists of the following fields:

Values in the Outgoing list

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.

Field	Description
Duration	Displays the duration of the connection.
User	Displays the user who called.
Int. No.	Displays the user's internal number.
Called Number	Displays the dialled number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the external connection was routed.
Costs	Displays the connection charge, but only if the provider transmits the corresponding data.

25.3.2 Incoming

The **Call Data Records**->**Incoming** menu consists of the following fields:

Values in the Incoming list

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Duration	Displays the duration of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
External Number	Displays the caller's number.
Project Code	Displays the call project number, if any.
Interface	Displays the interface over which the connection from outside was routed.

25.4 Call List

The menu **Applications**->**Call List** lists details of incoming and outgoing calls. Which kind of calls and how many of them are included can be spcified in the submenu **General**.

25.4.1 Incoming

The **Applications**->**Call List**->**Incoming** menu contains information that permits the monitoring of incoming activities.

The **Applications**->**Call List**->**Incoming** menu consists of the following fields:

Fields in the Incoming menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
Int. No.	Displays the user's internal number.
Caller Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

25.4.2 Outgoing

The **Applications**->**Call List**->**Outgoing** menu contains information that permits the monitoring of outgoing activities.

The **Applications**->**Call List**->**Outgoing** menu consists of the following fields:

Fields in the Outgoing menu

Field	Description
Date	Displays the connection date.
Time	Displays the time at call start.
Type	Displays the type of the connection.
User	Displays the user who was called.
Int. No.	Displays the user's internal number.
Called Number	Displays the caller's number.
Trunk Number	Displays the port number.
Interface	Displays the interface over which the connection from outside was routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

25.5 Settings

In the **Settings** menu, you can perform personal settings to performance features direct call, call forwarding (CF), parallel call and do not disturb, as well as customise general settings.

25.5.1 Feature Settings

In the **Settings**->**Feature Settings** menu, the settings for performance features direct call, call forwarding (CF), parallel call and do not disturb can be customised.

25.5.1.1 Call Forwarding

In the **Settings**->**Feature Settings**->**Call Forwarding** menu, you configure forwarding of incoming calls to your internal number onto the entered destination number.

You are temporarily away from your office, but don't want to miss a call. With call forwarding to another number, e.g. your mobile, you can receive your calls even when you are not at your desk. You can forward calls on your number to any call number. It can occur *Imme-*

diately, *On no reply* or *On Busy*. Call forwarding *On no reply* and *On Busy* can exist concurrently. If you are not near your telephone, for example, the call is forwarded to another number (e.g. your mobile phone) after a short period. If you are making a call at your desk, other caller may receive the busy signal. You can forward these callers e.g. to a colleague or the secretary by using call forwarding on busy.

Calls can be forwarded to internal subscriber numbers, internal team numbers or external numbers When the number to which calls shall be forwarded is entered, the system automatically checks whether it's an internal or external number.

To continue with configuring, click the ✎ symbol.

Select the 📠 button to go to the **IP1x0** telephone user interface administrator page. This is described in the telephone user guide!

The **Settings**->**Feature Settings**->**Call Forwarding** menu consists of the following fields:

Fields in the Call Forwarding menu.

Field	Description
Active Function	Select whether to enable the call forwarding (CF) function for your telephone. The function is enabled with *Enabled* The function is disabled by default.
Type	Select when incoming calls shall be forwarded to the specified internal number. Possible values: • *Immediately* • *On Busy* • *On no reply* (default value) • *On busy / On no reply*
Destination on no Reply	Enter the number to which incoming calls shall be forwarded after time.
Destination on Busy	Enter the number to which incoming calls shall be forwarded on busy.
Destination immediately	Enter the number to which incoming calls shall be forwarded immediately.

25.5.1.2 Parallel Ringing

In the **Settings**->**Feature Settings**->**Parallel Ringing** menu, you configure which calls should be signalled to your terminal.

The **Settings**->**Feature Settings**->**Parallel Ringing** menu consists of the following fields:

Fields in the Parallel Ringing menu.

Field	Description
Active Function	Select whether to enable the parallel call function for your telephone. The function is enabled with *Enabled* The function is disabled by default.
External Number	Under *Individual Number* enter the external telephone number to which a call should be signalled in parallel. If a mobile number and a call number are configured for personal use, these are displayed in *Configured Home Number* or *Configured Mobile Number* and can be selected.

25.5.1.3 Direct Call

You wish to install your telephone in such a way that connection to a specific call number is set up even without entry of the number (e. g. emergency phone). You are not at home. However, there is someone at home who needs to be able to reach you quickly and easily by telephone if necessary (e. g. children or grandparents). If you have set up the Direct Call function for your telephone, the telephone receiver only needs to be picked up. After a time period without further entries set in configuration, the system automatically dials the configured direct call number.

If you do not dial within the specified period from picking up the receiver, automatic dialling is initiated.

The **Settings**->**Feature Settings**->**Direct Call** menu consists of the following fields:

Fields in the Direct Call menu.

Field	Description
Active Function	Select whether to enable the direct call function for your telephone.

Field	Description
	The function is enabled with *Enabled* The function is disabled by default.
Number	Select which number to use for direct call. Possible values: • *Preconfigured Number*: Select the desired number for which to set up direct call from the dropdown list. • *Invidual Number*: Enter the desired number for which to set up direct call into the input field.

25.5.1.4 Do not Disturb

You can use the "station guarding" (do not disturb) feature to configure which calls will be signalled to your terminal.

The **Settings**->**Feature Settings**->**Do not Disturb** menu consists of the following fields:

Fields in the menu Do not Disturb

Field	Description
Active Function	Select whether to enable the "station guarding" function for your telephone. The function is enabled with *Enabled*. The function is disabled by default.
Do not Disturb	With the station guarding feature, you can enable call signalling to your terminal. Analogue terminals use system code numbers for this. Select the calls for which you wish to use the feature. Possible values: • *Internal Calls not signaled* • *External Calls not signaled* • *No Calls signaled*

25.5.1.5 Log on / Log off

With system telephones, it is only possible to log out of a team using the **Log on / Log off** function key. The team administrator must run this function manually if standard telephones are used.

The **Settings**->**Feature Settings**->**Log on / Log off** menu consists of the following fields:

Fields in the menu Log on / Log off

Field	Description
Description	Shows which teams the user belongs to.
Status	Select whether the team member shall be logged in or out of the team. The function is activated by selecting *Logged on*. The function is enabled by default.

25.5.2 General Settings

Your user's most important settings are listed in the **Settings**->**General Settings** menu. Personal access data (configuration password, IP phone password) as well as mobile and home office numbers can be customised.

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

Fields in the User Data menu.

Field	Description
Name	Displays your user's name.
Description	Displays the additional description for your user.
Login Name	Displays your user name for login to the user configuration interface.
Password for HTML Configuration Access	If you wish to change your password for access to the user configuration interface, enter a new password here. To check, you can display the password in plain text by clicking the **Show** option.

Field	Description
Password for IP Phone Registration	If you wish to change your password for IP telephone login, enter a new password here. To check, you can display the password in plain text by clicking the **Show** option.
PIN for Phone Access	If you wish to change the PIN for your personal voicebox, enter a new PIN here. To check, you can display the password in plain text by clicking the **Show** option.
Mobile Number	Here, you can enter the mobile number under which you can be reached.
Home Office Number	Here, you can enter the home office number under which you can be reached.
Busy on busy	Indicates whether performance feature Busy on Busy is enabled for the currently selected user.
	If a subscriber for whom multiple telephone numbers have been configured makes a call, you can decide whether additional calls for this user shall be signalled. If "Busy on Busy" is set for this user, other callers get an **Engaged** signal if the user is calling on one of her numbers.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.

Fields in the Status Information menu.

Field	Description
Extension Numbers	Displays the internal numbers assigned to you.
Current Class of Service	Displays the authorisation class to which you're currently assigned.
Dialling Authorization	Displays your dial permission.
Allow manual trunk group selection	Displays whether you're allowed to assign additional bundles to outside lines and, if so, which.
Pick-up Group	Displays the number of the group in which calls may be picked up.

25.6 Assigned elmeg Phones

The **Assigned elmeg Phones** menu shows the telephones that the system administrator has assigned to you.

> **Note**
>
> The **Assigned elmeg Phones** menu is only displayed if you've already been assigned system telephones by the administrator.

25.6.1 Assigned elmeg Phones

The **Assigned elmeg Phones**->**Assigned elmeg Phones** menu shows a list with the key information about your telephone. The [≡] symbol takes you to the **IP1x0** phone's configuration interface.

Select the ✎ symbol to reset the phone's user password.

The **Assigned elmeg Phones**->**Assigned elmeg Phones** ✎ menu consists of the following fields:

Fields in the System Phone menu

Field	Description
User password	Select whether the user password should be reset.
	The function is activated by selecting *Enabled*.
	The function is disabled by default.
	As soon as you select the **OK** button, the password is reset to the default setting.

25.7 elmeg System Phones

The menu **elmeg System Phones** displays the system telephones assigned to you by the system administrator.

Note

The **elmeg System Phones** menu is only displayed if you've already been assigned system telephones by the administrator.

25.7.1 Assigned System Phones

The system telephone offers typical system performance features associated with bintec elmeg systems. For example:

* Dialling from the system phone book
* Announcement and simplex operation with other system telephones on the system
* Function keys for control of system performance features (enable call options, login/ logout in teams, line keys, connection keys). The status of defined performance features can be indicated via LED's assigned to individual function keys.

Note

Configuration modifications are transmitted to the system telephones at the earliest 30 seconds after confirming the modification with the **Apply** button.

25.7.1.1 Settings

In the **elmeg System Phones**->**Assigned System Phones**->**Settings** you can release specific performance features and functions for your system telephone.

The **elmeg System Phones**->**Assigned System Phones**->**Settings** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Headset Support	Not for **S530** and **S560**. Select whether the headset should automatically accept calls.

Field	Description
	Note If you wish to use a headset, you must configure a headset key and a key for automatic call acceptance on your PABX system. On the system telephone, you must select a headset type and enable the key for automatic call acceptance.
Call Waiting	Select whether another call shall be supported for this telephone through call waiting or a display notification. The function is activated by selecting *Enabled*. The function is disabled by default. If **Call Waiting** is enabled, define for which calls you wish to allow call waiting. Possible values: • *Internal Calls* • *External Calls* • *Internal and External Calls* Under **Repeat Call Waiting Signal**, also decide whether the call waiting tone or the display notification should only be signalled once, or repeated.
Do not Disturb	Only for telephones in the **CS4xx** series, the **S530** telephones and **S560** and the **IP-S400** telephone. For the **S530** and **S560** telephones, you merely configure the function here. With these telephones, enable *Do not Disturb* via the function key. Select whether you wish to use the call protection (do not disturb) performance feature. With this performance feature, you can enable call signalling to your terminal. Select for which number you wish to use the station guarding performance feature. Possible values:

Field	Description
	• *First Number only* (**CS4xx** series only): Call protection applies only to the first configured MSN.
	• *All Numbers* (**CS4xx** series only): Call protection applies to all configured MSN's.
	Select whether incoming calls shall be signalled:
	• *Off*: Calls are signalled.
	• *On* (**CS4xx** series only): Calls are not signalled.
	• *Acknowledgement Tone only* (**CS4xx** series only): An attention tone is heard once for a call
	• *Attention tone 1* (only **S530** and **S560**)
	• *Attention tone 2* (only **S530** and **S560**)
	• *Attention tone 3* (only **S530** and **S560**)
	• *Attention tone 4* (only **S530** and **S560**)
	• *No attention tone* (only **S530** and **S560**)

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

Fields in the menu Advanced Settings

Field	Description
Status LED	Select whether and, if so, which events should be signalled by the system telephone status LED.
	Possible values:
	• *Off*: The status LED function is not used.
	• *Caller List*: The status LED signals calls and new messages.
	• *Messages only*: The status LED only signals new messages (MWI).
	• *New Message* (only **S5x0**)
	• *New Call* (only **S5x0**)
	• *Active Call* (only **S5x0**)
	You can use the options *New Message*, *New Call* and *Active Call* individually, or combine them freely.
Directory Softkey	Only for telephones in the **CS4xx** series

Field	Description
	Select whether calls shall be made with the softkey entries from the system phone book (*System*) or from the telephone phone book (*Telephone*).
Conversation Display	Not for **S5x0**
	Select which information shall be indicated in the system telephone display during a call.
	Possible values:
	• *Number and Charge or Duration*
	• *Number and Charge*
	• *Number and Duration*
	• *Number and Time*
	• *Number only*
	• *Date and Time only*
Default Signalling during Calls	Select whether DTMF signals or keypad functions shall be transmitted into the system in call status. You can use special functions during a call by entering character and numerical sequences. These entries must be made as keypad or MFV sequences, depending on the function to be used. You can define whether MFV or keypad functions are possible in the basic setting during a call.
	Possible values:
	• *DTMF* (default value)
	• *Keypad*
Automatic Call Pick-up	Select the period after which calls to this system telephone should be automatically accepted without you having to pick up the receiver or press the loudspeaker key. *Please note that to be able to use this function at least one telephone key must be assigned to automatic call acceptance.*
	Possible values:
	• *Immediately*
	• *After 5 seconds*

Field	Description
	• *After 10 seconds* • *After 15 seconds* (only **S5x0**) • *After 20 seconds* (only **S5x0**) • *Off* (only **S5x0**)
Mute after hands-free Calling	Not for **S5x0**, **CS290**, **CS290-U** You can dial the number of a subscriber without picking up the receiver (e. g. hands-free). Here, you have the choice of whether the built-in microphone shall be switched on immediately or only after pressing of the corresponding softkey. If the microphone is turned off during dialling, the corresponding softkey must be pressed, even if the connection is already active. The function is activated by selecting *Enabled*. The function is disabled by default.
Receiving UUS	Select whether performance feature UUS (User to User Signalling) can be used for this telephone. With this performance feature, you can receive short text messages from other telephones. In this way, you can send written information within the system, e. g. *Meeting at 9:30 AM* or *Will be on holiday on Monday*. Possible values: • *Off, UUS are blocked*: The UUS performance feature is not used. • *Internal only*: Text messages can only be received internally. • *External only*: Text messages can only be received externally. • *Internal and External* (default value): Text messages can only be received internally and externally.
Receive System Intercom Call	Select whether the system telephone assigned may accept simplex connections. If the system has more than one number then the settings are only applied to the first MSN. The function is activated by selecting *Enabled*. The function is disabled by default.

Field	Description
Receive Announce-ment Calls	Select whether the system telephone assigned may receive announcements. If the system has more than one number then the settings are only applied to the first MSN. The function is activated by selecting *Enabled*. The function is disabled by default.

25.7.1.2 Keys / T400 / T400/2 / T500

In the menu **elmeg System Phones**->**Assigned System Phones**->**Keys** configuration of system telephone keys is displayed.

Your telephone features several function keys to which you can assign various functions on two levels The functions that can be programmed on the keys vary from telephone to telephone.

Every function key with automatic LED functions (e. g. connection keys, line keys) can only be programmed once per system (telephone and key extensions).

Values in the list Keys

Field	Description
Key	Displays the name of the key.
Label Description	Displays the text which you have entered for the labelling page. The text contains the configured key name
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

You can use **Print** to print out a label sheet for the label field on your system telephone or your key extension.

Edit

Choose the ✐ icon to edit existing entries. In the pop-up menu, you configure the functions of your system telephone keys.

You can use the following functions with system telephones:

- *Dial Key (Standard)*: You can store a call number on every function key.

- *Dial Key (DTMF)*: You can store a MFV sequence on every function key.

- *Dial Key (Keypad sequence)*: You can store a keypad sequence on every function key.

- *Extension Key (User)*: You can set up dialling to an internal extension using a line key. After pressing the corresponding key, hands free is switched on and the internal extension entered is selected. If a call is signalled on the internal extension you have entered, you can pick this up by pressing the line key.

- *Extension Key (Team)*: You can set up dialling to a team using a line key. After pressing the corresponding key, hands-free is activated and the entered team is called according to its enabled call option. If a call is signalled for the entered team, you can pick it up by pressing this connection key.

- *Trunk Line*: An ISDN connection or a VoIP provider is set up under a connection key. If this key is pressed, automatic hands-free is enabled and the corresponding ISDN connection is assigned. You then hear the external dialling tone. If an external call is signalled on another internal telephone, you can pick it up by pressing this line key.

- *Login / Log Out, Team*: If you are entered as a subscriber in the call assignments for one or more teams, you can set up a key so that you can control the call signalling of your telephone. If you're logged in, team calls are signalled to your telephone. If you are logged out, no team calls will be signalled.

  The call numbers entered in the telephone can be logged in/logged out from a team using a set function key (**MSN**-1...**MSN**-9). Before entering a team number, you must select the telephone call number index (MSN) that is entered in the corresponding team call assignments.

- *System Call (Announcement User)*: You can set up a connection to another telephone without this connection having to be actively accepted. As soon as the telephone has accepted the announcement, the connection is established and the announcement key LED is enabled. The announcement can be ended by renewed pressing of the announcement key or by pressing the loudspeaker key. The LED switches off again at conclusion of the announcement.

- *System Call (Announcement Team)*: You can configure an announcement for a team by setting up a function key. The way this works is the same as that described above.

- *System Call (Announcement enable)*: You can also selectively deny or allow announcements using a function key. To use announcements, you must be authorised for the corresponding authorisation class.

- *System Call (Intercom)*: You can set up a key is such a way that a connection to the specified telephone is established without this connection having to be actively accepted.

- *System Call (Intercom enable)*: You can set up a key in such a way that the sim-

plex operation function is allowed or denied. To use simplex operation, the function must be allowed in the corresponding authorisation class.

- *Boss Key* / *Secretary Key*: You can set up a key as a special line key. The Boss telephone and Secretary telephone properties are saved in both telephones with these keys.

- *Diversion Secretary*: You can set up a key in such a way that incoming calls to the Boss telephone are automatically routed to the Secretary telephone.

- *Call Forwarding (CFNR)*: You can set up a key so that delayed call diversion is set up for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Configuring call forwarding with a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) on the phone. In order to be able to use call forwarding, you need to have set up at least one number.

- *Call Forwarding (CFU)*: You can set up a key so that immediate call diversion is set up for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.

- *Call Forwarding (CFB)*: You can set up a key so that call diversion on engaged is set up for a specific number (MSN) on your system telephone. Pressing the key when the phone is not in use turns call forwarding on and off. Call forwarding configuration over a programmed key is only possible for numbers 1 to 9 (MSN-1...MSN-9) of the phone. In order to be able to use call forwarding, you need to have set up at least one number.

- *Macro Function*: You can configure a key so that by pressing it a saved macro is executed.

  The macro function can only be programmed at the phone.

- *Headset Control* (not with the **S5x0**): If you've connected and configured a headset to your telephone over a separate headset socket, operation of the headset occurs over a function key. Press the headset key to initiate or accept calls. If you already have an active connection over the headset, you can end the call by pressing the headset key.

- *Automatic Call Pick-up*: Your telephone can accept calls automatically without you having to lift the receiver or press the loudspeaker key. Automatic call acceptance is switched on or off using the function key assigned. You can configure a separate function key for each number ("MSN-1"..."MSN-9"), or a function key for all numbers. The period after which calls are automatically accepted is configured once for all numbers of the telephone.

- *Trunk Group Access*: Several external ISDN (if supported by you device) or IP connections to bundles can be grouped in the system. With a bundle key, you can save these connections on a function key. If this key is pressed, automatic hands-free is enabled and a free B channel of the corresponding bundle is assigned. You then hear the external dialling tone.

- *Connection Key* (not with the **S5x0**): In addition to the softkeys "Connection 1..", function keys can be configured on the system telephone or the extension for operation while brokering. At least two connection keys must be configured.

- *Hotel Room*: You can assign a key in such a way that when pressed, the guest is checked in or out (first level), or the selected hotel room phone is called (second level). You must configure this key on the first level, then the connected key on the second level is automatically assigned and, as the case applies, its content overwritten.

- *System Parking*: The called party is put on hold for enquiry and dials a code. The telephone is now freed for other operations, e. g. announcements. Another party can accept the call, if he lifts the receiver and dials the relevant code of the held call. The codes assigned by the PABX can also be entered in the function keys of one or more system telephones. If a call is set to open hold for enquiry by pressing the function key, this is indicated by flashing LEDs on the function keys for the system telephones set up for this. The call is transferred by pressing the corresponding function key. This performance feature is only possible if only one call is on hold.

- *Agent wrap-up Time*: You can configure a key so that when it is pressed, an agent's post-processing time is switched on or off at a team call centre (first level), or extended (second level).

- *Night Mode*: You can configure a key so that by pressing it night operation is switched on or off.

> **Note**
>
> To manually switch night operation off again, the authorisation class **Switch signalling variants manually** must be enabled.

- *Parallel Ringing* (only **S5x0**): If a parallel call to another telephone is configured, both connections will ring when a call comes in. The call is accepted where first picked up.

- *Shift* (only **S5x0**): With this key, you can access second level functions.

- *Do not Disturb* (only **S5x0**): With this key, you enable or disable the Do not Disturb function which you have configured under **Terminals**->**elmeg System Phones**->**System Phone**->**Settings**.

The **elmeg System Phones**->**Assigned System Phones**->**Keys**-> **Edit** menu consists of the following fields:

Fields in the menu Phone: Type x

Field	Description
Key name	Enter a name for the key to be used as text for the corresponding key when the ID labels are printed.

Field	Description
Key Type	Depending on the model, the telephones feature from 5 to 15 keys on which functions may be assigned over two levels. You can reach the second layer of function keys by pressing the keys twice. This must be done quickly. With **S5x0** devices, you can alternately use the *Shift* function key. With the optional bintec elmeg key extensions, you have access to additional twice-assignable function keys.

Possible values:

- *Dial Key (Standard)*
- *Dial Key (DTMF)*
- *Dial Key (Keypad sequence)*
- *Extension Key (User)*
- *Extension Key (Team)*
- *Trunk Line*
- *Login / Log Out, Team*
- *System Call (Announcement User)*
- *System Call (Announcement Team)*
- *System Call (Announcement User)*
- *System Call (Announcement enable)*
- *System Call (Intercom)*
- *System Call (Intercom enable)*
- *Boss Key*
- *Secretary Key*
- *Diversion Secretary*
- *Call Forwarding (CFNR)*
- *Call Forwarding (CFU)*
- *Call Forwarding (CFB)*
- *Macro Function*
- *Headset Control*
- *Automatic Call Pick-up*
- *Trunk Group Access*
- *Connection Key*
- *Hotel Room*

Field	Description
	• *System Parking*
	• *Agent wrap-up Time*
	• *Night Mode*
	• *Shift key* (**S5x0** only)
	• *Parallel call* (only **S5x0**)
	• *Station guarding (quiet)* (**S5x0** only)
Number	Only where **Key Type** = *Dial Key (Standard)*, *Dial Key (DTMF)* and *Dial Key (Keypad sequence)* You can save a number, an MFV sequence or a keypad sequence on every function key. Enter the call number or the code for the MFV/keypad sequence.
Internal Number	Where **Key Type** = *Extension Key (User)* Select the internal number of a user to be called when this key is pressed. Where **Key Type** = *System Call (Announcement User)* Select the internal number of a user to whose telephone an announcement shall be sent. When **Key Type** = *Login / Log Out, Team* Select the internal number of a team to be logged into or out of when this key is pressed. When **Key Type** = *Receive Announcement Calls* Select the internal number of a user on whose telephone an announcement shall be made. When **Key Type** = *Receive Intercom Calls* Select the internal number of a user with which you wish to conduct simplex operations. When **Key Type** = *Call Forwarding (CFNR)*, *Call Forwarding (CFU)*, *Call Forwarding (CFB)* Select the internal number of a telephone MSN from which the indicated destination number can be forwarded

Field	Description
	When **Key Type** = *Automatic Call Pick-up* Select the internal number of this telephone, on which incoming calls shall be automatically accepted. When **Key Type** = *Hotel Room* Select the internal number of a hotel guest. When **Key Type** = *Agent wrap-up Time* Select the internal number of a user whose post-processing time shall be modified at regular intervals when this key is pressed. When **Key Type** = *Parallel Ringing* Select the internal number of a user whose phone should also ring when a call goes in to you.
Automatic Call Pick-up	Where **Key Type** = *Automatic Call Pick-up* Select when a call shall be automatically accepted by the entered internal subscriber. Possible values: • *Immediately*: The call is immediately and automatically accepted. • *After 5 seconds*: The call is automatically accepted after 5 seconds. • *After 10 seconds*: The call is automatically accepted after 10 seconds. • *After 15 seconds* (only **S5x0**): The call is automatically accepted after 15 seconds. • *After 20 seconds* (only **S5x0**): The call is automatically accepted after 20 seconds. • *Off* (only **S5x0**): The call is not automatically accepted.
Team	Where **Key Type** = *Extension Key (Team)* Select the internal number of a team to be called when this key is pressed.

Field	Description
	Where **Key Type** = *System Call (Announcement Team)*
	Select the internal number of a team to whose telephone an announcement shall be sent.
	When **Key Type** = *Login / Log Out, Team*
	Select the internal number of a team to be logged in/out when this key is pressed.
Trunk Line	Only where **Key Type** = *Trunk Line*
	Select the external connection over which an external call shall be set up when this key is pressed.
Number of Secretary Phone	Only where **Key Type** = *Boss Key*
	Select the internal number of the secretary telephone. The secretary telephone is called when this key is pressed.
Number of Boss Phone	Only where **Key Type** = *Secretary Key*
	Select the internal number of the Boss telephone. The Boss telephone is called when this key is pressed.
Target Number "On no reply"	Only where **Key Type** = *Call Forwarding (CFNR)*
	Enter the number to which calls shall be forwarded immediately when call forwarding is enabled.
Target Number "Immediate"	Only where **Key Type** = *Call Forwarding (CFU)*
	Enter the number to which calls shall be forwarded when call forwarding when busy is enabled.
Target Number "On busy"	Only where **Key Type** = *Call Forwarding (CFB)*
	Enter the number to which calls shall be forwarded when call forwarding is enabled when the call is not answered.
Trunk Group Access	Only where **Key Type** = *Trunk Group Access*
	Select the bundle via which an outside call shall be set up.
Waiting Queue	Only where **Key Type** = *System Parking*

Field	Description
	Select the queue in which the current call should be held.

Move

Select the ↑↓ icon to move configured function keys.

Fields in the menu Phone

Field	Description
Key name	Displays the name of the key.
Key Type	Displays the key type.
Settings	Displays the additional settings with a summary

Fields in the menu Move to

Field	Description
Phone	Displays your system telephone. In **User Access** you can only move keys within your own telephone key extension combination.
Module	Select telephone or a key extension module.
Key	Select the key to which you wish to transfer the configured function.

25.7.1.3 Device Info

In the **elmeg System Phones**->**Assigned System Phones**->**Device Info** menu the system data read out of the system telephone are displayed.

Meaning of the list entries

Description	Meaning
Description	Displays the entered description of the telephone.
Phone Type	Displays the type of telephone.
Serial Number	Displays the serial number of the telephone.

Description	Meaning
Software Version	Displays the current version of the telephone software.
Release Date and Time	Displays the date and time of the telephone software version.
Last Device Configuration	Displays the date and time of the last telephone configuration.
Answering Machine	Displays whether an answering machine module is inserted in the telephone (Yes) or not (No).

Meaning of the key extension

Description	Meaning
Module 1: Type / Serial Number **Module 2: Type / Serial Number** **Module 3: Type / Serial Number**	Displays the type and serial number of the connected key extension.
Module 1: Software Version **Module 2: Software Version** **Module 3: Software Version**	Displays the current software version of the connected key extension.

25.8 Voice Mail System

You can access information on you voicemail box in the **Voice Mail System** menu.

Note

The **Voice Mail System** menu is only displayed once a personal voicemail box has been set up for you.

25.8.1 Settings

In the **Voice Mail System** ->**Settings** menu, your voicemail box settings are displayed.

Values in the Settings list

Field	Description
Internal Number	Displays your internal number.
User	Displays your user name.
Status of Mail Box Owner	Displays your status.
Check PIN	Indicates whether access to your voicemail box is protected by a PIN.
Mode for status "In the Office"	Indicates in which mode your voicemail box operates for the "In Office" status.
Mode for status "Out of Office"	Indicates in which mode your voicemail box operates for the "Out of Office" status.
New Calls	Indicates the number of new calls.
Old Calls	Indicates the number of old calls.
Saved Calls	Indicates the number of saved calls.

25.8.1.1 Edit

Choose the icon to edit existing entries. You can change the settings of selected parameters.

The menu **Voice Mail System** ->**Settings** consists of the following fields:

Fields in the Basic Settings menu.

Field	Description
Status of Mail Box Owner	Define in which mode your mailbox shall be used when starting the voicemail system.

Field	Description
	Possible values: • *In the Office* (default value): Select this setting if you're in the office when the voicemail system is started. • *Out of Office* : Select this setting if you're out of the office when the voicemail system is started.
Check PIN	Select whether your voicemail box should be protected with a PIN.
Mode for status "In the Office"	Your voicemail box can be operated with two different settings during office hours. Possible values: • *Announcement only*: A caller hears an announcement, but cannot leave a message. • *Announcement and Record*: A caller hears an announcement and can leave a message.
Mode for status "Out of Office"	Your voicemail box can be operated with two different settings outside office hours. Possible values: • *Announcement only*: A caller hears an announcement, but cannot leave a message. • *Announcement and Record*: A caller hears an announcement and can leave a message.

Fields in the Voice Mail Message via E-Mail menu.

Field	Description
E-Mail Notification	Once a message has been left on the voicemail box, the subscriber can be notified. Possible values: • *None* (default value): The subscriber is not notified. • *E-Mail*: The subscriber is informed of a present message via e-mail. • *E-Mail with Attachment*: Once a caller has left a message, the subscriber receives an e-mail with a recording of the

Field	Description
	message in the attachment.
	Note
	After a subscriber has been informed about a new message through an E-Mail, the **Status** of the message is chnaged according to the configuration in **User Access**->**Voice Mail System** ->**Settings** under **E-Mail forwarding behavior**.
E-Mail forwarding behavior	Only for **E-Mail Notification** = *E-Mail* or *E-Mail with Attachment*
	Select an option for forwarded messages.
	Possible values:
	• *Keep Message in 'new' after forwarding*: Following an e-mail alert or forwarding, the status of the voicemail message is set to *New*.
	• *Move Message to 'old' after forwarding*: Following an e-mail alert or forwarding, the status of the voicemail message is set to *Old*.
	• *Remove Message after forwarding*: The voicemail message is deleted following an e-mail alert or forwarding.

25.8.2 Messages

In the **Voice Mail System** ->**Messages** menu, a list of your messages is displayed. You also have the option to play back voicemail messages or download these to your PC. To save a message, click on the 🗎 icon. The download dialog then opens. To listen to a message, click on the ▶ icon.

Individual or all wave files can be deleted by clicking the **Select all** / **Deselect all** checkbox then pressing **Delete Selected**.

Values in the Messages list

Field	Description
Internal Number	Displays the internal number of a voicemail box.

Field	Description
	Several internal numbers can be assigned to a single user. The user can operate a separate voicemail box under each internal number.
User	Displays the name of the voicemail box user.
Call from	Displays the caller's number.
Date/Time	Displays the date and time of the call.
Call Status	Indicates whether the call is *New*, *Old* or *Saved*.
Select all / **Deselect all**	You can select individual entries using the checkbox in the corresponding line, or select them all using the **Select all** button or **Deselect all**. You can delete the selected entries by pressing the **Delete Selected** option.

Glossary

2G	See GSM.
3DES	See DES.
3G	See UMTS.
4G	See LTE.
802.11	The 802.11 norm describes wireless LAN (WLAN). There are a variety of amendments: 802.11a: Gross data transfer rates: 54 Mbit/s, frequency band: 5 GHz, 802.11b/g: Gross data transfer rates: 11 Mbit/s, frequency band: 2.4 GHz, 802.11g: Gross data transfer rates: 54 Mbit/s, frequency band: 2.4 GHz, 802.11n: Gross data transfer rates: 600 Mbit/s, frequency band: 2.4 GHz (optional: 5 GHz)
A-subscriber	The A-subscriber is the caller.
a/b interface	An a/b interface is used to connect an analogue terminal. In the case of an ISDN terminal (terminal adapter) with a/b interface, a connected analogue terminal is enabled to use the supported ISDN performance features.
Access client	Client mode is an operating mode of a wireless access point (AP) in which the latter behaves like a wireless adapter vis-a-vis the higher level AP. With an AP run in client mode, individual computers or entire sub-networks can be connected to higher level networks.
Access point	An access point (AP) is a device for wirelessly connecting clients (computers). The AP thus serves to create a wireless network (WLAN) and connect that WLAN to a wired Ethernet network (bridging).
Accounting	Accounting refers to the recording of connection data, e.g. date, time, connection duration, charging information and number of data packets transferred.
Activity monitor	The activity monitor is used to oversee the status of physical and virtual device interfaces.
Ad-hoc network	In an ad-hoc network, individual clients connect to an independent wireless LAN via a wireless adapter. Ad-hoc networks work independently, with no access point on a peer-to-peer basis. The ad-hoc mode is also referred to as IBSS (Independent Basic Service Set)

mode and is useful in very small networks, e. g. when linking two notebooks with no access point.

ADSL	Asymmetric digital subscriber line. See DSL.
AES	Advanced Encryption Standard (AES, Rijndael) is an encryption method (see Cipher). AES uses a fixed block length of 128 bits. The key length is 128, 192 or 256 bits. AES is a very fast and secure algorithm.
Agent	The call centre agent is a member of a call centre.
Aggressive mode	When an IPSec connection is being established, aggressive mode is used to implement a phase 1 exchange. Aggressive mode offers no identity protection for negotiating nodes, since they have to transmit their identity before they can establish a secure channel. See also Main mode.
AH	The authentication header (AH) is used with IPSec to ensure the authenticity and integrity of the packets transmitted and to authenticate the sender.
Analogue	Analogue signals are used to transmit data. They are more susceptible to errors than digital signals.
Analogue terminals	Terminals that transmit voice and other information analogously, e.g. telephones, fax machines, answering machines and modems. Performance features can only be used with terminals that dial using the MFC dialling method and that have an R or flash key.
Annex A	Annex A is a DSL variant which occurs in connection with analogue telephone connections, e. g. in France.
Annex B	Annex B is a DSL variant which occurs in connection with ISDN, e. g. in Germany.
Annex J	Annex J is a DSL variant purely for data transmission, with no voice data (unbundled connection). Annex J is an extension of specification G.992. These DSL connections require no splitter and have a greater range and faster transmission speed.
Annex L	Annex L is an extension of Annex A. The range is increased at the expense of the data transmission rate.
Annex M	Annex M is an extension of Annex A. The upstream is increased at the expense of the downstream.

Announcement   The announcement is a performance feature. The announcement function enables a connection to be established to other phones which is automatically accepted by the subscribers called. The caller speaks and those called hear the announcement. If one of those called lifts the receiver, a normal connection is established.

ANSI T1.413   ANSI T1.413 is an ADSL variant.

Answering machine   Analogue answering machines are configured as an analogue terminal and selected via the terminal type. The PABX voice mail system is used as the answering machine.

ARP   The Address Resolution Protocol (ARP) supplies the associated MAC addresses to IPv4 addresses. The information required is shared between the network nodes, stored in the device's cache, and deleted again after the ARP lifetime has expired. For IPv6 this functionality is provided by the Neighbor Discovery Protocol (NDP).

ARS   The PABX uses Automatic Route Selection (ARS) to determine the ideal route to the called party, depending on the provider, service, QoS, …

ATM   Asynchronous Transfer Mode (ATM) is a data transmission technology in which the data traffic is coded in small packets – called cells or slots – with a fixed length and is transmitted via asynchronous time multiplexing.

Authentication   Check on the user's identify.

Authorisation   Based on their identity (authentication), the user can access certain services and resources.

Authorisation class   See CoS.

Automatic callback on busy (CCBS)   Callback on busy is a performance feature. If the connection of the subscriber called is engaged, a callback can be requested. When the called subscriber's phone call ends, the caller is phoned and automatically connected to the called subscriber.

Automatic callback on no reply (CCBS)   Callback on no reply is a performance feature. If the called subscriber fails to take the call, a callback can be requested. When the called subscriber ends a call, the caller is phoned and automatically connected to the called subscriber.

Automatic outside line   Automatic outside line enables the phone number of an external party to be dialled (without entering a code).

Automatic redialling If the connection of the called party is engaged, an automatic redial can be initiated. This notifies the caller as soon as the line is free.

Automatic Route Selection Automatic route selection can be used to route calls whatever the number (zone) dialled, via specified providers or bundles.

AUX AUX is a signal input for external devices, e. g. analogue or GSM modems.

B channel See Basic Rate Interface and Primary Rate Interface.

B channel See B channel.

B subscriber The B subscriber is the called party.

Back Route Verify If a Back Route Verify is activated for an interface, incoming data packets are only accepted over this interface if outgoing response packets are routed over the same interface.

Backbone area The core area of a network which connects all the sub-networks (areas) with one another is known as the backbone.

Basic Rate Interface The Basic Rate Interface is a network connection to the ISDN. This type of connection is often abbreviated to BRI. A basic rate interface includes two basic channels (B channels) each with 64 kbps and one control and signalling channel (D channel) with 16 kbps. There are two operating modes for the Basic Rate Interface: Point-to-point ISDN and Point-to-multipoint The Primary Rate Interface (PRI) is used with larger installations.

Beacon The central access point sends beacons to create a wireless LAN in infrastructure mode. These messages contain the network name (SSID), a list of the supported transmission rates and the type of encryption.

Bit A binary digit (bit) is the smallest unit of data in computing technology. Signals are represented in the logical states "0" and "1".

Black / White List Entries in the Black List are blocked, entries in the White List are allowed through. (Example: Any telephone number beginning with 01234 is blocked in the Black List. The number 01234987 can nonetheless be approved in the White List.)

Blowfish Blowfish is an encryption method (see Cipher). Blowfish uses a fixed block length of 64 bits. The key length can be between 32 and 448 bits.

BootP	The Bootstrap Protocol (BootP) is used to automatically issue an IP address.
Bps	Bits per second. A unit of measure for the transmission rate.
BRI	See Basic Rate Interface
Bridge	A bridge is a network component for connecting the same types of network at Level 2 of the OSI model. Data packets are transmitted using MAC addresses. The use of bridges divides up the network and reduces the load.
Broadcast	In a broadcast, data packets are sent from one point to all the subscribers in a network, e. g. if the recipient is not yet known. Examples of this are the ARP and DHCP protocols. The communication is via broadcast addresses: MAC networks: FF:FF:FF:FF:FF:FF, IPv4 networks: 255.255.255.255, IPv6 networks: ff00::/8
Broker	Brokering makes it possible to switch between two subscribers without the waiting subscriber being able to hear the other conversation.
BRRP	BRRP is an implementation of the Virtual Router Redundancy Protocol (VRRP). The aim of the method is to compensate for the failure of the default gateway. Multiple routers are combined to form one virtual router. If one of these routers falls over, the others are able to replace it.
Bundle	The external connections of a PABX can be grouped into bundles.
Busy On Busy	If Busy on Busy is enabled, anyone who calls an engaged subscriber hears the engaged tone. Call waiting or call forwarding to a team are not possible.
CA	Certificate Authority. See Certificate.
Cache	The device temporarily stores data used in name resolution in the cache. See also ARP.
Call allocation	With call allocation, calls coming into the PBX are assigned to particular numbers or applications (remote access, ISDN login, ...).
Call centre	A call centre provides support, shares information and sells over the telephone.
Call deflection	Call deflection (CD) is a performance feature. A call can be forwar-

ded without it having been taken.

Call deflection (CD)   See Call forwarding.

Call forwarding   Call forwarding is a performance feature. When call forwarding (CF) is used, incoming calls can be routed to another, internal or external, phone number. The call can be forwarded in the telephone system or the switchboard, or by the SIP provider.

Call pickup   See pickup

Call Through   Call Through refers to dialling into the system via an external connection and the system putting the call through to a different external connection. This can reduce call costs.

Call variant   The call variant specifies which terminals a call is signalled to. The calendar can be used to control the individual call variants on a time basis.

Call waiting   Call waiting is a performance feature. Another caller is signalled during a phone call.

Call waiting protec- When call waiting protection is enabled, other callers are not sig-
tion   nalled on the terminal. The caller hears the engaged tone.

Callback on Busy   See Automatic callback on busy (CCBS)

Callback on no reply See Automatic callback on no reply (CCBS)

Called party number   The number of the party being phoned.

Caller list   On system telephones, missed calls are saved in a caller list. To achieve this, calling line identification presentation (CLIP) needs to be enabled.

Calling party number The number of the calling terminal.

CAPI   The Common ISDN Application Programming Interface (CAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also TAPI.

CAPWAP   Control And Provisioning of Wireless Access Points Protocol (CAPWAP) is used to have wireless access points (slaves) monitored by a WLAN controller (master). It uses UDP port 5246 for monitoring and 5247 to send data.

CAST   CAST is an encryption method (see Cipher). CAST uses a fixed

block length of 64 bits. The key length can be between 40 and 128 bits. Alternative names are CAST-128 and CAST5.

Certificate   A certificate identifies a person, an institution, a device or an application. A public key certificate is a digital certificate and it creates a connection between the identity and a public key. Certificates with public keys are issued by a certification authority (CA). Certificates that can no longer be trusted may be revoked using certificate revocation lists (CRLs)

CFB   Call Forwarding Busy (CFB) is a performance feature. CFB forwards callers to a different connection if the connection of the party called is engaged.

CFNR   Call Forwarding No Reply (CFNR) is a performance feature. CFNR forwards callers to a different connection if the call is not taken.

Channel   A wireless channel is a frequency band used for wireless LAN. Devices that send on adjacent channels disrupt one another.

Channel bundling   When channels are bundled, the B channels in an ISDN connection are combined to increase data throughput.

CHAP   The Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol for PPP connections. As well as the standard CHAP, Microsoft also has the variants MS-CHAPv1 and MS-CHAPv2. You dial into a network via PPP and you authenticate yourself with a username and password. The username and password are transmitted encrypted. See also PAP.

Cipher   A block cipher is an encryption algorithm. In this encryption method, a data block of a fixed size (normally 64 bit) is rewritten to a block of the same size using a so-called key. The longer the key, the more secure the algorithm.

CLID   Calling Line Identification (CLID), also known as Caller ID, is used for authentication. A caller is identified by means of his or her ISDN extension number before the connection is established.

Client   A client uses the services provided by a server. Clients are usually workstations.

CLIP   See Display caller number (CLIP / CLIR).

CLIP no Screening   See also Display caller number (CLIP / CLIR). With CLIP no Screening, as well as the normal caller number, another number is also sent, e. g. the number of the switchboard or a service number. The

normal number can also be suppressed using CLIP, so that the party called only sees the other number.

CLIP off Hook   See Display caller number (CLIP / CLIR).

CLIR   See Display caller number (CLIP / CLIR).

Code procedure   A sequence (code procedure) (consisting of 0 - 9, *, # and R) can be entered on the telephone keypad in order to access the PBX's functions.

COLP   See Display called party number (COLP / COLR).

COLP no Screening   See also Display called party number (COLP / COLR). With COLP no Screening, as well as the normal caller number, another number is also sent, e. g. the number of the switchboard or a service number. The normal number can also be suppressed using COLP, so that the party called only sees the other number.

COLR   See Display called party number (COLP / COLR).

Conference call   With a conference call, multiple internal subscribers can speak to one another on the phone at the same time.

Configuration   The configuration refers to all of a device's settings. It is stored internally, in MIB tables. This data can be backed up, loaded and deleted externally. The configuration is edited using the HTTP(S) user interface, an SNMP client or connected telephones.

CoS   The term Class of Service (CoS) means different things depending on the area in which it is applied. In telecommunications CoS refers to the permission class assigned to the user. The permission class defines the user's rights, e. g. exchange access right, features that can be used, access to applications, ... In network technology CoS refers to the classification of certain services as per IEEE 802.1p. CoS enables priorities to be set in a targeted way, while Quality of Service (QoS) is used to set up explicit bandwidth guarantees or restrictions. Data packets are classified using a DSCP (Differentiated Services Code Point) value.

CRC   Cyclic Redundancy Check (CRC) is a method of detecting errors in the data transmission.

CRL   See Certificate.

D channel   See Basic Rate Interface and Primary Rate Interface.

Daemon   A daemon refers to a program that runs in the background and provides certain services.

Data compression   Data compression is a method of reducing the data volume transmitted. See STAC and MPPC.

Datagram   A datagram is a self-contained data entity with user and control data. It generally stands for the terms data frame, data packet and data segment.

DCN   DCN stands for data communication network.

DDI   DDI stands for Direct Dial In. See Point-to-point ISDN access and Direct dial-in (VoIP).

Dead Peer Detection   In IPSec, Dead Peer Detection is used to identify IKE peers that can no longer be accessed.

DECT   Digital Enhanced Cordless Telecommunications (DECT) is a standard for cordless telephones and wireless PABX systems.

Default gateway   All the data traffic which is not intended for one's own network is sent to the default gateway (default router).

Default route   See Standard route

Default route   The default route is used when no other suitable route is available.

Default router   See Default gateway.

Deffie-Hellman   Diffie-Hellman is a public key algorithm for negotiating and establishing keys. Because data is neither encrypted nor signed, the method is only secure if the connecting partners authenticate themselves using other mechanisms such as RSA and DSA.

Denial-Of-Service At-   In a Denial-Of-Service Attack (DoS), a network component is
tack   flooded with queries so that it becomes totally overloaded. As a result, the system or a particular service can no longer function.

DES   The Data Encryption Standard (DES) is an encryption method (see Cipher). DES uses a fixed block length of 64 bits. The key length is 56 bits. Triple DES or 3DES is based on using DES three times (three different, independent keys).

DHCP   The Dynamic Host Configuration Protocol (DHCP) allows IP addresses to be assigned dynamically. A DHCP server allocates each client in a network an IP address from a defined address pool. The

clients need to be configured accordingly.

Dial preparation   Dial preparation describes the entering of the telephone number be-
                           fore initiating the call, e. g. by lifting the receiver.

Dialling control   See Black / White List.

Dialup connection   When required, a dialup connection is established by dialling a
                           phone number, in contrast to a fixed connection (see Leased line)
                           which is permanently enabled.

Digital   Digital signals are used to transmit data. They are less susceptible
                           to errors than analogue signals.

DIME   Desktop Internetworking Management Environment (DIME) is used
                           to configure and monitor gateways.

Direct call   If the direct call function is set up, the user merely has to lift the tele-
                           phone receiver to, after a short wait, automatically get a connection
                           to a particular phone number.

Direct dial exception See Point-to-point ISDN access and Direct dial-in (VoIP).

Direct dial-in (VoIP) Direct dial-in is a VoIP connection that is also known as point-
                           to-point. It is used to connect a PBX. A main phone number and a
                           number block are issued. Each of the numbers in the number block
                           is called a direct dial exception. (Example: Main number 1234, num-
                           ber block: 1 - 99, numbers of the individual extensions: 1234-1,
                           1234-2, 1234-3, …)

Direct dialling range See number block in Point-to-point ISDN access and Direct dial-in
                           (VoIP)

DISA   DISA - Direct Inward System Access A call, after it has been taken
                           by the PBX, is automatically forwarded after a code has been
                           entered. In the PBX, this code is assigned to an internal telephone
                           number.

Display called party   Connected Line Identification Presentation (COLP) is used to send
number (COLP /   the phone number of the called party (B phone number) to the
COLR).   caller. Connected Line Identification Restriction (COLR) is used to
                           suppress the transmission of the phone number of the called party
                           to the caller.

Display caller num-   Calling Line Identification Presentation (CLIP) is used to send the
ber (CLIP / CLIR).   caller's phone number (A phone number) to the called party. CLIP
                           off Hook sends the phone number of the caller waiting. Calling Line

Identification Restriction (CLIR) is used to suppress the transmission of the phone number of the caller to the called party.

DNS   The Domain Name System (DNS) is used to convert the domain name (e. g. www.example.org) to an IP address (name resolution).

Do not disturb   See Station guarding.

Domain   A domain is a contiguous sub-set of the DNS (e. g. example.org).

Door intercom   A door intercom is mounted on entrances, and may be part of a PBX.

Downstream   The gateway receives the data from a higher-level network and forwards it to its connected network.

DSA   The Digital Signature Algorithm (DSA) is used to create digital signatures and encrypt data packets. Signatures can be used to verify changes made to the information in the data packet. DSA is used for public-key cryptography (IPSec). See also RSA. Key generation is quicker with DSA than with RSA, but key processing is slower.

DSCP   Data packets can be marked with a Differentiated Services Codepoint (DSCP). DSCP values classify data packets in such a way that important packets can be routed through the network more quickly. See also QoS.

DSL modem   See Modem.

DSP   A digital signal processor (DSP) converts analogue, ISDN and VoIP signals to one another. So, e. g., analogue terminals can also be used on an SIP connection.

DSS1   Digital Subscriber Signalling System No. 1 (DSS1) is a signalling protocol for the D channel in the ISDN. It is also known as Euro ISDN.

DTIM   A Delivery Traffic Indication Message informs the clients that multicast or broadcast data is available at the access point.

DTMF   See Multifrequency code dialling method.

**DTMF Inband / Out-   See also Multifrequency code dialling method. With inband, the
band**   DTMF signal is transmitted in the voice band (G.711) With outband, the DTMF signal is transmitted as specified in RFC 2833.

Dynamic IP address In contrast to a static IP address, a dynamic IP address is assigned

temporarily by DHCP. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.

DynDNS   A DynDNS provider can be used to link a domain name with a dynamically changing IP address.

Encapsulation   Encapsulation of data packets is a particular protocol to transmit the data packets in a network. See also VPN.

Encryption   Refers to the encryption of data, e.g. using MPPE.

Engaged when busy See Busy on Busy.

ESP   Encapsulating Security Payload (ESP) is a protocol for IPSec. It uses protocol number 50 and supports data encryption and authentication.

Ethernet   Ethernet is a specification for cable data networks. Ethernet works on the first and second layer of the OSI model.

Euro ISDN   Standard ISDN in Europe, based on the DSS1 signalling protocol.

Eurofile transfer   Eurofile transfer (EFT) is a protocol for sharing files over ISDN.

Exchange access right
The telephone system distinguishes between the following exchange access rights: Unlimited: Any international, national or internal connection is permitted. National long-distance calls: Only domestic connections may be established - i. e. dialling any number that begins with 0 but not with 00. Incoming external calls can be received without restrictions. Locality: Only connections to the same area code may be established. So the number may not begin with a 0. Incoming external calls can be received without restrictions. Incoming: Only connections to other terminals in the telephone system may be established. Incoming external calls can be received without restrictions. Internal: Only connections within the telephone system are permitted.

Extension   In PBX systems, an extension refers to the terminal connected to the system.

Extension number   See Point-to-point ISDN access and Direct dial-in (VoIP).

Extension number block
See Point-to-point ISDN access and Direct dial-in (VoIP).

Extension numbers   See Extension number block in Point-to-point ISDN access.

range

Fax	Fax is used to send text, graphics and documents over the phone network. A distinction is drawn between Group 3 fax machines for the analogue network (transmission rate: 9.6 or 14,4 kbit/s) and Group 4 fax machines for ISDN (transmission rate: 64 kbit/s). To connect Group 3 fax machines to ISDN, a terminal adapter or a suitable PBX is required.
Filter	A filter comprises a number of criteria (e.g. protocol, port number, source and destination address). If these criteria match a data packet, the data packet can be subjected to a particular action (forward, reject, ...). This creates a filter rule.
Filter rule	A rule that defines which data packets should or should not be transmitted by the gateway.
Firmware	The firmware (system software) is programming code that is permanently embedded in the device. It provides the device's functions.
Flash key	The flash key on a telephone is the R button. The key interrupts the line briefly to start certain functions such as inquiries.
Follow-me	Follow-me is a performance feature. This function can be used to route incoming calls from a different extension to one's own terminal.
Fragmentation	If the overall length of the data packet is greater than the Maximum Transmission Unit (MTU) of the network interface, the data packet has to be broken down into multiple physical data blocks using IP fragmentation. The reverse process is known as reassembly.
Frame	A data frame is an information unit (Protocol Data Unit) in the data link layer in the OSI model.
Frame relay	Frame relay is a data transmission technology and upgrade of X.25 (smaller packets, less error checking). Frame relay is primarily used for GSM networks.
FTP	The File Transfer Protocol (FTP) regulates data transmission in IP networks. It regulates the exchange between FTP server and client.
Full-duplex	With full-duplex, data can be sent and received simultaneously over a line.
Function keys	Function keys are special keys on system telephones which can be assigned phone numbers or functions.

FXO   Foreign Exchange Office (FXO) refers to the connection to the ana-logue terminal. See also FXS.

FXS   Foreign Exchange Station (FXS) refers to the analogue connection to the connection socket or PBX. See also FXO.

G.711   G.711 is an audio codec. Audio signals from the frequency range between 300 Hz and 3400 Hz are passed with a sampling rate of 8 kHz. At a data transmission rate of 64 kbit/s, the codec achieves ex-cellent voice quality (MOS value: 4.4). The A-law quantisation meth-od is used in Europe, and the µ-law method in the USA.

G.722   G.722 is an audio codec. Audio signals from the frequency range between 50 Hz and 7000 Hz are passed with a sampling rate of 16 kHz. At a data transmission rate of 64 kbit/s, the codec achieves outstanding voice quality (MOS value: 4.5).

G.726   G.726 is an audio codec. Audio signals from the frequency range between 200 Hz and 3400 Hz are passed with a sampling rate of 8 kHz. The codec achieves an acceptable voice quality. MOS value: 3.7 (16 kbit/s), 3.8 (24 kbit/s), 3.9 (32 kbit/s), 4.2 (40 kbit/s). There are two different coding methods: I.366 and X.420

G.729   G.729 is an audio codec. Audio signals from the frequency range between 300 Hz and 2400 Hz are passed with a sampling rate of 16 kHz. At a data transmission rate of 8 kbit/s, the codec achieves an acceptable voice quality (MOS value: 3.9).

G.991.1   Data transmission recommendation for HDSL.

G.991.2   Data transmission recommendation for SHDSL.

G.992.1   Data transmission recommendation for ADSL. There are two coun-try-specific versions: G.992.1 Annex A and G.992.1 Annex B. Data transfer rates: 12 Mbit/s (downstream), 1.3 Mbit/s (upstream)

G.992.2   Data transmission recommendation for ADSL (G.LITE / ADSL-Lite). There are two versions: G.992.2 Annex A and G.992.2 Annex B. Data transfer rates: 12 Mbit/s (downstream), 1.3 Mbit/s (upstream)

G.992.3   Data transmission recommendation for xDSL2. There are three vari-ants: G.992.3 Annex A/B (G.DMT to ADSL2) with data transmission rates of 12 Mbit/s in the downstream and 1.0 Mbit/s in the upstream, G.992.3 Annex L (RE-ADSL2) with data transmission rates of 5 Mbit/s in the downstream and 0.8 Mbit/s in the upstream and G.992.3 Annex M (ADSL2) with data transmission rates of 12 Mbit/s

in the downstream and 2.5 Mbit/s in the upstream.

G.992.4   Data transmission recommendation for ADSL2 with Annex A/B.
                     Data transmission rates: 12 Mbit/s (downstream), 1.0 Mbit/s
                     (upstream)

G.992.5   Data transmission recommendation for xDSL2+. There are three
                     variants: G.992.5 Annex A/B (ADSL2+) with data transmission rates
                     of 25 Mbit/s in the downstream and 1.0 Mbit/s in the upstream,
                     G.992.5 Annex L (RE-ADSL2+) with data transmission rates of 25
                     Mbit/s in the downstream and 1.0 Mbit/s in the upstream and
                     G.992.5 Annex M (ADSL2+) with data transmission rates of 25 Mbit/
                     s in the downstream and 3.5 Mbit/s in the upstream.

G.993.1   Data transmission recommendation for VDSL. Data transmission
                     rates: 52 Mbit/s (downstream), 16 Mbit/s (upstream)

G.993.2   Data transmission recommendation for VDSL2. Data transmission
                     rates: 200 Mbit/s (downstream), 200 Mbit/s (upstream)

G.DMT   See F.992.1.

G.Lite   See F.992.2.

G.SHDSL   See G.991.2.

Gateway   The gateway is a network component for connecting different types
                     of network.

GPRS   General Packet Radio Service (GPRS) is the name for the packet-
                     oriented service for transmitting data in GSM networks.

GRE   Generic Routing Encapsulation (GRE) is a network protocol for en-
                     capsulating other protocols so that they can be transported via the
                     Internet Protocol (IP) in the form of a tunnel (VPN). GRE uses pro-
                     tocol number 47.

GSM   The Global System for Mobile Communications (GSM), also known
                     as 2G, is a mobile communications standard. It achieves, along with
                     GPRS, a specified max. data transmission rate of 171.2 kbit/s.

Half-duplex   With half-duplex, data can only be sent and received back-to-back
                     over a line.

Hands-free calling With hands-free calling, calls can be made without lifting the receiv-
                     er. Other people in the room can participate in the conversation us-
                     ing a microphone and loudspeakers.

Hash   To ensure data integrity, the information needs to be protected from unauthorised manipulation while it is being transmitted. To ensure that this happens, every item of communication received has to match the information originally sent. Therefore erratic mathematical value functions (hash functions) are used to calculate checksums (hash values). These are encrypted and sent as a digital signature with the message. The recipient, in turn, checks the signature before opening the packet. If the signature and, thus, the content of the data packet has changed, the packet is discarded. The hash algorithms used most frequently are Message Digest Version 5 (MD5) and Secure Hash Algorithm (SHA1).

HDSL   High Data Rate Digital Subscriber Line. See DSL.

Heartbeat   A network's subscribers use heartbeats to signal that they are ready to receive.

Hold   A telephone call is put on hold without breaking the connection (inquiry/brokering). A distinction is drawn between holding the connection in the PBX (holding in the system) and holding in the switchboard or by the SIP provider.

Hold for enquiry With hold for enquiry, the phone call with the first party is held while one conducts a second call.

Hop   Hop is the term for the connection from one network node to the next.

Host   A host is a computer system that provides its services to the network.

Host name   The domain name of a host. See DNS.

Host route   A host route is the name for the route to a single host.

Hotspot   A hotspot is a public internet access point via WLAN or wired Ethernet.

HSDPA   High Speed Downlink Packet Access (HSDPA, 3.5G, 3G+ or UMTS broadband) is a data transmission method in the UMTS mobile communications standard.

HTTP   The HyperText Transfer Protocol (HTTP) is a protocol for transmitting HTML pages (web pages) between server and client. By default it uses port 80.

HTTPS   The HyperText Transfer Protocol Secure (HTTPS) is a protocol

which protects against eavesdropping when transmitting HTML pages (web pages) between server and client. HTTPS is schematically identical to HTTP. SSL / TLS is used for additional data encryption. The standard port for HTTPS connections is 443.

Hyperchannel
With a hyperchannel, multiple subscribers have access to the transmission medium. A subscriber can only transmit their data if no other subscriber is using the medium. A hyperchannel network is mainly used for short-range operation with top data rates.

IAE
IAE refers to the standard socket (ISDN connection unit) to which ISDN terminals are connected.

ICMP
The Internet Control Message Protocol (ICMP) is used to exchange information and error messages over IPv4. The version ICMPv6 exists for IPv6.

IGMP
The Internet Group Management Protocol (IGMP) is used in IPv4 networks to organise multicast groups.

IKE
The Internet Key Exchange Protocol (IKE) is used for automatic key management with IPSec connections. The IKE process runs in two phases. During phase 1, the IKE subscribers authenticate themselves to one another and establish a secure channel. In phase 2, the two IPSec subscribers negotiate the SAs. There are two versions of the IKE mechanism.

Infrastructure network
In an infrastructure network the individual terminals (clients) form a wireless LAN via a central access point. This central access point may also be an agent in other networks.

Internal call tone
The internal call tone on a PBX is used to differentiate between internal and external calls.

Internal telephone numbers
Internal phone numbers are used for calls within the PBX.

IP
The Internet Protocol (IP) is a network protocol and it is the basis for the Internet. It works on the network layer of the OSI model. The TCP and UDP protocols are based on IP. There are two versions, Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

IP address
IP addresses are used to navigate in an IP network, to unambiguously identify the source and destination. IPv4 addresses consist of 32 bits, IPv6 addresses of 128 bits. So, with IPv4 232, i.e.

4.294.967.296 addresses can be represented, with IPv6 2128 = 340.282.366.920.938.463.463.374.607.431.768.211.456 addresses. Dotted decimal notation, e. g. 192.168.0.250, is used for IPv4. Hexadecimal notation, e. g. 2001:db8:85a3::8a2e:370:7344, is used for IPv6. See also netmask.

IPCP
The Internet Protocol Control Protocol (IPCP) is used, in a similar way to DHCP, to configure a host with an IP address, gateway and DNS server, when a PPP network connection is being used. With the extension Robust Header Compression over PPP, the header can be compressed for faster data transmission. Similarly, in IPv6 networks, the functionality is provided by the Internet Protocol version 6 Control Protocol (IPV6CP).

IPSec
IPSec (Internet Protocol Security) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). The protocol number for IPSec depends on the protocol used. The Authentification Header (AH) uses protocol number 51, while the Encapsulating Security Payload (ESP) uses number 50.

IPv6
See IP.

ISDN
Integrated Services Digital Network (ISDN) is a data transmission standard that includes telephony, fax and data transmission. There are two ISDN connection variants: Basic Rate Interface and Primary Rate Interface.

ISDN address
The ISDN address of an ISDN device comprises an ISDN number followed by other numbers that relate to the specific terminal.

ISDN login
The ISDN login is used to remotely configure the device via SNMP. To do so, it needs to have a configured ISDN or wireless connection.

ISDN number
The ISDN number is the network address of the ISDN interface.

ISDN router
See Router.

ISDN-BRI
See BRI.

ISDN-Internal/External
Alternative name for the So bus.

ISDN-PRI
See PRI.

ISP
Internet Service Providers (ISPs) supply technical services for using

the Internet.

ITU   The International Telecommunication Union (ITU) coordinates the setting up and operating of telecommunications networks and services.

Keepalive   Keepalive packets are used to check that the communication partner can be contacted.

Keepalive   Keepalive is a mechanism for maintaining the network connection and for checking that the communication partner can be reached. Specific packets are usually sent to the network for this purpose.

Keypad   The keypad protocol (network direct) is used to access and manage performance features provided by the switchboard.

L2TP   The Layer 2 Tunneling Protocol (L2TP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). By default, L2TP uses protocol number 1701. The architecture in an L2TP network consists of an L2TP access concentrator (LAC) which may also be permanently integrated into the client, and the L2TP network server (LNS). The LAC establishes the connections to the LNS and manages them. The authorisation is regulated using a network access server (NAS), which can be implemented in the LAC or LNS. The LNS is responsible for routing and controlling the packets received from the LAC. The user data itself is exchanged unencrypted, while control messages for maintaining the accessibility of the tunnel endpoints are transmitted securely.

LAC   See L2TP.

LAN   A Local Area Network (LAN) refers to a network that is geographically very limited and normally spans one building or a company head office.

Layer   A layer refers to a layer in the OSI model.

LCP   The Link Control Protocol (LCP) is used in PPP connections to automatically negotiate encapsulation, process limits for varying packet sizes, authenticate the connection partner, determine faulty links, identify connection faults and terminate the connection.

LDAP   The Lightweight Directory Access Protocol (LDAP) regulates the communication between a client and the directory server. LDAP is used for sharing and updating directories, e. g. a phone book.

Lease time	The lease time refers to the validity period of a dynamic IP address that a client has been given by a DHCP server.
Leased line	See Leased line
Leased line	A leased line is a permanent connection of two communication partners via telecommunications network.
Line access authorisation	See Exchange access right.
LLC	The Link Layer Control (LLC) regulates the media allocation at MAC level.
LNS	See L2TP.
Load balancing	With load balancing, data is sent via different interfaces in order to increase the overall bandwidth available. In contrast to Multilink, load balancing also functions with accounts with different providers.
Loopback	In a loopback switch the sender and recipient are identical.
LTE	Long Term Evolution (LTE), also known as 4G, is a mobile communications standard with a standardised maximum data transmission rate of 300 Mbit/s.
MAC address	The Media Access Control address (MAC address) is the hardware address of the network adapter and is used to identify the device at the hardware level.
Main Mode	When establishing an IPSec connection, main mode is used to implement a phase 1 exchange by setting up a secure channel. See also Aggressive mode.
Man-in-the-Middle attack	In a Man-in-the-Middle attack, the attacker is physically or logically between the two communication partners and so is able to view, and even manipulate, the data traffic.
MD5	Message Digest Algorithm 5 (MD5) is a hash function that generates a 128 bit hash value (checksum). See also Hash.
Media gateway	A media gateway converts the network type of digital voice, audio or image information. For example, the signals from an ISDN network can be converted to an IP network.
Metric	The metric is a measure for the properties of the route. The fastest route has the lowest metric (costs). Simplified, this is connecting

	with the smallest number of node points (routers).
MFC	See Multifrequency code dialling method.
MFV	See Multifrequency code dialling method.
MIB	The Management Information Base (MIB) describes the data that can be queried or modified via a network management protocol (e. g. SNMP). The MIB is a database that describes all the devices and functions in the network.
MLP	The Multicast Listener Discovery (MLD) is used in IPv6 networks to organise multicast groups.
Mobile subscriber	If the mobile subscriber is enabled, an external telephone, e. g. a mobile phone can be called in parallel (parallel calling). The system's functions, e. g. callback, can also be used externally. For these functions, the external telephone's star key is interpreted as the R key.
Modem	A modem is an electronic device that converts digital signals to frequency signals in order to distribute data in a wired or wireless network.
MOH	See Music on hold.
MPDU	The MAC Protocol Data Unit (MPDU) refers to a data packet, including management frames and fragmented MSDUs, exchanged wirelessly.
MPPC	Microsoft Point-to-Point Compression (MPPC) is a method of data compression.
MPPE	Microsoft Point-To-Point Encryption (MPPE) is used to encrypt data transmitted via PPP. It was developed by Microsoft and Cisco and specified as RFC 3078.
MS-CHAP	The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a method of authentication. MS-CHAPv1 is intended for authenticating DCN connections and is largely the same as the standard CHAP. MS-CHAPv2 is an authentication method for PPTP connections (VPN).
MSDU	A MAC Service Data Unit (MSDU) is a data packet that is exchanged at LLC level.
MSN	See Multiple subscriber number

MSS	The Maximum Segment Size (MSS) defines the maximum number of bytes that can be used as user data in a TCP segment. The MSS must be smaller than the Maximum Transmission Unit (MTU) to avoid fragmenting the IP packets.
MSS clamping	MSS clamping reduces the Maximum Segment Size (MSS) in order to connect networks with different Maximum Transmission Units (MTU).
MTU	The Maximum Transmission Unit (MTU) is the largest possible data unit that can be transmitted over a physical line.
Multicast	With a multicast, data packets are sent from one point to particular subscribers in a network. In IPv4 this is controlled via the address range 224.0.0.0 to 239.255.255.255 and the IGMP protocol, while in IPv6 it is controlled by ff00::/8 addresses and ICMPv6.
Multifrequency code dialling method	The multifrequency code dialling method, also known as tone dialling, MFV, MFC and DTMF, is a signalling method for automatic telephone routing. Key inputs are represented by overlaid, sinusoidal signals. See also Pulse dialling.
Multilink	With multilink, multiple interfaces (PPP, PPPoE, ...) are combined into a single virtual connection in order to increase the total bandwidth available.
Multiple subscriber number	Multiple subscriber numbers are the individual phone numbers in the ISDN point-to-multipoint connection.
Music on Hold	The term Music On Hold (MOH) refers to automated announcements or hold music on the PBX.
Music on hold	See Music on hold.
MWI	The Message Waiting Indicator (MWI) signals that a new message is available.
NAPT	Network Address Port Translation (NAPT) is another term for PAT. See PAT.
NAT	Network Address Translation (NAT) is used to replace the source and destination IP addresses of a data packet with others. This enables different networks to be connected to one another. See also PAT.
NBNS	Like DNS, NetBIOS Name Service (NBSN) is used in centralised name resolution. See also WINS and DNS.

Netmask	With IPv4 in connection with the IP address, the netmask, also network mask and subnet mask, defines the network by dividing the IP address into network and device parts and thus determining which addresses need to be routed. Example of a netmask: 255.255.255.0. With IPv6 one refers to prefix length.
Network address	A network address is the address of the network as a whole. The network mask and prefix length divide the IP address into the network address and host address (device address). Example of a network address: 192.168.0.250/24
Network direct	See Keypad.
Network route	The network route refers to the route to a particular network.
Network termination	Network termination (NT) refers to a connection or operating type. A terminal is given access to a communication network at the NT interface (connection socket). The connector is called a TAE with an analogue connection, an NTBA with the basic ISDN connection, and NTPMGF with the ISDN Primary Rate Interface. In the NT operation, the gateway is connected to the PABX's external S0 and is an external exchange connection for it. See also TE.
NT	See Network termination.
NTBA	See Network termination.
NTP	The Network Time Protocol (NTP) is used to synchronise the time of day.
NTPMGF	See Network termination.
OAM	OAM is a service for monitoring ATM connections.
Open hold for enquiry	With open hold for enquiry, a call is put on hold and either party can then resume it once more.
OSI model	The OSI model divides the flow of communication between the physical medium and the user level into layers. The requirements at each layer are met by relevant protocols.
OSPF	OSPF is a dynamic routing protocol which is usually used in larger network installations as an alternative to RIP.
PABX	Private Automatic Branch Exchange (PABX) is another expression for a telephone system.

PABX	PABX is another term for a telephone system.
PAP	The Password Authentication Protocol (PAP) is an authentication method for connections via PPP. Unlike with CHAP, the username and password are not sent encrypted.
Parallel call	See Mobile subscriber.
Park	When a call is parked, the connection is held even if the receiver of the terminal involved is replaced or the cable connection is cut off.
PAT	Port and Address Translation (NAT) is used to replace the source and destination IP addresses and source and destination ports of a data packet with others. This enables different networks to be connected to one another. See also NAT.
PBX	Private Branch Exchange (PABX) is another expression for a telephone system.
PDM	See Pulse dialling
Peer	A peer is the endpoint of a communication in the network.
Phase 1/2	See IKE.
Pick-up	With pick-up, calls can be received using code procedures on an internal terminal that is not part of active call allocation.
PIM	The Protocol Independent Multicast (PIM) enables the dynamic routing of multicast packets on the Internet.
PIN	A personal identification number (PIN) can be used to authenticate oneself on the device so that one can use the device's functions.
Ping	Ping is a diagnostic tool that can be used to check whether a particular host in an IP network can be contacted. A measurement is taken of the time interval between sending a data packet (ICMP(v6) echo request packet) and receiving a response packet sent back immediately. This enables the connection quality to be determined.
PKCS	The Public-Key Cryptography Standards (PKCS) are standards for public key cryptography. The PKCS are designed for binary and AS-CII data and are compatible with the X.509 standard. The public standards are PKCS #1, #3, #5, #7, #8, #9, #10, #11, #12 and #15. PKCS #10 describes the syntax for certification inquiries.
PKI	A public key infrastructure (PKI) is used to issue, distribute and veri-

fy digital certificates for an encryption procedure.

PMTU	The Path MTU (PMTU) describes the maximum packet size that can be transmitted along the entire connection route without needing to be fragmented.
Point-to-multipoint	Point-to-multipoint connection is an ISDNB connection. It is used to connect ISDN terminals. Multiple subscriber numbers (MSNs) are provided. See also Point-to-point ISDN access
Point-to-multipoint	See Single phone number (VoIP).
Point-to-point	See Point-to-point ISDN access and Direct dial-in (VoIP).
Point-to-point connection number:	See Point-to-point ISDN access
Point-to-point ISDN access	Point-to-point ISDN access refers to an ISDN connection that is also called point-to-point. It is used to connect a PBX. A point-to-point number and a number block are issued. Each of the numbers in the number block is called a direct dial exception. (Example: Point-to-point connection number: 1234, number block: 1 - 99, numbers of the individual extensions: 1234-1, 1234-2, 1234-3, …) See also Point-to-multipoint connection.
Pool	An address pool is a collection of IP addresses that can be assigned to the connected clients, e. g. by DHCP.
POP3	The Post Office Protocol Version 3 (POP3) is a transmission protocol which controls how a client accesses emails from an email server.
Port	The port number is used to decide the service (telnet, FTP, ...) to which an incoming data packet should be sent.
POTS	Plain Old Telephone System (POTS) refers to the analogue telephone network.
PPP	The Point-to-Point Protocol (PPP) is a standardised technology for setting up a direct connection between the network nodes via dial-up lines.
PPPoA	The Point-to-Point-over-ATM Protocol (PPPoA) enables PPP data packets to be transported directly over an ATM network.
PPPoE	The Point-to-Point-over-Ethernet Protocol (PPPoE) enables PPP data packets to be transported directly over an Ethernet network.

PPTP	The Point-to-Point Tunneling Protocol (PPTP) is a network protocol for encapsulating other protocols so that they can be transported via the Internet Protocol (IP) in the form of a tunnel (VPN). PPTP uses protocol number 1723. The PPTP architecture is divided into two logical systems. The PPTP Access Concentrator (PAC) and the PPTP Network Server (PNS). The PAC is usually integrated into the Windows client. It establishes the connection to the PNS and manages it. The PNS is responsible for routing and controlling the packets received by the PNS.
Pre-shared key	A pre-shared key (PSK) is a key for an encryption procedure. The parties shared the key's value beforehand.
Prefix	See Network address
Prefix delegation	In IPv6 networks, prefix delegation is used to assign the network address (prefix) to the router.
Prefix length	See netmask.
PRI	See Primary Rate Interface.
Primary Rate Interface	The Primary Rate Interface is a network connection to the ISDN. This type of connection is often also called a PRI or S2Minterface. A Primary Rate Interface offers 30 user channels (B channels), each with 64 kbits/s, in Europe and 23 in the USA, one control channel (D channel) with 64 kbits/s and one synchronisation channel with 64 kbits/s in Europe and 8 64 kbits/s in the USA. See also Basic Rate Interface.
Proposal	When an IPSec connection is being established, the initiator of the connection makes proposals with relation to the authentication and encryption methods to be used.
Protocol	Protocols regulate the flow of a data communication on different levels of the OSI model. Protocols control addressing, coding, authentication, formatting, etc. Examples: Ethernet, IP, TCP, HTTP
Proxy	A proxy is a network component. The proxy is an agent. It routes a query from the source with its own IP address to the destination.
Pulse dialling	Pulse dialling is a signalling method for automated telephone routing. Key inputs are represented by a defined number of dc pulses. See also Multifrequency code dialling method (MF).
PVID	The Port VLAN Identifier (PVID) is the standard VLAN ID for the port concerned. A packet that reaches this port without a VLAN tag is as-

signed this ID.

Q-SIG Q-Interface Signalling Protocol (Q-SIG) is an ISDN-based signalling protocol for linking PABX systems.

QoS Quality of Service (QoS) describes the properties of the communication service. It is defined using bandwidth, delay, packet losses and jitter. To transmit time-critical data packets for VoIP or video streaming as quickly as possible, QoS is used to sort all the data packets into groups and forward them on in the network either more quickly or slowly, depending on their priority.

Queue The data packets accumulate in a queue before they are sent.

RADIUS Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol for authenticating, authorising and accounting for users with dial-in connections. The RADIUS server authenticates the client, e. g. by checking the username and password. See also TACACS+.

RE-ADSL2 See G.992.5.

Real Time Jitter Con- Real Time Jitter Control is used, where necessary, to reduce the
trol size of data packets during a telephone conversation so that voice packets are not blocked.

Registrar The SIP server (registrar) needs to be used in case the subscribers to a VoIP call are not using static IP addresses The SIP server registers the clients' IP addresses and sends this data to the SIP proxy, which connects the calls. The SIP proxy and SIP registrar are usually identical.

Reject / reject func- When a phone number that has not been set up in the telephone
tion system is dialled, or if the connection of the party called is engaged, or the party called does not take the call, the reject function determines how to proceed with the call. The call can be routed to a different destination or discarded.

Repeater A repeater is a device that strengthens electric or optical signals and thus increases the range of the network.

Reset This returns the device to its unconfigured state.

RFC A Request For Comments (RFC) is a document that describes the standards and guidelines for the Internet.

Rijndael See AES.

RIP	The Routing Information Protocol (RIP) is a routing protocol. It is restricted to small networks. See also OSPF.
RipeMD 160	RACE Integrity Primitives Evaluation Message Digest (RipeMD 160) is a hash function that generates a 160 bit hash value (checksum). See also Hash.
RJ45	RJ45 refers to a jack or connector with a maximum of eight wires to the digital terminals' connection.
Roaming	With roaming, a client moves through a WLAN logging on and off at different access points in the same network.
Room monitoring	Room monitoring is a performance feature. One can listen in to the sounds in a room.
Router	A router is a network component for connecting different types of network at the network layer of the OSI model. Data packets are transmitted using IP addresses. Routing tables are used to identify the best routes through the network. In order to keep the routing tables up to date, the routers exchange information via routing protocols (e.g. OSPF, RIP).
Router advertisement	Router advertisements are messages that the router sends to the network. They announce the presence of the router in the network. Router announcements are also used to issue prefixes, organise the autoconfiguration and specify the standard router.
Routing	Routing refers to the identifying of routes for sending messages.
RSA	The RSA algorithm (named after its inventors, Rivest, Shamir and Adleman) is used to create digital signatures and encrypt data packets. The signature can be used to verify changes made to the information in the data packet. RSA is used for public-key cryptography (IPSec). See also DSA. Key generation is slower with RSA than with DSA, but key processing is faster.
RTP	The Real-Time Transport Protocol (RTP) is used to transmit audio and video data (streams) via IP-based networks.
RTS threshold	Once the number of frames in the data packet exceeds the RTS threshold, a connection check (RTS/CTS handshake) is run before a data packet is sent.
RTSP	The Real-Time Streaming Protocol (RTSP) controls the transmission of audio and video data (streams) via IP-based networks. While the Real-Time Transport Protocol (RTP) is used to transmit user

data, the main function of RTSP lies in controlling the data streams.

Rule chain   A rule chain contains a combination of different filter rules. A filter rule selects part of the data traffic based on particular features, e. g. the source IP address, and applies an action, e. g. block, on this part.

S0 bus   The S0 bus is an interface for the ISDN Basic Rate Interface, and links multiple ISDN terminals to the NTBA. The bus is implemented by a four-wire circuit. See also UP0.

S2M interface   See Primary Rate Interface.

SA   So-called security associations (SA) receive information about the measures to secure the communication connection. One SA, at least, is a prerequisite for establishing a secure connection. An SA receives the subscriber's IP address, the authentication protocol used, the encryption algorithm used, the security parameter index (SPI), the selector and the period of validity.

SAD   All the parameters that are set while configuring IPSec are stored in the router in the form of databases. These are the Security Policy Database (SPD) and the Security Association Database (SAD). The SAD receives information about every security connection. That is, which encryption algorithms, keys, protocols, session numbers or periods of validity are to be used. For an outgoing connection, an SPD entry displays an SAD entry. In this way, the SPD can specify which SA is to be used for a particular packet. With an incoming connection, the SAD is addressed in order to specify how the packet is to be processed.

SCEP   The Simple Certificate Enrollment Protocol (SCEP) is used to manage digital certificates.

Scheduling   Scheduling refers to the planning of tasks. Particular actions (e. g. deactivating an interface) are triggered by events (e. g. time or changing a MIB variable).

Serial interface   The serial interface is used to exchange data between computers and peripheral devices. It can be used to configure the device or to transmit data via an IP infrastructure (Serial over IP).

Server   A server offers services used by clients.

SFP   Small Form-factor Pluggable (SFP) is a plug-in connector that was developed for extremely fast Ethernet.

SHA1	Secure Hash Algorithm version 1 (SHA1) is a hash function that generates a 160 bit hash value (checksum). See also Hash.
SHDSL	Symmetrical High-bit-rate Digital Subscriber Line. See DSL.
Shell	The shell is an input interface (e. g. command line or graphic user interface) between computer and user.
Short hold	The short hold is the defined amount of time after which a network connection is automatically cleared if no more data is transmitted.
SIF	With a Stateful Inspection Firewall (SIF), the routing of a data packet is not determined only by source and destination addresses but also using dynamic packet filtering based on the connection status.
Simplex operation	Simplex operation is a performance feature. Simplex operations are used to take a call automatically and switch the speaker function on. If the called party lifts the receiver, a normal voice connection is established.
Single phone number (VoIP)	Single phone number access is a VoIP connection that is also known as a point-to-multipoint connection. It is used to connect VoIP terminals. Multiple subscriber numbers (MSNs) are provided. See also Direct dial-in (VoIP)
SIP	The Session Initiation Protocol is a network protocol for setting up a communication session between two or more subscribers. The protocol is used for IP telephony (VoIP).
SIP provider	A SIP provider does the switching between a SIP connection and other analogue, ISDN and VoIP connections.
SMTP	The Simple Mail Transfer Protocol (SMTP) is used to exchange emails.
SNMP	The Simple Network Management Protocol (SNMP) is used to configure, control and monitor different network components (e. g. routers, servers, etc.) from a single, central system. The network component settings that can be changed are stored in a database – the Management Information Base (MIB). SNMP uses UDP. The network component receives requests to port 161 while the managing system receives confirmation messages (TRAPs) at port 162.
SNTP	The Simple Network Time Protocol (SNTP) is used to transmit the time and to synchronise the server and client.
Softkey	A softkey refers to a key whose function is determined by the asso-

ciated screen display.

Spatial streams   Spatial streams are data streams that are sent out at the same time on the same frequency in the wireless LAN. The transmission rate is multiplied as a result.

SPD   All the parameters that are set while configuring IPSec are stored in the router in the form of databases. These are the Security Policy Database (SPD) and the Security Association Database (SAD). The Security Policy Database lists the forms of data traffic that are to be secured. Factors such as the source and destination address of the data packet are used to do this.

Speaker function   With the speaker function, the people present in the room can listen in to the telephone call.

Speed dial number   A speed dial index (000...999) is assigned to every number in the phone book. This speed dial index can be used to dial instead of the long phone number.

Splitter   A broadband access unit, commonly known as a splitter, is used to split signals that come via a subscriber loop into data and telephone lines.

SRTP   The Secure Real-Time Transport Protocol (SRTP) is the variant of the Real-Time Transport Protocol (RTP) that is encrypted using AES.

SSH   Secure Shell (SSH) is a network protocol that can be used to establish an encrypted connection to a device's shell.

SSID   The Service Set Identifier (SSID) defines a wireless network that is based on IEEE 802.11. The SSID is the network name of the wireless LAN. All the access points and clients that belong to the same network use the same SSID. The SSID string can be up to 32 characters long and is placed, unencrypted, in front of all packets. A client uses SSID ANY to contact all the accessible access points. The user is then shown all the available WLANs and he can select the appropriate network. If an access point is used for different networks, each wireless network is given a separate MSSID (Multi Service Set Identifier).

SSL   Secure Sockets Layer (SSL) is a protocol for data encryption. Since version 3.1, the new term Transport Layer Security (TLS) has been used. SSL is mainly used for HTTPS to encrypt the data transmission between web server and web browser.

STAC	STAC is used to reduce the data volume transmitted (data compression).
Static IP Address	In contrast to a dynamic IP address, the static IP address is assigned permanently by the user. Network components such as the web server or printer usually have static IP address, while clients such as notebooks or workstations usually have dynamic IP addresses.
Station guarding	When station guarding is enabled, acoustic call signalling is switched off. This function is also known as Do not disturb.
STUN Server	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). A STUN server enables VoIP devices behind an active NAT to access the network.
Sub-addressing	As well as the ISDN telephone number, a sub-address can also be sent when establishing the connection. This sub-address can transmit any additional information. It can be used, e. g., to systematically address multiple ISDN terminals that can be reached under one telephone number, or to open particular programs on a PC.
Subnet	A sub-network in an IP network is known as a subnet. A subnet is defined like a normal network, via an IP address and (sub-)netmask (IPv4) and prefix length (IPv6). Example: 192.168.1.250/24 (192.168.1.250/255.255.255.0, 256 possible IP addresses) is a subnet of 192.168.1.250/16 (192.168.1.250/255.255.0.0, 65536 possible IP addresses).
Suppress telephone number	See Display caller number (CLIP / CLIR) and Display called party number (COLP / COLR).
Switch	A switch is a network component that connects individual network segments to one another. On the one hand, a switch can be operated as a bridge to the data link layer in the OSI model. Unlike the bridge, however, a switch has more than one input and output. On the other hand, the switch can be operated as a gateway to the network layer in the OSI model. The device comparable to the switch in the physical layer is known as the hub.
Switch contact	A telephone can be used to switch a device connected to the switch contact, e. g. a door opener, on and off.
SWYX	SwyxWare is a software-based communication solution for VoIP.
Syslog	The syslog protocol is used to transmit status messages in an IP

network. In this way, different network components can be monitored from a single, central system. Syslog messages are sent as unencrypted text messages over the UDP port 514.

System telephone   A system telephone has multiple function and special keys and can use the performance features of a PBX.

T.38   T.38 or Fax over IP (FoIP) refers to fax transmission via an IP network.

TA   See Terminal adapter

TACACS+   The Terminal Access Controller Access Control System Plus (TACACS+) is a client-server protocol for authenticating, authorising and accounting for users. The TACACS+ server authenticates the client by checking, e. g., the username and password. In contrast to the UDP-based RADIUS protocol, TACACS+ uses TCP on port 49 and transmits the entire communication encrypted.

TAPI   The Telephony Applications Programming Interface (TAPI) is a programming interface for ISDN. It enables application programs to access ISDN hardware from a PC. See also CAPI.

TCP   The Transmission Control Protocol (TCP) is a connection-oriented protocol. It works on the transport layer of the OSI model. With a connection-oriented protocol, a logical connection is established before transmission and maintained. This enables data to be transmitted reliably. Nonetheless, control information is constantly being sent alongside the actual data packets. This causes the data volume sent to increase. See also UDP.

TCP-ACK packet   An ACK (acknowledgement) signal is used when transmitting data to confirm the receipt or the processing of data or commands. TCP uses ACK signals for communication.

TCU   See Network termination. A distinction is drawn between F-coded connectors for telephones and N-coded connectors for fax machines, modems and answering machines.

TE   Terminal equipment (TE) refers to a connection or operating type. The TE connector is a terminal's connector. In TE operation, the gateway is connected to the PABX's internal S0 and thus constitutes an ISDN terminal. See also NT.

TEI   Under ISDN protocol DSS1, the Terminal Endpoint Identifier (TEI) is an identifier for terminals.

Telefax	See Fax.
Telnet	Telecommunication Network (Telnet) is a network protocol. It enables communication with another, remote device in the network, e. g. PCs, routers, etc.
Terminal adapter	A terminal adapter (TA) can be used to connect terminals to an interface on which they cannot be operated directly, e. g. analogue terminals to an ISDN connection.
TFTP	The Trivial File Transfer Protocol (TFTP) regulates the transmission of files. Compared with FTP, there is no option to display data, issue permissions or authenticate users.
Three-party conference	The three-party conference is a performance feature. Three subscribers can speak to one another on the phone simultaneously.
Tiger 192	Tiger 192 is a hash function that generates a 192 bit hash value (checksum). See also Hash.
Time service	The Time protocol is used to synchronise the date and time. The protocol uses port 37 via TCP and UDP.
Time slot	A time slot is a period of time which is permanently assigned within a transmission frame, and is usually equivalent to one transmission channel.
TLS	See SSL.
Tone dialling	See Multifrequency code dialling method.
TOS	Type of Service (TOS) is a field in the header of IP data packets. It specifies the priority of the data packet. See also QoS.
Traceroute	Traceroute is used to determine which routers will be used to route data packets to the queried destination host.
Trigger	This refers to a trigger impulse.
Triple DES	See DES.
Trunk	A trunk consists of bundled connections or transmission channels. See also Bundle.
TTL	The Time to live (TTL) is the configured period of validity of a data packet. With the Internet Protocol (IP), TTL specifies how many hops a data packet may pass. The maximum value is 255 hops. The

	TTL is reduced by 1 with each hop. If a data packet has not yet reached its destination when its TTL expires, it is discarded.
Twofish	Twofish is an encryption method (see Cipher). Twofish uses a fixed block length of 128 bits. The key length is 128, 192 or 256 bits.
U-ADSL	Universal Asymmetric Digital Subscriber Line (UADSL) is a DSL variant. It was developed as ANSI T1.413 and standardised as G.992.2. U-ADSL enables different communication technologies to be used in parallel, e. g. ISDN and POTS, and does not require a splitter.
UDP	The User Datagram Protocol (UDP) is a connectionless protocol. It works on the transport layer of the OSI model. With a connection-less protocol, no control is integrated for delivering the packet. The control must take place in the application layer. Conversely, UDP is faster than connection-oriented protocols.
ULA	Unique Local Addresses (ULA) are IPv6 addresses that are not routed. They can be used in private networks (e. g. a LAN). ULAs begin with the prefix fd.
UMTS	The Universal Mobile Telecommunications System (UMTS), also known as 3G, is a mobile communications standard with a specified max. data transmission rate of 384 kbit/s and 21 Mbit/s in association with HSPA+.
Unicast	With Unicast, data packets are transmitted from a sender to a single recipient.
UP0	The UP0 connection is an interface for the ISDN Basic Rate Interface, and links one ISDN terminal to the NTBA. The connection is implemented via a two-wire circuit, and offers a greater range than the S0 bus.
UPnP	Universal Plug and Play (UPnP) is used to control devices (audio devices, routers, printers, etc.) from any manufacturer via an IP-based network.
Upstream	The gateway forwards the data from its own network.
URL	A Uniform Resource Locator (URL) identifies a file's storage location. Example: http://www.example.org/index.htp (Internet website)
UUS	With User to User Signalling (USS), text messages can be exchanged with other subscribers.

V.110	V.110 describes a method of aligning bitsteams with 0.6, 1.2, 2.4, 2.8, 7.2, 9.6, 12, 14.4, 19.2 and 38.4 kbit/s with the ISDN bitstream of 64 kbit/s.
VDSL	Very High Speed Digital Subscriber Line. See DSL.
VID	See VLAN.
VLAN	A network can be divided up into one or more logical sub-networks– so-called Virtual Local Area Networks (VLAN) – by the network components no longer forwarding the data packet of a defined sub-network to other sub-networks. Each VLAN is assigned a unique number, This number is called a VLAN ID (VID) and assigned to the data packets in the VLAN tag.
Voice mailbox	A voice mailbox is a user's personal answering machine in a voice-mail system.
Voicemail system	A voicemail system enables voice messages to be stored, accessed and forwarded, like an answering machine, but with more options.
VoIP	Voice over IP (VoIP), also known as IP telephony, refers to the transmitting of voice via an IP network. The telephone is connected and disconnected using signalling protocols, e. g. SIP.
VPN	A virtual private network (VPN) is used to transport private data packets through a public network. The data is separated from the publicly accessible data by being encapsulated in new protocols so that they can be routed to the intended recipient. In this context, one also refers to a tunnel that is established between the private networks of the two connected parties. VPN protocols are IPSec, PPTP, L2TP and GRE.
VSS	The Virtual Service Set (VSS) refers to a prefix for wireless LAN interfaces.
Walled garden	In the context of hotspots, a walled garden refers to the area of the website which is available to users free of charge and without logging in.
WAN	A Wide Area Network (WAN) refers to a network that is spread over a large geographic area. Global WAN networks provide access to the Internet.
WDS	The Wireless Distribution System (WDS) is used to establish a wireless connection between access points.

Web server	A web server provides HTML documents (web pages).
WEP	Wired Equivalent Privacy (WEP) is an encryption protocol for WLANs. The key length is 40 or 104 bits.
WINS	The Windows Internet Name Service (WINS) is a translation of the NetBIOS over TCP/IP network protocol by Microsoft. Like DNS, WINS is used for centralised name resolution. See also DNS.
WLAN	Wireless Local Area Network (Wireless LAN, WLAN) refers to a local wireless network based on the 802.11 standard.
WMM	Wi-Fi Multimedia (WMM) prioritises the data packets from different applications, thus improving the transmission of voice, music and video data in WLAN networks. To do this, WMM provides quality-of-service features (QoS) for IEEE 802.11-based networks.
WPA	Wi-Fi-Protected Access (WPA) is an encryption protocol for WLANs. WPA uses dynamic keys that are based on the Temporal Key Integrity Protocol (TKIP).
WPA 2	Wi-Fi Protected Access (WPA) is an encryption protocol for WLANs. WPA 2 uses AES.
WPA Enterprise	With WPA 1 / 2, WPA Enterprise enables subscribers to be authenticated using the Extensible Authentication Protocol (EAP). After successful authentication, the server transfers a shared key to the client and the access point for data transfer in the WLAN.
WPA-PSK	With WPA 1 / 2, WPA-PSK enables subscribers to be authenticated using pre-shared keys. The access point and the client use the same string for the key calculation in the WLAN. This string needs to be configured by the users.
X.25	X.25 is a standardised series of protocols for wide area networks (WANs) via the telephone network.
X.31	The X.31 standard describes the connecting of ISDN and X.25 systems. It is a standard for connecting card terminals.
X.500	The X.500 standard describes the setting up of a directory service. See also LDAP.
X.509	The X.509 standard describes the generating of certificates for a public key insfrastructure (PKI).
X.75	X.75 is a standardised series of protocols for ISDN networks with a

transmission rate of 64 kbit/s.

XAuth   XAUTH (Extended Authentication) is used to add further authentica-
               tion mechanisms to IKE. After a successful phase 1 authentication,
               the user can be separately identified again. The identifying is done
               using the username and password, PAP, CHAP or hardware-based
               systems.

Zone   A zone refers to a phone number or numbers that begin with the
               same sequence.

Index