Manual
be.IP smart

Advanced Configuration

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.

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 Scope of this manual

On the one hand, this manual describes the commissioning of your **be.IP** from a technical point of view, on the other hand, it describes the menus that can be accessed in the user interface via the link **Show more** and that allow the configuration of advanced functions. The setup by means of the **Assistants** is supported by the online help system.

Chapter 2 Installation

2.1 be.IP smart

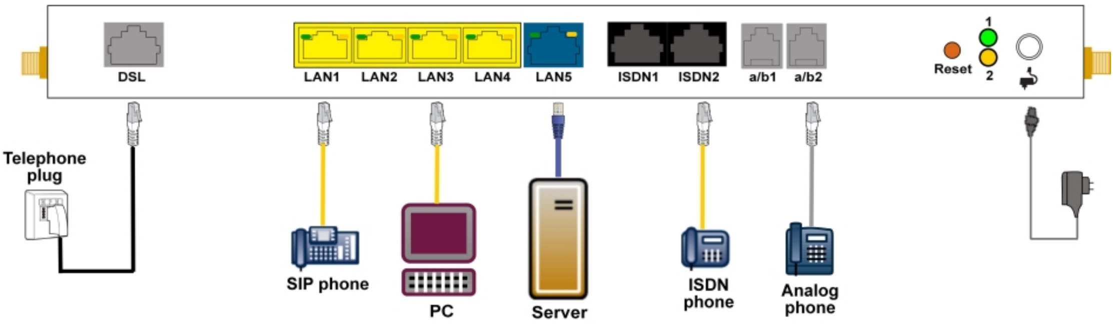
This chapter will show you how to set your device up, connect it and get it working in just a few minutes.

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.

The PDF version of this document contains a slim version of the manual. It comprises all information on installation as well as the description of all configuration parameters, but no screen shots. An HTML-based version containing the screen shots is available as a ZIP file in the download section of your device. Unpack the ZIP file into a folder of your choice and call “start.html” in a web browser.

2.1.1 Setting up and connecting

be.IP smart is operated at a purely IP-based connection. Telephony is exclusively VoIP-based, but your choice of connected devices is not restricted in any way. You can connect SIP and ISDN phones as well as 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!

Set up and connect in the following sequence:

(1) Installation
When operational, **be.IP smart** needs to be wall-mounted in an upright position or well ventilated inside of a device rack (please read chapter *Mounting* on page 7 carefully).

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

(3) Antennas
Screw the standard antennas supplied on to the connectors provided for this purpose

(4) DSL
Connect the **DSL** connector to the TAE plug using the grey cable

(5) ISDN PABX
Connect an ISDN PABX at the internal ISDN connector of the **be.IP smart**. Up0 interfaces are not suported.

(6) SIP telephones

Connect your SIP telephones to the 10/100/1000 Base-T Ethernet interfaces. In a last step connect your PC and follow the instructions from the installation poster.

(7) Analogue telephones

Connect your analogue terminals to the internal interfaces for analogue terminals (a/b1 - a/b2). To do this, use the cable provided with the terminal.

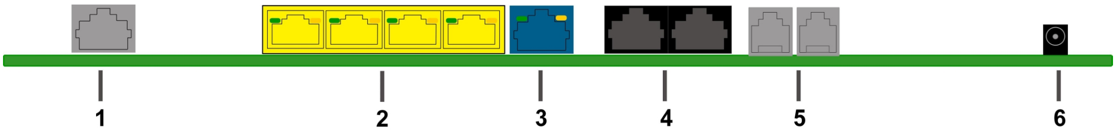
(8) PC

Connect a suitable PC to one of the Ethernet ports of **be.IP smart** using an Ethernet cable. Should you run into any problems with the connection between your C and your **be.IP smart**, read the corresponding sections on the basic configuration of your device.

(9) VoIP

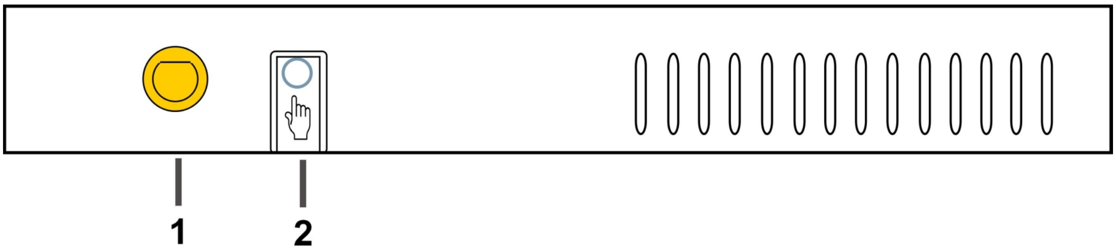
For a pure IP connection without ISDN refer to the instruction provided by your service provider.

2.1.2 Connectors



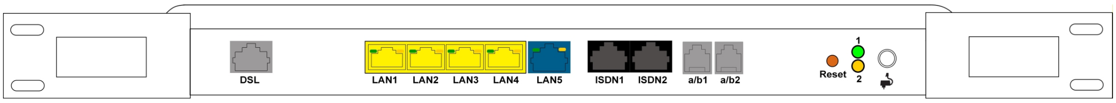
1	DSL interface Annex B/J
2	10/100/1000 Base-T Ethernet interface (LAN1 - LAN4)
3	Ethernet WAN interface (LAN5)
4	Interface for ISDN telephones (ISDN1, ISDN2)
5	Internal interface for analogue telephones (a/b1, a/b 2)
5	Socket for the power supply unit

2.1.3 Connections (on the side)



1	Antenna connector
2	Function button

2.1.4 Mounting brackets



Due to the position of the devices in a rack it is recommended to use remote antenna. Attach the mounting brackets to the device using the supplied screws. The mounting brackets and screws are available as an accessory (Part No. MN40285514).

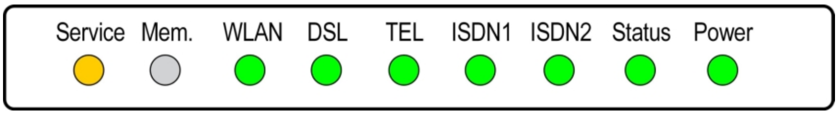
Note

During operation in a rack the ambient temperature must not exceed 40 °C.

2.1.5 LEDs

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

The LEDs on your **be.IP smart** are arranged as follows:



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

LED status display

LED	Colour	Status	Information
Service	Yellow	on	Undergoing automatic maintenance
		off	No automatic maintenance
Mem.			No function
WLAN		off	WLAN or all assigned wireless networks disabled
	Green	slow flashing	Wireless network is enabled, no client is logged in
	Green	flashing quickly	Wireless network is enabled, at least one client is logged in
	Green	flickering	Wireless network is enabled, at least one client is logged in, there is some data traffic
DSL	Green	on	Connection established
	Green	slow flashing	Synchronisation running
		off	No synchronisation
	Green	flickering	Data transfer
TEL	Green	on	Telephony ready at IP connector (Voice over IP)
		off	Telephony not configured
ISDN1 / ISDN 2	Green	on	ISDN telephone system connected
		off	On standby or not functioning
Status	Green	on	After switching on: Device is started While operation: Fault
	Green	slow flashing	The device is active
Power	Green	on	The power supply is connected
		off	No power supply

The LEDs for the Ethernet sockets LAN 1-4 (LAN) and LAN5 (WAN) show the following status information:

Ethernet LEDs

LED	Colour	Status	Information
LAN 1 - 4 (Link/Act)	Green	on	Ethernet connection established

LED	Colour	Status	Information
LAN 1 - 4 (Link/Act)	Green	flashing	Data transmission via Ethernet
LAN 1 - 4 (Link/Act)		off	No Ethernet connection
LAN 1 - 4 (Speed)	Green	on	1000 Mbit/s transfer rate
LAN 1 - 4 (Speed)	Orange	on	100 Mbit/s transfer rate
LAN 1 - 4 (Speed)		off	10 Mbit/s transfer rate
LAN 5 (Link/Act)	Green	on	WAN Ethernet connection established
LAN 5 (Link/Act)	Green	flashing	Data transmission via ETH5t
LAN 5 (Link/Act)		off	No Ethernet connection
LAN 5 (Speed)	Green	on	1000 Mbit/s transfer rate
LAN 5 (Speed)	Orange	on	100 Mbit/s transfer rate
LAN 5 (Speed)		off	10 Mbit/s transfer rate

2.1.6 Scope of supply

Your device is supplied with the following parts:

Product name	Cable sets/other	Documentation
be.IP smart	One Ethernet LAN cable (yellow) One DSL cable (grey) Two FXS adapter for analogue devices (black) Power supply unit Two Wi-Fi antennas	Installation poster Safety instructions

2.1.7 General Product Features

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

General Product Features be.IP smart

Property	
Dimensions and weights:	
Equipment dimensions without cable (B x H x D):	328 x 193 x 44 mm
Weight	approx. 900 g
Transport weight (incl. documentation, cables, packaging)	approx. 1,800 g
Memory	128 MB SDRAM
LEDs	18 (7 x Function, 1 x Service, 5x2 Ethernet)
Power consumption of the device	approx. 24 W 12 V DC

Property	
Voltage supply	12 V DC, 2,5 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:	
DSL interface	Internal DSL modem
Ethernet IEEE 802.3 LAN (4-port switch)	Permanently installed (twisted pair only), 10/100/1000 mbps, auto-sensing, MDIX
ISDN interfaces	2 internal ISDN interfaces, ISDN termination
Available sockets:	
WLAN antennas	R-SMA socket
Ethernet interfaces 1- 4 (LAN)	RJ45 socket
Ethernet interface 5 (WAN)	RJ45 socket
ISDN interface (ISDN1, ISDN2)	RJ12 socket
FXS interface (a/b1 to a/b4)	RJ45 socket
Barrel connector socket for power supply	

2.2 Reset

The reset is performed by using the reset button at the terminal area.

The device is rebooted by quickly pressing the key (ca. one second). Pressing the key is equivalent to an interruption of the power supply. Saved data are preserved, but all connections are interrupted.

If you press the reset key for approx. 30 seconds, the device performs a factory reset. This means the device is returned to its ex works state. Connection data for incoming and for outgoing phone calls are preserved. The configuration is deleted and all passwords are reset.

The reset has finished once the status LED flashes continuously again after approx. 30 seconds.

2.3 Support information

(!TBD!)You can call the free numbers 0800 330 1300 or 0800 330 2870 (for corporate clients) during normal business hours for any further advice on your **be.IP smart**. You can also find more information online at *http://hilfe.telekom.de*. If you think your connection may be faulty, please call Technical Customer Service free of charge at the respective number above, or refer to *http://hilfe.telekom.de*.

Chapter 3 Mounting

Warning

To avoid electric shocks, please take care when connecting telecommunications networks (TNV electric circuits). LAN ports also use RJ connectors.

Caution

To ensure that the **be.IP smart** can operate free of faults, it must be mounted upright on a wall or well ventilated inside of a device rack. The device should not be exposed to direct sunlight or other sources of heat. Please note, too, the gaps that you need to comply with (see *Wall mounting* on page 7).

3.1 Connecting terminals

3.1.1 ISDN connection

In the ex-works state, the ISDN connections of your **be.IP smart** are configured to be internal connections. An adapter which is available as an accessory (Part number 40298094) allows you to operate them as external connections, as well.

To complete the change, settings to adapt the configuration to point-to point or point-to-multipoint connections may be required in the menu **Physical Interfaces**->**ISDN Ports**->**ISDN External**.

The internal ISDN connection on the **be.IP smart** 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.

3.2 Reset button

The reset button which allows you to restart the device or to reset it to the ex works state is located at the terminal area (cf. *Reset* on page 6).

3.3 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 **be.IP smart** 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 in such a way that there is still a gap of about 5 mm between the screw head and the wall.

(8) Hang the **be.IP smart** with the rear brackets from above behind the screw heads.

(9) 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,

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

(11) Connect the **be.IP smart** to the external connections. To do this, you can follow the instructions given on the installation poster provided.

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

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

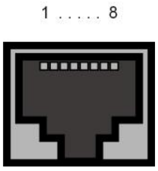
(14) Now you are ready to use the device.

3.4 Pin Assignments

3.4.1 Ethernet interfaces

The devices feature 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 occurs via RJ45 sockets.



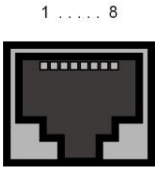
The pin assignment for the Ethernet 10/100/1000 Base-T interface (RJ45 connector) is as follows:

RJ45 socket for Ethernet connection

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

3.4.2 ISDN interface

The connection is made via an RJ45 socket:



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

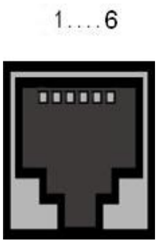
RJ45 socket for ISDN connection

Pin	Function
1	Not used
2	Not used
3	Transmit (+)

Pin	Function
4	Receive (+)
5	Receive (-)
6	Transmit (-)
7	Not used
8	Not used

3.4.3 FXS interfaces

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



The pin assignment for the FXS interface (RJ12 socket) is as follows:

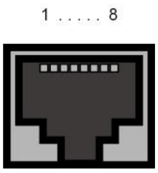
RJ12 socket for FXS connection

Pin	Function
1	Not used
2	Not used
3	FXS
4	FXS
5	Not used
6	Not used

3.4.4 xDSL interface

The **be.IP smart** has an xDSL interface. The xDSL interface is connected via an RJ45 plug.

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



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

RJ45 socket for xDSL connection

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

Chapter 4 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.

4.1 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 *Setting up a PC* on page 12.

Note

If you already run a DHCP server on your LAN, it is recommended that you connect only a single PC to your **be.IP smart** so that a separate network is created.

4.1.1 Automatic configuration

todo: tbd

4.1.2 System software

The device is delivered with the system software version which is current at the time of production. The system software is continually being upgraded to improve the security and functionality of the device. When you first start the device, you may be prompted to update the software. If you have access to Telekom's **automatic configuration**, the system software for your device will automatically be updated to the latest version (see *Automatic configuration* on page 10).

Alternatively, you can update the software in the **Maintenance**->**Software &Configuration**->**Options** menu. For a description of the procedure, see *Software Update be.IP smart* on page 14.

4.1.3 System requirements

To configure the device, your PC must meet the following system requirements:

- Operating system Microsoft Windows XP SP3 or later; Windows XP SP3 requires the following hotfix: http://support.microsoft.com/kb/953761
- Internet Explorer ab Version 7 oder 9 (bei Bedarf sind die Sicherheits- einstellungen anzupassen), Mozilla Firefox ab Version 4, Chrome
- Installed network card (Ethernet)
- Installed TCP/IP protocol
- PC configured to automatically obtain IP address and DNS server
- High colour display to show the graphics correctly

4.1.4 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

- 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 device, you need information that relates to your network environment:

Network settings

Access data	Example value	Your values
IP address of your gateway	*192.168.2.1*	
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. *Telekom*.	
Authentication ID	Enter you ID, e.g. your Email Address	
Password	Enter your password that you received from your SIP provider.	
Registrar	Enter the appropriate registrar, e. g. *tel-t-online.de*.	
Call number	e. g. *123456*	

Data for internet access over xDSL

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*	

4.1.5 Setting up a PC

To access your device via the network and to be able to do a configuration using the configuration interface, 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 the protocol installed:

(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 on **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 (192.168.2.1) 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`).

4.2 Configuring the system

4.2.1 Modify system password

All **be.IP** 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.

4.2.2 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.

4.2.3 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**.

4.3 Setting up an internet connection

You can establish an Internet connection with your device.

4.3.1 Internet connection via the internal VDSL modem

To make it easier to configure an VDSL 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) Use **New** to create a new entry, and copy 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.

4.3.2 Other internet connections

In addition to an VDSL connection over the internal VDSL 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 with configurations of this type.

4.3.3 Testing the configuration

Once you have finished configuring 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. *`192.168.2.1`*). A window appears with the message `"Reply from..."`.

(2) Test the Internet access by entering *www.telekom.de* 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).

4.4 User access

Those who administer and set up the system can set up a personalised configuration access for the users. This will enable the users to view their main personal settings and customise some of them.

Note

Those who administer and set up the system can access the settings and data of all the 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.

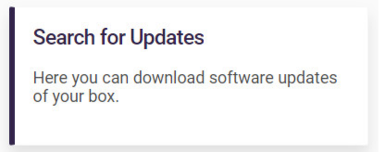
The administrator configures the user accesses in the **Numbering**->**User Settings**->**Users** menu.

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

4.5 Software Update be.IP smart

The functional variety of **be.IP smart** is permanently extended.

The software update can be performed via the **GUI**. Prerequisite for an automatic update is an existing Internet connection. The Home Screen shows the following card:



Search for Updates

Here you can download software updates of your box.

When you click on this card, your device connects the download server and checks whether an updated version of the system software is available. If this is the case, the update will be of your device. After installing the new software, you will be prompted to restart the device.

Caution

The update cannot be aborted after confirming with **Start**. If there should be an error with the update, do not restart the device and contact support.

Chapter 5 Operation via the telephone in PABX mode

The operation and configuration of the system via a connected telephone is described in two separate documents. You will find the document as download under *!!!todo!!!!*

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 Home

7.1 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.

7.1.1 Global Settings

Basic system parameters are managed in the **Global Settings** menu.

7.1.1.1 System

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

The menu consists of the following fields:

Fields in the Basic Settings menu

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. The default value is *Telekom Germany*.
Maximum Number of Syslog Entries	Enter the maximum number of syslog messages that are stored internally in the device. Possible values are *0* to *1000*. The default value is *50*. You can display the stored messages in **Monitoring**->**Internal Log**.
Maximum Message Level of Syslog Entries	Select the priority of system messages above which a log should be created. System messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level *Debug*. Possible values: • *Emergency*: Only messages with emergency priority are recorded. • *Alert*: Messages with emergency and alert priority are recorded. • *Critical*: Messages with emergency, alert and critical priority are re-

Field	Value
	corded. - *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 accounting 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. The option is enabled per default. You can find a detailed description of this function below.

Autosave Configuration

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

As soon as this state has been reached and the configuration session via the browser is terminated without the user actively saving the new configuration, your device automatically saves the new configuration once the HTTP(S) session has timed out.

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

Transfer to busy subscriber

In configuration, you can define whether transfer of a call to an engaged subscriber is possible, or whether the caller hears the busy tone on Off and the call is thus ended. Otherwise, the caller remains on hold and hears the music-on-hold. If the target subscriber hangs up, the subscriber on hold hears the ringing tone if *With Ringing Tone* has been selected, or Music on Hold if *With Music on Hold* has been selected until the target subscriber accepts the call. The target subscriber is called and can take the call on hold.

Fields in the System Settings menu

Field	Value
Transfer Signalling	Set how the connecting to an internal subscriber shut be managed. Possible values: - *With Ringing Tone* (default value): While being transferred, the

Field	Value
	caller hears music on hold from the system; after being transferred, the ringing tone. • *With Music On Hold*: The caller hears the system's on-hold music until the targte subscriber accepts the call.
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	Define where incoming calls should be redirected , e.g., in case of wrong dialling. Possible values: • *None - Busy Tone*: The caller hears the engaged tone by default and cannot be redirected to a destination. • *<Extension number>*: The incoming call is routed to the selected extension. The preset internal number *40 (Team All)* is the default value.
Interconnect external calls	Select whether, while brokering two external subscribers, these should 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 structure between countries, you wish to use the same system in each subsidiary. By setting the country option, the system can be adapted to the specificities of the network in the target country.

As system requirements vary from country to country, the functionality of certain performance features must be customised. Basic settings for different country options are saved in the system.

Fields in the Country Settings menu

Field	Value
Country Profile	Select the country in which the system is to be used. Note: This will not alter the language used in the system menu of the system telephone. Possible values: • *Deutschland* (default value) • *Nederland* • *Great Britain* • *België* • *Italia* • *Danmark* • *España* • *Sverige* • *Norge* • *France*

Field	Value
	• *Portugal* • *Österreich* • *Schweiz* • *Česko* • *Slovenija* • *Polska* • *Magyarország* • *Ellada*
International Prefix / Country Code	The values for **International Prefix / Country Code** are preset . You need this country code if, for example, you wish to automatically generate an international number under **SIP Provider**. You dial the national prefix in the customary way , e.g. 5151 909999, the system then automatically dials +495151 909999. If you do not enter the country code, this can result in wrong dialling; the system then dials +5151 909999. Without the entry **Generate international phone number** (in the **VoIP**->**Settings**->**SIP Provider** menu) and the **International Prefix / Country Code** the complete number including country code must always be dialled with the SIP providers. **Note** Not all SIP providers support this setting.
National Prefix / City Code	The value for the National Prefix is preset. Enter the area code for the city in which your system is installed. Using **National Prefix / City Code** you can automaticalls generate national numbers (see also **Generate national subscriber number** in the **VoIP**->**Settings**->**SIP Provider** menu. This area code is crucial for a point-to-point connection, as otherwise, automatic callback to an external number, for example, is not possible.

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

Fields in the Charge Settings menu

Field	Value
Charge Rate Factor	Enter the factor for the connection costs. The default value is `0,00`.
Currency	Enter the name of the currency, e.g., *EUR* (default value) (max 3-digit) here. This entry is only a name not taken up in any calculation of tariff unit factors. Special characters are not allowed.
Charge Information (S0 / Upn Extension)	Select the transmission method for charging information at the internal S0 bus. Possible values: • *Keypad*: Depending on the country and provider, the charging information is transmitted so as to allow direct display by the terminal. • *Functional*: Charging information is transmitted in a binary code and must first be decoded by the terminals (EURO ISDN). • *Both* (default value): Both protocols are recognised.

Night operation

You can switch the system to night operation and thus enable certain call options for team signalling, intercom signalling and redirect functions.

Advanced switching of call options is possible via a code, or the calendar configured for night operation. You configure a calendar for night operation in the **Applications**->**Calendar**->**Calendar**->**New** menu.

Fields in the Night Mode menu

Field	Value
Team Signalling	Select the call option for team signalling in night operation.
Doorcom Signalling	Select the intercom call option for intercom signalling in night operation.

7.1.1.2 System (Media Gateway)

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

The menu consists of the following fields:

Fields in the Basic Settings menu

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. The default value is `Telekom Germany`.
Maximum Number of Syslog Entries	Enter the maximum number of syslog messages that are stored internally in the device. Possible values are `0` to `1000`. The default value is `50`. You can display the stored messages in **Monitoring**->**Internal Log**.
Maximum Message Level of Syslog Entries	Select the priority of system messages above which a log should be created. System messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level `Debug`. Possible values: • `Emergency`: Only messages with emergency priority are recorded. • `Alert`: Messages with emergency and alert priority are recorded. • `Critical`: Messages with emergency, alert and critical priority are recorded.

Field	Value
	• *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 accounting 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. The option is enabled per default. You can find a detailed description of this function below.

Autosave Configuration

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

As soon as this state has been reached and the configuration session via the browser is terminated without the user actively saving the new configuration, your device automatically saves the new configuration once the HTTP(S) session has timed out.

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

7.1.1.3 Passwords

Setting the passwords is another basic system setting.

> ☞ **Note**
>
> All devices are delivered with the same username, password and PIN. As long as the passwords or PIN's remain unchanged, they are thus not protected against unauthorised use.
>
> Make sure you change all the passwords and PIN's to prevent unauthorised access to the device
>
> If the password is not changed, under **System Management**->**Status** there appears the warning: "System password not changed!"

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

Fields in the System Password menu

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

PIN1 and PIN2

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

PIN1 is a 4-digit PIN that allows you to protect system settings from unauthorised access. PIN2 is a 6-digit PIN number that prevents use of your system by unauthorised remote users. These functions can only be used after entering a 6-digit PIN2.

Various settings are protected by the system PIN1. In the basic setting, PIN1 is set to *none*.

The following performance features are protected by PIN2:

- Remote access for 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 shall be permitted on your system. The function is enabled 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*. With the 6-digit **PIN2** you protect the access from outside (remote access). **Note** Change the default value of **PIN2** to allow external access.

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).

Field	Value
	The function is enabled with *Show* The function is disabled by default. If you activate the function, passwords and keys are displayed and can be edited as plain text with the following exceptions: • IPSec keys: These can only be entered, but not edited in plain text. After clicking **OK** or calling the menu again, they will be displayed as an asterisk. • The internet connection password: Since this is usually set via automatic configuration, it cannot be displayed in this way.

7.1.1.4 Passwords (Media Gateway)

Setting the passwords is another basic system setting.

Note

All 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
Password	Enter the password for the user name `admin`. The default value is *admin*. This password is also used with SNMPv3 for authentication (MD5) and encryption (DES).
Confirm Password	Confirm the password by entering it again.

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. If you press **OK** or call the menu again, they are displayed as asterisks.

7.1.1.5 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):

Manual

The switch from summer to winter time (and back) occurs 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	Only for devices with an ISDN interface. Determine whether the system time is to be updated via ISDN.

Field	Description
	If a time server is configured, the time is only determined over ISDN until a successful update is received from this time server. Updating over ISDN is deactivated for the period in which the time is determined by means of a time server. The function is activated by selecting *Enabled*. The function is disabled by default.
First Timeserver	Enter the primary time server, by using either a domain name or an IP address. In addition, select the protocol for the time server request. Possible values: • *SNTP* (default value): This server uses the simple network time protocol with 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. The server *ntp1.sda.t-online.de* is entered here in the ex works state.
Second Timeserver	Enter the secondary time server, 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 with 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. The server *ntp1.sul.t-online.de* is entered here in the ex works state.
Third Timeserver	Enter the tertiary time server, 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 with 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 up-

Field	Description
	dated. 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, then every 10 seconds. • *Endless*: For an unlimited period, the system attempts to contact the time server after 1, 2, 4, 8 seconds, 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. Time requests from clients in the LAN are answered.

7.1.1.6 Timer

In the **Timer** menu, you can configure the times after which specific 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 after which **Call Forwarding (CFNR)** occurs. Possible values are *1* to *99*. The default value is *15*.
Direct Call	Enter the time from when the receiver is picked up at which the configured number is dialled. 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. Possible values are *1* to *30*. The default value is *5*.
External Door Connec-	If an intercom call is queried by an external telephone, you can set the

Field	Description
tions	period after which this call is disconnected here. Possible values: • *infinite* • *60 seconds* • *120 seconds* • *180 seconds* (default value) • *240 seconds* • *300 seconds*

Fields in the Timer Settings menu

Field	Value
Explicit Call Transfer	Enter the time after which another call or call waiting is to occur to the initiating subscriber, if the desired subscriber cannot be reached. You have forwarded a caller to another subscriber via transfer or relay. This subscriber could not be reached or is engaged. However, you wish to avoid the subscriber ending the call or being redirected by the system after time. This is achieved by an automatic callback to your phone. For calls forwarded without announcement (special transfer types, UbA), there is a callback or call waiting (if a new call is already in progress) 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 after which a subscriber on hold is reconnected to the exchange. The exchange wishes to transfer a call to a specific employee. However, he/she is presently on the phone. In this case, the call can be switched to the subscriber's queue. If the call is not picked up within the period defined here, the switchboard is called again. Possible values are *10* to *600*. The default value is *30*.
System Parked Enquiry	Enter the period after which an open inquiry is terminated, and the subscriber is called again or has a call waiting. You're conducting a call and wish to transfer it to a colleague. Unfortunately, you're not sure of this colleague's current whereabouts. With **System Parked Enquiry**, the subscriber is held in the system's queue. From your telephone, you can now make an announcement advising your colleague of the waiting call. Using a code on the open inquiry, your colleague can take the call from any telephone. If a call held in the queue is not taken by a subscriber within the period entered here, there is a callback or call waiting to the initiating subscriber. Possible values are *10* to *600*. The default value is *30*.

7.1.1.7 System Licences

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

The options for editing, adding and restoring licenses are usually not needed.

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 that your system does not support.

The **System Licence ID** is also displayed above the list.

Note

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

7.1.1.7.1 Edit or New

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

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**.

(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.

7.1.2 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)

7.1.2.1 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*, after you click the **OK** button, a new bridge group is automatically created.
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.

7.1.2.1.1 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.

7.1.3 Administrative Access

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

7.1.3.1 Access

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

For each Ethernet interface you can select the access parameters *HTTP*, *HTTPS*, *Ping* and for the ISDN interfaces *ISDN Login* options can be selected.

You can also authorise your device for maintenance work to be done by Telekom's Customer Service department. To do this you enable, depending on the service required, the **Service Call Ticket (SSH Web-Access)** option or the **Automatic Configuration (TR-069)** option and select the **OK** button. Follow the instructions given by Telekom's Customer Service.

The **Service Call Ticket (SSH Web-Access)** option is disabled by default, the **Automatic Configuration (TR-069)** option is enabled by default.

7.1.3.1.1 Add

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

Fields in the Access menu

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

7.1.4 Remote Authentication

This menu contains the settings for user authentication.

7.1.4.1 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

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

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

7.1.4.1.1 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 standard applications, leave the value set to *Default*. Possible values: • *France Telecom*: For France Telecom 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.

Field	Value
Default User Password	Some Radius servers require a user password for each RADIUS request. Enter the password that your device sends as the default user password in the prompt for the dialout routes on the RADIUS server.
Priority	If a number of RADIUS server entries were created, the server with the highest priority is used first. If this server does not answer, the server with the next-highest priority is used. Possible values from *0* (highest priority) to *7* (lowest priority). The default value is *0*. See also **Policy** under **Server Options**.
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 configuration. • *<Group Name>*: Select a predefined group from the list.

The **Server Options** menu consists of the following fields:

Fields in the Server Options 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 until your device receives a response from a server configured as authoritative.
UDP Port	Enter the UDP port to be used for RADIUS data. RFC 2138 defines the default ports 1812 for authentication (1645 in older RFCs) and 1813 for accounting (4,180.84 cm 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*.

Field	Value
	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 accessible, **Status** is reset to *alive* . 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 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.

7.1.4.2 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:

Field	Description
	• `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 activated by default.

7.1.5 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.

7.1.5.1 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 ↻.

7.1.5.1.1 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**. The function is enabled with `Enabled`. The function is disabled by default.

Fields in the menu Navigation Entries

Field	Description
Navigation Entries	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: • `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.

7.1.5.2 Users

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

There are no preconfigured users.

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

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

7.1.5.2.1 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.
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.

Field	Description
	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**.

7.1.6 Certificates

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

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

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

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

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

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

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

7.1.6.1 Certificate List

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

7.1.6.1.1 Edit

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

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

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

Fields in the Edit parameters menu

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

7.1.6.1.2 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* (standard value) and *DSA* are available. Also select the length of the key to be created. Possible values: *512*, *768*, *1024*, *1536*, *2048*, *4096*. Please note that a key with a length of 512 bits could be rated 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.beispiel.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.

Field	Description
	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.
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.
E-mail	Only for **Custom** = disabled. Enter the e-mail address according to CA.

Field	Description
Organizational Unit	Only for **Custom** = disabled. Enter the organisational unit according to CA.
Organization	Only for **Custom** = disabled. Enter the organisation according to CA.
Local	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.

Field 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.

7.1.6.1.3 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. Enter the password here.

7.1.6.2 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.

7.1.6.2.1 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*
Password	Enter the password to be used for the import.

7.1.6.3 Certificate Servers

A list of all 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.

7.1.6.3.1 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.

7.2 Local Services

This menu offers services for the following application areas:

7.2.1 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.

Caution

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of **be.IP** 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.

7.2.1.1 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.

7.2.1.1.1 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.
Description	Only for **Event List** *New* Enter your chosen designation for the **Event List**.
Event Type	Select the type of initiator. Possible values: • *Time* (default value): The operations configured and assigned in **Actions** are initiated at specific points in time. • *MIB/SNMP*: The operations configured and assigned in **Actions** are initiated when the defined MIB variables assumes the assigned values. • *Interface Status*: Operations configured and assigned in **Actions** are initiated, when the defined interfaces take on a specified status. • *Interface Traffic*: Operations configured and assigned in **Actions** are initiated when the data traffic on the specified interfaces falls below or exceeds the defined value. • *Ping Test*: Operations configured and assigned in **Actions** are initiated when the specified IP address is / is not accessible. • *Certificate Lifetime*: Operations configured and assigned in **Actions** are initiated when the defined period of validity is reached. • *Function Button*: The option *Function Button* determines that pushing the function button on the device can serve as a trigger for any configured action. Pushing the button for approx. one second (but less than three seconds) sets the button status to *Active*, pushing it for more than three seconds sets it to *Inactive*. Actions depending on the state of the button are then carried out after the next cyclical query determined by the **Schedule Interval**. In this way, e.g., a WLAN interface can be activated when the button is pushed 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

Field	Description
	MIB variables present in the respective area are displayed.
Compare Condition	Only for **Event Type** *MIB/SNMP* Select whether the MIB variable *Greater* (default value), *Equal*, *Less*, *Not Equal* must have the value given in *Compare Value* or must lie within *Range* to initiate the operation.
Compare Value	Only for **Event Type** *MIB/SNMP* Enter the value of the MIB variable.
Index Variables	Only for **Event Type** *MIB/SNMP* If required, select MIB variables to uniquely identify a specific data set in a **MIB Table**, e.g. *ConnIfIndex*. The combination of **Index Variable** (normally an index variable labelled by a *) and **Index Value** creates the unique identification of a specific table entry. Create additional **Index Variables** with **Add**.
Monitored Interface	Only for **Event Type** *Interface Status* and *Interface Traffic* Select the interface whose defined status or data traffic shall initiate an event.
Interface Status	Only for **Event Type** *Interface Status* Select the status that the interface must have in order to initiate the intended operation. Possible values: • *Up* (default value): The function is enabled. • *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*

Field	Description
	Enter an IP address to be used as sender address for the ping test. Possible values: • *Automatic* (default value): The IP address of the interface over which the ping is sent is automatically entered as sender address. • *Specific*: Enter the desired IP address in the input field.
Status	Only for **Event Type** *Ping Test* Select whether **Destination IP Address** *Reacheable* must be (default value) or *Unreacheable* in order to initiate the 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. The default value is *3*.
Monitored Certificate	Only for **Event Type** *Certificate Lifetime* Select the certificate whose validity should be checked.
Remaining Validity	Only for **Event Type** *Certificate Lifetime* Indicate the remaining validity of the certificate in percentage.
Function Button Status	Only for **Event Type** *Function Button*. When creating the trigger the dropdown selection **Function Button Status** allows you to choose which status of the function button activates or deactivates the trigger. If you set the status to *On*, the trigger becomes active if the status of the function button is *Active*, and inactive, if the state of the function button is *Inactive*. If your set it to *Off*, the trigger becomes active if the state of the function button is *Inactive*, and inactive if the state of the function button is *Active*. The current state is checked cyclically at the configured schedule interval.

Fields in the Select time interval menu

Field	Description
Time Condition	Only for **Event Type** = *Time* First select the type of time entry in **Condition Type**. Possible values: • *Weekday* : Select a weekday in **Condition Settings**. • *Periods* (default value): In **Condition Settings**, select a 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*.

Field	Description
	Possible values for **Condition Settings** in **Condition Type** = *Periods*: • *Daily* : The initiator becomes active daily (default value). • *Monday - Friday* : The initiator becomes active daily from Monday to Friday. • *Monday - Saturday* : The initiator becomes active daily from Monday to Saturday. • *Saturday - Sunday* : The initiator becomes active on Saturdays and Sundays. Possible values for **Condition Settings** in **Condition Type** = *Day of Month*: *1* ... *31*.
Start Time	Enter the time from which the initiator is to be activated. Activation is carried on the next scheduling interval. the default value of this interval is 55 seconds.
Stop Time	Enter the time from which the initiator is to be deactivated. Deactivation is carried on the next scheduling interval. If you do not enter a **Stop Time** or set a **Stop Time** = **Start Time**, the initiator is activated, and deactivated after 10 seconds.

7.2.1.2 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**.

7.2.1.2.1 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.

Field	Description
	• *5.8 GHz WLAN Bandscan*: Only for devices with a wireless LAN. A scan of the 5.8 GHz frequency range is performed. • *WLC: New Neighbor Scan*: Only for devices with a WLAN controller. A Neighbor Scan is initiated by the WLAN network controlled by the WLAN controller. • *WLC: VSS State*: Only for devices with a WLAN controller. The status of a wireless network is modified. • *WLAN: Operation Mode*: The operating mode of a WLAN radio module is modified.
Event List	Select the event list you want which has been created in **Local Services**->**Scheduling**->**Trigger**.
Event List Condition	For the selected chains of events, select how many of the configured events must occur for the operation to be initiated. Possible values: • *All* (default value): The operation is initiated if all events occur. • *One*: The operation is initiated if a single event occurs. • *None*: The operation is triggered if no event occurs. • *One not*: The operation is triggered if one of the events does not occur.
Reboot device after	Only if **Command Type** = *Reboot* Enter the timespan in seconds that must elapse after occurrence of the event until the device is restarted. The default value is *60* seconds.
MIB/SNMP Variable to add/edit	Only if **Command Type** = *MIB/SNMP* Select the MIB table in which the MIB variable whose value shall be changed is saved. First, select the **System**, then the **MIB Table**. Only the MIB tables present in the respective area are displayed.
Command Mode	Only if **Command Type** = *MIB/SNMP* Select how the MIB entry is to be manipulated. Possible settings: • *Change existing entry* (default value): An existing entry shall be modified. • *Create new MIB entry*: A new entry shall be created.
Index Variables	Only if **Command Type** = *MIB/SNMP* Where required, select MIB variables to uniquely identify a specific data set in **MIB Table**, e.g. *ConnIfIndex*. The unique identification of a particular table entry is derived from the combination of **Index Variable** (usually an index variable which is flagged with *) and **Index Value**. 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.

Field	Description
	Possible values: • *Active* (default value): The value of the MIB variable is modified if the initiator is active. • *Inactive*: The value of the MIB variable is modified if the initiator is inactive. • *Both*: The value of the MIB variable is differentially modified if the initiator status changes.
MIB Variables	Only if **Command Type** = *MIB/SNMP* Select the MIB variable whose value is to be configured as dependent upon initiator status. If the initiator is active (**Trigger Status** *Active*), the MIB variable is described with the value entered in **Active Value**. If the initiator is inactive (**Trigger Status** *Inactive*), the MIB variable is described with the value entered in **Inactive Value**. If the MIB variable is to be modified, depending on whether the initiator is active or inactive (**Trigger Status** *Both*), it is described with an active initiator with the value entered in **Active Value** and with an inactive initiator with the value in **Inactive Value**. Use **Add** to create more entries.
Interface	Only if **Command Type** = *Interface Status* Select the interface whose status should be changed.
Set interface status	Only if **Command Type** = *Interface Status* Select the status to be set for the interface. Possible values: • *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

Field	Description
	server that you define in *Server URL*. • *HTTPS Server*: The latest software will be downloaded from an HTTPS server that you define in *Server URL*. • *TFTP Server*: The latest software will be downloaded from an TFTP server that you define in *Server URL*.
Server URL	Where **Command Type** = *Software Update* if **Source Location** not *Current Software from Update Server* Enter the URL of the server from which the desired software version is to be retrieved. Where **Command Type** = *Configuration Management* with **Action** = *Import configuration* or *Export configuration* Enter the URL of the server from which a configuration file is to be retrieved, or on which the configuration file is to be backed up.
File Name	For **Command Type** = *Software Update* Enter the file name of the software version. Where **Command Type** = *Certificate Management* with **Action** = *Import certificate* Enter the file name of the certificate file.
Action	For **Command Type** = *Configuration Management* Select which operation is to be performed on a configuration file. Possible values: • *Import configuration* (default value) • *Export configuration* • *Rename configuration* • *Delete configuration* • *Copy configuration* For **Command Type** = *Certificate Management* Select which operation you wish to perform on a certificate file. Possible values: • *Import certificate* (default value) • *Delete certificate* • *SCEP*
Protocol	Only for **Command Type** = *Certificate Management* and *Configuration Management* if **Action** = *Import configuration* Select the protocol for the data transfer. Possible values: • *HTTP* (default value) • *HTTPS* • *TFTP*
CSV File Format	Only where **Command Type** = *Configuration Management* and **Ac-**

Field	Description
	tion = *Import configuration* or *Export configuration* Select whether the file is to be sent in the CSV format. The CSV format can easily be read and modified. In addition, you can view the corresponding file clearly using Microsoft Excel for example. The function is enabled by default.
Remote File Name	Only if **Command Type** = *Configuration Management* For **Action** = *Import configuration* Enter the name of the file under which it is saved on the server from which it is to be retrieved. For **Action** = *Export configuration* Enter the file name under which it should be saved on the server.
Local File Name	Only where **Command Type** = *Configuration Management* and **Action** = *Import configuration*, *Rename configuration* or *Copy configuration* At import, renaming or copying enter a name for the configuration file under which to save it locally on the device.
File Name in Flash	Where **Command Type** = *Configuration Management* and **Action** = *Export configuration* Select the file to be exported. Where **Command Type** = *Configuration Management* and **Action** = *Rename configuration* Select the file to be renamed. 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. The default value is *3*.
Server Address	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter the URL of the server from which a certificate file is to be retrieved.
Local Certificate Description	Where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Enter a description for the certificate under which to save it on the device. Where **Command Type** = *Certificate Management* and **Action** = *Delete certificate* Select the certificate to be deleted.
Password for protected Certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to use a secure certificate requiring a password and enter it into the entry field. The function is disabled by default.
Overwrite similar certificate	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to overwrite a certificate already present on the your

Field	Description
	device with the new one. The function is disabled by default.
Write certificate in configuration	Only where **Command Type** = *Certificate Management* and **Action** = *Import certificate* Select whether to integrate the certificate in a configuration file; and if so, select the desired configuration file. The function is disabled by default.
Certificate Request Description	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a description under which the SCEP certificate on your device is to be saved.
URL SCEP Server URL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter the URL of the SCEP server, e.g. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Your CA administrator can provide you with the necessary data.
Subject Name	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Enter a subject name with attributes. Example: *"CN=VPNServer, DC=mydomain, DC=com, c=DE"*
CA Name	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* 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.

Field	Description
	The function is enabled by default.
Use CRL	Only where **Command Type** = *Certificate Management* and **Action** = *SCEP* Define the extent to which certificate revocation lists (CRLs) are to be included in the validation of certificates issued by the owner of this certificate. Possible values: • *Auto* (default value): In case there is an entry for a CDP, CRL distribution point this should be evaluated in addition to the CRLs globally configured in the device. • *Yes*: CRLs are always checked. • *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.

7.2.1.3 Options

You configure the schedule interval in the **Local Services**->**Scheduling**->**Options** menu.

The menu consists of the following fields:

Fields in the Scheduling Options menu

Field	Description
Schedule Interval	Select whether the schedule interval is to be enabled. Enter the interval in seconds after which the system checks whether events have occured. Possible values are *0* to *65535*. The value *300* is recommended (5 minute accuracy).

7.3 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.

7.3.1 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.

7.3.1.1 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**.

7.3.1.1.1 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.

7.3.2 Diagnostics

In the **Maintenance**->**Diagnostics** menu, you can test the availability of individual hosts, the resolution of domain names and certain routes.

7.3.2.1 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*

Field	Description
	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.

7.3.2.2 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 DSN test is launched by entering the domain name to be tested in **DNS Address** and clicking the **Go** button.

7.3.2.3 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.

7.3.3 Trace

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.

7.3.3.1 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.

7.3.3.2 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.

7.3.4 Software & Configuration

You can use this menu to manage the software version of your device, your configuration files and the language of the **GUI**.

7.3.4.1 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.

> ⚠ **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.

⚠ **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. 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 *http://telekom.de/hilfe* 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.

Field	Description
	- *Import Additional Files (to usb storage)*: You can upload additional files to the USB memory. Choose which file to load under **File Name** - *Import Voice Mail Wave Files*: In **file name**, select the *vms_wavfiles.zip* file that you wish to import. - *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. - *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* Define whether the selected **Action** should also be applied for certificates and keys. The function is activated by selecting *Enabled*. The function is enabled by default.
Configuration Encryption	Only for **Action** = *Import configuration*, *Export configuration*, *Export configuration with state information*. Define whether the data of the selected **Action** are to be encrypted. The function is activated by selecting *Enabled*. The function is disabled by default. If the function is enabled, you can enter the **Password** in the text field.
Filename	Only for **Action** = *Import configuration*, *Import language Update system software*. Enter the path and name of the file or select the file with **Browse...** via the explorer/finder.
Source File Name	Only for **Action** = *Copy configuration* Select the source file to be copied.
Destination File Name	Only for **Action** = *Copy configuration* Enter the name of the copy.
Select file	Only for **Action** = *Rename configuration*, *Delete configuration* or *Delete software/firmware* Select the file or configuration to be renamed or deleted.
New File Name	Only for **Action** = *Rename configuration* Enter the new name of the configuration file.
Source Location	Only for **Action** = *Update system software* Select the source of the update. Possible values:

Field	Description
	• *Local File* (default value): The system software file is stored locally on your PC. • *HTTP Server*: The file is stored on a remote server specified in the **URL**. • *Current Software from Update Server*: The file is on the official update server.
URL	Only for **Action** = *Update system software* and **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.

7.3.5 Update System Phones

In the **Maintenance**->**Update System Phones** menu you can update the software for your system telephones.

7.3.5.1 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 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

Field	Description
	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.

7.3.6 Reboot

7.3.6.1 System Reboot

In this menu, you can trigger an immediate reboot of your device. Once the system has restarted, you must call the configuration interface again and log back in.

Pay attention to the LEDs on your device. For information on the meaning of the LEDs, see the **Technical Data** sect1 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 on the **OK** button. The device will reboot.

7.3.7 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.

Note

Note that connected IP devices should be briefly disconnected from the power supply in order for the system to properly discover them again.

7.4 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.

7.4.1 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.

7.4.1.1 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.

7.4.1.1.1 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* - *local7*. The default value is *local0*.
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 sys-

Field	Description
	log 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*

7.4.2 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).

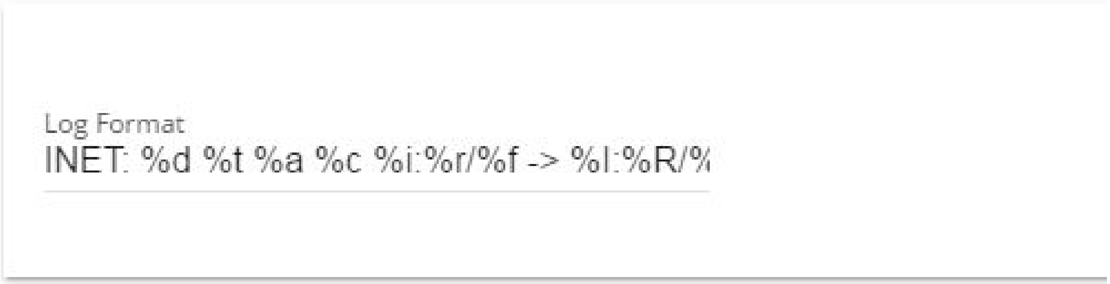
7.4.2.1 Interfaces

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.

7.4.2.2 Options

In this menu, you configure general settings for IP Accounting.



Log Format
INET: %d %t %a %c %i:%r/%f -> %l:%R/%

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

Field	Description
%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]*

7.4.3 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.

7.4.3.1 Alert Recipient

A list of Syslog messages is displayed in the **Alert Recipient** menu.

7.4.3.1.1 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.

Field	Description
Subject	You can enter a subject.
Event	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 Rough 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*.
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*.

7.4.3.2 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*.

Field	Description
	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. 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.

7.4.4 SIA

7.4.4.1 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.

7.5 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.

7.5.1 Internal Log

7.5.1.1 System Messages

In the **Monitoring**->**Internal Log**->**System Messages** menu, a list of all internally stored system messages is displayed. Above the table, you'll find the configured **Maximum Number of Syslog Entries** and the configured **Maximum Message Level of Syslog Entries**. 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.

Chapter 8 Telefonie

8.1 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.

8.1.1 Access Codes

To operate certain performance features in day-to-day operations, you've used codes which you'd like to continue employing with your new system. However, other codes are configured in the basic setting for these performance features. No problem--you can individually extend the codes for individual performance features. Thus, you'll be able to continue using these performance features with your accustomed codes.

8.1.1.1 Alternative Access Codes

In the **Alternative Access Codes** menu, you configure the system's access code plan.

For certain performance features, the access numbers can be individually set in the system configuration. Here, the preset system access number is completed by a call number from the internal system dial plan. For performance features **Open inquiry** and **Bundles**, several access codes can be assigned. Operation of performance features with a modified code occurs as described for the corresponding performance feature You can either use the modified code (internal number) or the code described in the user's guide (except exchange 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 (Extension)**.
Assign project codes	Enter the new access code for the **Assign project codes** feature.
Speed Dial	Enter the new access code for the **Speed Dial** feature.
Trunk Group Selection	Create the new access codes for the **Trunk Group Selection** feature. For this, first create a bundle selection by clicking **Add**, select the bundle and enter the desired code for the bundle.

Field	Description
System Parking (Open Enquiry)	Create the new access codes for the **System Parking (Open Enquiry)** feature. For this, first create a queue for the caller to be held by clicking **Add**, then enter the desired code for the queue. You can create up to 10 entries.

8.2 Physical Interfaces

8.2.1 ISDN Ports (PABX)

The ISDN connections of the system are as internal ISDN connections provided for connecting various ISDN terminals (system telephones, ISDN telephones, ...).

> **Note**
>
> Without an adapter which is available as an accessory, both ISDN connections can only be operated as internal ISDN connections (NT mode). If you have connected the adapter, you can switch the corresponding port to external operation (TE mode) in this menu.
>
> Note that switching the operation mode is only possible if your device has been manufactured in 2016. You can determine if this is the case if a unique WLAN password is printed on the type label of your device.

8.2.1.1 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).

8.2.1.1.1 Edit

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.
Name	Shows the name of the ISDN interface. Possible values: • *`Module Slot`* : Displays the slot in which the module with the ISDN interface is inserted. • *`/`*: Displays the port on the module to which the ISDN connection is connected. • *`S/U`*: 4 wire (S) Example: *`Module slot 3/2 S/U`* = The interface is located on the module inserted in slot 3 on port 2, and is used as an S connection.
Access Configuration	Select whether the ISDN interface will be operated as a point-to-multipoint connection or as a point-to-point connection.

Field	Description
	Possible values: • *ISDN P-MP* (default value) • *ISDN P-P*

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

Fields in the Advanced Settings menu.

Field	Description
Permanent Layer 2 Activation	This function (also known as permanent monitoring) constantly 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.

8.2.1.2 ISDN Internal

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

The internal ISDN interfaces are designed for connecting different kinds of ISDN terminals (system phones, ISDN phones, etc.)

Two predefined entries with the parameters **Name** = *S/U* 1, **Usage** = *S0*, **Default MSN** = *30 (ISDN 30)*

and *S/U* 2, **Function** = **Default MSN** *S0* and **Default MSN** = *35 (ISDN 35)*

are displayed.

Internal ISDN connections are always point-to-multipoint connections

When connecting terminals to an internal ISDN connection, please note that not all commercially available ISDN terminals can use the performance features offered 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	Displays the designation of the ISDN interface.
Function	Displays the function of the ISDN interface. Possible value: • *S0*: Interface for ISDN S0 connection.

Field	Description
Default MSN	Shows whether a standard MSN has been assigned for an internal S0 bus. You cannot access configured S0 terminals via a standard MSN. As standard MSN, you can dial internal numbers that have been configured in the **Numbering**->**User Settings**->**Users** menu and which have been assigned to a terminal in the **Terminals** menu.
Status	Displays the status of the interface.

8.2.1.2.1 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 required extension. You can dial under the numbers that you have configured in the **Numbering**->**User Settings**->**Users**->**Numbers** menu. Possible values: • *Not configured* • *<Number>*

8.2.1.3 ISDN Configuration

Switching the ISDN connections to external operation (TE mode) requires an adapter that is available as an accessory. Otherwise, both ISDN connections can only be operated as internal connections (NT mode). If you have attached the respective adapter, you can switch the corresponding port to external operation in this menu (if you use the device as a phone system (PBX).

8.2.2 Analogue Ports

8.2.2.1 Analogue Internal (FXS)

All of your system's available analogue internal connections are displayed in the **Analogue Internal (FXS)** menu.

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

Fields in the Analogue Internal (FXS) menu

Field	Description
Name	Displays the designation of the analogue interface.
Usage	Displays the function of the analogue interface. Possible values: • *Telephone* • *Doorcom Units* • *Multi Function Device/Telefax* • *Modem*

Field	Description
	• *Answering Machine* • *Emergency Phone* The analogue terminal's function is configured in the **Terminals**->**Other phones**->**analog** menu.
Status	Displays the status of the interface.

8.3 VoIP

Voice over IP (VoIP) uses the IP protocol for voice and video transmission.

The main difference compared with conventional telephony is that the voice information is not transmitted over a switched connection in a telephone network, but divided into data packets by the Internet protocol and these packets are then passed to the destination over undefined paths in a network. This technology uses the existing network infrastructure for voice transmission and shares this with other communication services.

8.3.1 Settings

In the **VoIP**->**Settings** menu, you set up your VoIP connections.

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 licences that have been entered.

8.3.1.1 SIP Provider

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

You modify 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).

8.3.1.1.1 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 designation for the SIP provider. A 20 digit alpha-numeric sequence is possible.
Provider Status	Select whether this VoIP provider entry is enabled (*Enabled*, standard value) or not (*disabled*).
Access Configuration	Select which type of VoIP phonenumbers you wish to configure. Possible values:

Field	Description
	- *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 signalling you want for outgoing calls. Possible values: - *Standard* (default value) - *Global CLIP no Screening Number* - *Individual CLIP no Screening Number* - *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 called party for all external connections. 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* 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 alphanumeric sequence is possible.

Field	Description
Registrar Port	Enter the number of the port to be used for connection to the server. The default value is *5060*. A 5 digit sequence is possible. If you prefer a DNS SRV request instead of a DNS A record request for this provider, enter port *0* here. For connections offered by Deutsche Telekom this is a required setting because the SRV entry provides additional server addresses which may provide a better service quality. SIP provider that are created with the Initial Operation menu or with the Telephony assistant automatically use the correct port number.
Transport Protocol	Select the transport protocol for the connection. Possible values: • *UDP* (default value) • *TCP* • *TLS* • *Automatic* - With this setting, your device supports automatic negotiation of the protocol with your provider's servers. For this setting to work, this negotiation must also be supported by the provider.

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 and uses this for 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 Proxy menu

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

Field	Description
	Possible values: • *UDP* (default value) • *TCP* • *TLS* • *Automatic* - With this setting, your device supports automatic negotiation of the protocol with your provider's servers. For this setting to work, this negotiation must also be supported by the provider.

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).
MediaSec	*MediaSec*: MediaSec regulates the protection of SIP data between the SIP server and your system. For seamless support, automatic negotiation of the transport protocol is mandatory. Fixed transport protocol settings (UDP and TCP) may cause problems during registration. Additionally, the use of SRTP must be allowed. Your VoIP provider must support MediaSec.

Fields in the 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:

Field	Description
	- *Any Location* (default value): The server is not operated at any defined location. - *<Location Name>*
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 Deutsche Telekom and customer is required which incluides a bandwidth limitation (number of simultaneously usable voice channels). If a SIP provider - Deutsche Telekom in particular - 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*. 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* .

Field	Description
	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.
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.

Field	Description
	• *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
Substitution of International Prefix with "+"	Select whether the prefix (e. g. 00) should be replaced by + for 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 enabled 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 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.

Field	Description
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, 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.

8.3.1.2 Locations

In the **VoIP**->**Settings**->**Locations** menu, you configure locations of the VoIP subscribers configured on your system, and define bandwidth management for the VoIP traffic.

Individual locations can be created for use of bandwidth management. A location is identified by its fixed IP address, or DynDNS address, as the case applies, or on the basis of the interface to which the device is connected. The available VoIP bandwidth (up- and downstream) can then be configured for every 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.

8.3.1.2.1 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 entry description.
Parent Location	You can cascade the SIP locations at will. Define which previously-defined SIP location shall constitute the higher-level node for the SIP location to be configured here.
Type	Select whether the location shall be defined using IP addresses/DNS names or interfaces. Possible values: • `Addresses` (default value): The SIP location is defined by an IP address or a DNS name. • `Interfaces`: The SIP location is defined via the available interfaces.
Addresses	Only for **Type** = `Addresses` Enter the IP addresses of the devices at the SIP locations. Click **Add** to configure new addresses. Enter the IP address or the DNS name required under **IP Address/DNS Name**. Also enter the **Netmask** required.
Interfaces	Only for **Type** = `Interfaces` Indicate the interfaces to which the devices of a SIP location are connected. Click **Add** to select the new interface. Under **Interface**, select the desired interface.
Upstream Bandwidth Limitation	Select whether the upstream bandwidth is to be restricted for this location. 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	Select whether the downstream bandwidth is to be restricted for this location. 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 DSCP menu

Field	Description
DSCP Settings for rtp Traffic	Select the type of services for RTP data (TOS, type of service). Possible values: • `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.

8.3.1.3 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 creating codecs, please bear in mind that good voice quality requires corresponding bandwidth, which will limit the number of possible simultaneous calls. Moreover, the remote station must also support the corresponding codec selection.

8.3.1.3.1 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 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	Not for **Codec Proposal Sequence** = `default`

Field	Description
	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	Not for **Codec Proposal Sequence** = *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	Not for **Codec Proposal Sequence** = *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	Not for **Codec Proposal Sequence** = *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.
DTMF	Not for **Codec Proposal Sequence** = *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.

8.3.1.4 Options

General VoIP settings are located in the **VoIP**->**Settings**->**Options** menu.

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 transmitted. The default value is *10000*.
Client Registration Timer	Enter a default value for the period in seconds within which the SIP clients must re-register to prevent automatic disconnection. The default value is *60*.

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

Fields in the Advanced Parameter menu

Field	Description
DSCP Settings for sip	Select the Type of Service (TOS) for SIP data.

Field	Description
Traffic	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. 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.

Fields in the SIP dual Stack (IPv4/IPv6) menu

Field	Description
SIP dual Stack (IPv4/IPv6)	Enable this option if you want to support IPv6 for VoIP. Both, IPv4 as well as IPv6 are supported, and if a VoIP provider supports IPv6, IPv6 is preferred. If a VoIP provides does not support IPv6, IPv4 is used. With selection of `Activated` the option is anabled. The function is not enabled by default. This means that only IPv4 is used until you enable dual stack SIP.

8.4 Numbering

8.4.1 Trunk Settings

Your system is a telecommunication installation for external connection to the Internet.

8.4.1.1 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.

8.4.1.2 Trunk Numbers

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

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 accessed directly via the extension number range as **Internal numbers** in the **Numbering**->**User Settings**->**User**->**Add**->**Trunk Numbers**->**Internal Numbers** menu.

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. The internal numbers are specified under **Numbering**->**User Settings**->**User**->**Add**->**Trunk Numbers**.

8.4.1.2.1 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 **Assistants**->**PBX**->**Trunks** for which you want to configure the numbers.
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.

Field	Description
	For **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 make additional settings in **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.

8.4.1.3 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.

8.4.1.3.1 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.
Sequence of Trunk Lines in Group	Select the desired external connections for a bundle. The order when dialling to the outside matches the sequence of external connections in this

Field	Description
	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.

8.4.2 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 **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**.

8.4.2.1 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

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

8.4.2.1.1 Basic Settings

In the **Numbering**->**User Settings**->**Users**->**Basic Settings** you enter basic information about the user.

The 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).

Field	Description
Home Number	Enter a number under which the user can be reached via home 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).
E-mail Address	Enter the e-mail address for the user.

Fields in the Class of Service menu

Field	Description
Standard	Select the classes of service = CoS. The authorisation class and the creating of new authorisation classes is done under **Numbering**->**User Settings**->**Class of Services**. Only the selecting is done in this setting. Possible values: • *Uneingeschr. AutoAmt* (default value): All connections can be established and taken, automatic outside line is enabled. • *Uneingeschränkt*: All connections can be established and taken, automatic outside line is not enabled. • *Not allowed*: No class of service • *<Authorisation class>*
Optional	Select an optional authorisation class. This CoS is required for the calendar settings. The authorisation class and the creating of new authorisation classes is done under **Numbering**->**User Settings**->**Class of Services**. Only the selecting is done in this setting. Possible values: • *Uneingeschr. AutoAmt* (default value): All connections can be established and taken, automatic outside line is enabled. • *Uneingeschränkt*: All connections can be established and taken, automatic outside line is not enabled. • *Not allowed*: No class of service • *<Authorisation class>*
Night	Select the authorisation class for night operation. This CoS is required for the calendar settings. The authorisation class and the creating of new authorisation classes is done under **Numbering**->**User Settings**->**Class of Services**. Only the selecting is done in this setting. Possible values: • *Uneingeschr. AutoAmt* (default value): All connections can be established and taken, automatic outside line is enabled. • *Uneingeschränkt*: All connections can be established and taken, automatic outside line is not enabled. • *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 user for whom more than one phone number has been set up is currently engaged, you can decide whether additional calls for this user

Field	Description
	should be signalled. If "Busy on Busy" is set for this user, other callers get the **Engaged** signal if the user is calling on one of their numbers. The function is activated by selecting *Enabled*. The function is disabled by default.

8.4.2.1.2 Numbers

The internal numbers which are later assigned to the terminals can be entered in the **Numbering**->**User Settings**->**Users**->**Numbers** menu. 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**.

8.4.2.1.3 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 ✎ symbol to define, for every internal number (indicated in the table by **Internal Number** and **Displayed Description**), the number that should 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 ⇅ 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 **Apply**.
The entries display in the changed order.

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

(5) Close the window by clicking **OK**.

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.

8.4.2.1.4 Authorizations

In the **Numbering**->**User Settings**->**Users**->**Authorizations** menu you can allow this user to perform certain configurations 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 create the PIN for access to protected functions. These functions are: • Access to the voice mailbox from a phone not assigned to the user • Access to the configuration of the system via the phone via dial codes . In the default configuration no PIN is created.

Fields in the User HTML Configuration menu

Field	Description
Personal Access	Select whether this user shall receive access authorisation to a personalised user interface where he can perform his own entries and settings. The function is activated by selecting *Enabled*.

Field	Description
	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. If 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.

8.4.2.2 Class of Services

In the **Numbering**->**User Settings**->**Class of Services** (CoS) the functions and performance 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 authorisation classes.

8.4.2.2.1 Basic Settings

The basic settings and the name for the new CoS is specified in the **Numbering**->**User Settings**->**Class of Services**->**Basic Settings** menu. 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 Authorization	Select line access authorisation for the authorisation class. Line access authorisation determines which calls (internal, external,...) are allowed. The system distinguishes several authorisation levels. Possible values: • *Unlimited*: 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. • *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. **Note** If you are conducting an external call when automatic outside line access is active and then want to start a second external call, you must select a leading *0* for the second call so that it can be set up. 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 with the corresponding code number is initiated for selective use of the bundle, and not by dialling the exchange 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. The function is activated by selecting *Enabled*.

Field	Description
	The function is disabled by default. Then select the bundles for which manual bundle assignment is to be allowed. You 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 the numbers entered in the **Call Routing**->**Outgoing Services**->**Dial Control** menu shall be allowed or denied also for this CoS. 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*.

Field	Description
	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.

8.4.2.2.2 Features

Additional functions are set up 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 performance 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 ongoing 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 immediately 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 unreachable 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 in which the data protection performance feature is enabled (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 *Enabled*. The function is enabled by default.
Switch signalling variants manually	Select whether manual switching of call options shall be allowed for this authorisation class. The function is activated by selecting *Enabled*. The function is enabled by default.
Call Through	Select whether Call Through shall be allowed for this authorisation class. The function is activated by selecting *Enabled*. The function is disabled 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 telephone 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 Intercom Call	Select whether simplex operation calls to the system telephone shall be allowed for this authorisation class. The function is activated by selecting `Enabled`. The function is enabled by default.
Receive Announcement Calls	Select whether this authorisation class may receive announcements. The function is activated by selecting `Enabled`. The function is enabled by default.
Receive MWI Information	Select whether this authorisation class may receive information about existing messages (MWI = Message Waiting Indication). The function is activated by selecting `Enabled`. 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.

Field	Description
	The function is activated by selecting *Enabled*. The function is enabled by default.

8.4.2.2.3 Applications

Additional applications are set up in the **Numbering**->**User Settings**->**Class of Services**->**Applications** menu.

The 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. 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*.

Field	Description
	The function is enabled by default.

8.4.2.3 Parallel Ringing

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

8.4.2.3.1 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 home number have been set up under **Users**->**Basic Settings**->**External Numbers**, they will be displayed and can be selected under **Configured Home Number** or **Configured Mobile Number**.
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.

8.4.3 Groups &Teams

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

8.4.3.1 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.

8.4.3.1.1 General

In the **Numbering**->**Groups &Teams**->**Teams**->**General** menu, the 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** after which call forwarding after time shall be done 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 when **Signalling** *Even Distribution (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

Field	Description
	are not included in the time calculation. The default value is *0* seconds; the range *0... 999* seconds.

8.4.3.1.2 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.

Under **Internal Assignment**, select the internal subscribers who are to belong to this team. If you wish to temporarily exclude one of the team subscribers from call signalling (e.g. a team subscriber is on holiday), you can **Logout** this 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 subscriber 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.
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 the 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 sequence 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 subscribers 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 subscribers 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 equates to **SignallingRotating** and ensures 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 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 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 function 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 shall 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.

Field	Description
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: • *MOH Internal 1* • *MOH Internal 2*

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

Fields in the Rerouting Functions menu

Field	Description
Rerouting on no response	Select whether and, if so, to which team an incoming call should be redirected on no reply. Possible values: • *None* • *<Team>* Also enter the time after which the call should be redirected.

8.4.3.1.3 Log on / Log off

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

8.4.4 Call Distribution

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

8.4.4.1 Incoming Distribution

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

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

8.4.4.1.1 Edit

Choose the ✎ icon to edit existing entries.

The **Numbering**->**Call Distribution**->**Incoming Distribution**->**New** 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* • *Phone Remote Access*

•

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**.

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 entering the PIN. • *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 entering the PIN.
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.

Field	Description
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.

8.4.4.2 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.

8.4.4.2.1 Edit

Choose the ✎ icon to edit existing entries.

The **Numbering**->**Call Distribution**->**Misdial Routing**-> **Edit** 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.

8.4.4.3 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.

8.4.4.3.1 Edit or New

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

The menu 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) .

Field	Description
	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. 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.

Note

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

8.5 Terminals

8.5.1 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.

8.5.1.1 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.

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.

8.5.1.1.1 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 Basic Settings menu

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*

Field	Description
	For **Phone Type** = *ISDN / Upn*: Displays system telephone product description. Possible values: • *CS290* • *CS400xt* • *CS410* • *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 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.
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 Number Settings menu

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.

Field	Description
	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 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 Extensions menu

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 Codec Settings menu

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 Further Settings menu

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

Field	Description
	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.

8.5.1.1.2 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 Basic Settings menu

Field	Description
Display Language	Select the display language for your telephone. Possibe values: • *Deutsch* • *Dutch* : Not for **S530** and **S560** • *English* • *Italian* • *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.
Call Waiting	Select whether another call shall be supported for this telephone through

Field	Description
	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 **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 of the **CS4xx** series, the **S530** and **S560** telephones 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* (**S530** and **S560** only) • *Attention tone 2* (**S530** and **S560** only) • *Attention tone 3* (**S530** and **S560** only) • *Attention tone 4* (**S530** and **S560** only) • *No attention tone* (**S530** and **S560** only)

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

Fields in the Advanced Settings menu

Field	Description
Status LED	Select whether and, if so, which events should be signalled by the system telephone status LED.

Field	Description
	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 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. ☞ **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** *Activated* turns on the automatic call acceptance. You can configure the corresponding duration in the **Terminals**->**elmeg**

Field	Description
	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 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	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.

8.5.1.1.3 Keys / T400 / T400/2 / T500

In the menu **Terminals**->**elmeg System Phones**->**System Phone**->**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 Keys list

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

Fields in the Telephone menu

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, 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*

Field	Description
	• *Trunk Group Access* • *Connection Key* • *Hotel Room* • *System Parking* • *Agent wrap-up Time* • *Night Mode* • *Shift key* (**S5x0** only) • *Parallel call* (only **S5x0**) • *Station guarding (quiet)* (**S5x0** only)
Number	Only with **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	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. 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*

Field	Description
	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)* 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 if **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 immediately.
Target Number "Immediate"	Only if **Key Type** = *Call Forwarding (CFU)* Enter the number to which incoming calls shall be forwarded on busy.
Target Number "On busy"	Only if **Key Type** = *Call Forwarding (CFB)* Enter the number to which incoming calls shall be forwarded on no reply.

Field	Description
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 ⇅ icon to move configured function keys.

Fields in the Key menu

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 Move to menu

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.

8.5.1.1.4 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.
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:**	Displays the type and serial number of the connected key extension.

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

8.5.1.2 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 ≡+ synbol 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 **IP1x0** 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.

8.5.1.2.1 General

You can change the IP telephone's basic settings in the **Terminals**->**elmeg System Phones**->**elmeg IP**->**General** menu.

The menu consists of the following fields:

Fields in the Basic Settings menu

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 IP640* • *elmeg IP680*
Location	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 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.
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 enabled for quick login after a functional disruption.

Key Extensions

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 Further Settings menu

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 Codec Settings menu

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

8.5.1.2.2 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 telephone's display.
User	Displays the user's name.

8.5.1.2.3 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 functions 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 **Media-Pool** 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 selected 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. The keys can be used for the following features:
  - User defined: freely configurable
  - Night mode: switch between day and night modes
  - CFU; CFNR; CFB; CFB/CFNR: Call Forwarding (immediately, delayed, on Busy)
  - Team Signalization: log in to our of a team

> **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 Keys

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* • *Macro Function* • *XML-Content* • *Next call anonymous* • *Menu - Call Forwarding* • *Menu - Resource Directory* • *Menu - Internet Radio* • *Macro Function*

Field	Description
	• *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.
Macro Function	Only for **Key Type** = *Macro Function* The keys can be used for the following features: • *User defined*: Freely configurable • *Night mode*: Switch between day and night modes • *CFU; CFNR; CFB; CFB/CFNR*: Call Forwarding (immediately, delayed, on Busy) • *Team Signalization*: You can log in to a team or log out of a team.
On Code	Only for**Macro Function** = *User defined* Define an arbitrary code to be executed when the key is switched on.
Off Code	Only for**Macro Function** = *User defined* Define an arbitrary code to be executed when the key is switched off.
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 ⇅ icon to move configured function keys.

Fields in the menu Key

Field	Description
Key name	Displays the name of the key.

Field	Description
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.

8.5.1.2.4 Settings

You can reset the phone's administrator password in the **Terminals**->**elmeg System Phones**->**elmeg IP**->**Settings** menu.

The menu consists of the following fields:

Fields in the System Phone menu

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

8.5.1.3 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 respectice numbers.

Use automatic provisioning to have your PABX system transfer elementary telephony parameters to the DECT system. If you want to use the assistant **First Steps** to do this, you activate 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**->**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.

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.

8.5.1.3.1 General

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

The 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.

Field	Description
Phone Type	Displays the type of base station. Possible values: • *elmeg DECT150* • *elmeg DECT200* • *elmeg DECT210*
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.

8.5.1.3.2 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 🗑.

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.

8.5.1.3.3 Settings

In the **Terminals**->**elmeg System Phones**->**elmeg DECT**->**Settings** menu you can reset the administrator password for the base station.

The 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.

8.5.2 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 (Octophon, 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

8.5.2.1 VoIP

In the **Terminals**->**Other phones**->**VoIP** menu, you configure the connected VoIP terminals. For example, you perform assignment of a configured internal number.

8.5.2.1.1 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 Basic Settings menu

Field	Description
Description	Enter a description for the IP telephone.

Field	Description
Location	Select the location of the IP 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 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.

Fields in the Number Settings menu

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 SIP Client Settings menu

Field	Description
SIP Client Mode	Select whether a *Dynamic* or a *Static* SIP client is to be used. Possible values: • *Dynamic* (default value): Your device (e.g. a standard SIP telephone) performs a SIP registration to publish its IP address to the system. • *Static* : An incoming call of a (statically configured) SIP client will be accepted without prior registration of this client if the IP address of the client matches the entered IP address under **SIP Client IP Address**. A Microsoft Office Communications Server and other Unified Communication Servers use this mode.
SIP Client IP Address	Only if **SIP Client Mode** = *Static* Enter the static local IP address of the SIP client.
Port Number	Only if **SIP Client Mode** = *Static* Enter the number of the port to be used for connection. A 5 digit sequence is possible. For example, the port *5065* must be entered for connection to a Microsoft Exchange Communication Server.
Transport Protocol	Only if **SIP Client Mode** = *Static*

Field	Description
	Select the transport protocol for the connection. Possible values: • *UDP* (default value) • *TCP* • *TLS* • *Automatic* - With this setting, your device supports automatic negotiation of the protocol with your provider's servers. For this setting to work, this negotiation must also be supported by the provider. For example, the protocol *TCP* must be entered for connection to a Microsoft Exchange Communication Server.

Fields in the Codec Settings menu

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.
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 Further Settings menu

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.

8.5.2.2 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.

8.5.2.2.1 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*
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.

8.5.2.3 analog

In the **Terminals**->**Other phones**->**analog** 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	a/b 1	Telephone	10	Enabled
a/b 2	a/b 2	Telephone	11	Enabled

8.5.2.3.1 Edit or New

Choose the ✎ icon to edit existing entries.

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**->**analog**-> ✎ menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the analogue telephone.
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: • *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.

Field	Description
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 disabled 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. 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, "re-

Field	Description
	placed receiver" is detected. Values from *100 ms* (standard value) to *1000 ms* are possible. The default value is *400 ms*.

8.5.3 Overview

8.5.3.1 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.

8.6 Call Routing

The functions for external calls and automatic route selections for external calls are defined in call routing.

8.6.1 Outgoing Services

In the **Call Routing**->**Outgoing Services** menu you can configure the features **Direct Call**, **Call Forwarding**, **Dial Control** and **Priority Numbers**.

8.6.1.1 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.

8.6.1.1.1 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.

8.6.1.2 Call Forwarding

In the **Call Routing**->**Outgoing Services**->**Call Forwarding** menu you configure the 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.

8.6.1.2.1 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. Possible values: • *Immediately* • *On Busy* • *On no reply* (default value) • *On busy / On no reply*

Field	Description
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.

8.6.1.3 Dial Control

In the **Call Routing**->**Outgoing Services**->**Dial Control** menu you can block particular numbers/partial numbers or permit them.

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.

8.6.1.3.1 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.

8.6.1.4 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.

8.6.1.4.1 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.

8.6.1.5 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.

8.6.1.5.1 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.

8.6.2 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.

8.6.2.1 General

In the **Call Routing**->**Automatic Route Selection**->**General** menu, you activate the ARS (Automatic Route Selection) function and select the desired route level.

The menu 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

Field	Description
	bundle cannot be accessed. Possible values: • *1 (No Fallback)*: If the entered provider or the selected bundle (**Call Routing**->**Automatic Route Selection**->**Zones &Routing**-> **Edit/Add**-> **Mo-Su** ->**Routing Stage 1**) is not available, the connection setup is terminated. • *2*: If the entered provider or the 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 option (**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** und **Routing Stage 2**) is available, dialling occurs via the provider entered as default for the user(**Numbering**->**Class of Service**->**Add**->**Basic Settings**->**Trunk Line Selection with Line Access Number**).

8.6.2.2 Interfaces / Provider

In the **Call Routing**->**Automatic Route Selection**->**Interfaces / Provider** menu you enter the routes and providers and their network access prefixes.

8.6.2.2.1 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 consists 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.

8.6.2.3 Zones &Routing

In the **Call Routing**->**Automatic Route Selection**->**Zones &Routing** menu 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 weekday. 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.

8.6.2.3.1 Trunk Numbers

In the **Trunk Numbers** area, enter the numbers or partial numbers 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.

8.6.2.3.2 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**.

8.7 Applications

Internal telephone performance features of the system are set up under **Applications**.

8.7.1 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.

8.7.1.1 Calendar

In the menu **Applications**->**Calendar**->**Calendar** menu 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.

8.7.1.1.1 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 Basic Settings menu

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.

8.7.1.1.2 Mon - Sun / Exception

In the **Mo - Su** area you set up the switching days and times for this calendar.

The **Applications**->**Calendar**->**Calendar**->**Mo - Su** 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 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

Field	Description
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*. 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. You configure the weekdays in the **Applications**->**Calendar**->**Calendar**->**Mo - Su** menu. 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

8.7.1.2 Public Holiday

In the **Applications**->**Calendar**->**Public Holiday** menu you can enter public holidays or any special days for which divergent settings should be made via the calendar.

8.7.1.2.1 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.

8.7.3 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** of the user interface. Entries in the system telephone phone book menu with the (M) mark refer to an entered **Mobile Number** for a user, those with (H) mark to the **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.

8.7.3.1 Entries

The **Applications**->**System Phonebook**->**Entries** menu displays all the phone book entries that have been set up along with the associated speed dial number. The entries in the **Description** column are sorted alphabetically. In any of the columns you can click the column header and can sort the entries in ascending or descending order.

8.7.3.1.1 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 no speed dial number is entered, the count is automatically continued, i.e. a speed dial code is assigned automatically. A 3 digit sequence of *000* to *999* is possible.
Call Through	Select whether the phone number is to be authorised for the **Call Through** function. 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.

8.7.3.2 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 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). • *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*

Field	Description
	• *Tabulator*
Select file	Only for **Action** = *Import* Select the file that is to be imported.

You also have the option to import a CSV file.

Example of a CSV file which can be imported

```
"Title","First Name","Last Name","Office Number","Home Number"
"Mr","Thomas","Kirk","+44 (123) 111111","+44 (123) 222222"
"Mrs","Emma","Watson","+44 (123) 333333","+44 (123) 444444"
```

If there are multiple numbers in a data record, you will have the option in the next step to generate two phonebook records from a single data record. To do this, specify the data to be used as the name and phonenumber. 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 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.

8.7.3.3 General

In the **Applications**->**System Phonebook**->**General** menu 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 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.

8.7.4 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 need to enable the recording of connection data in the **Numbering**->**User Settings**->**Class of Services**->**Applications** menu. The function is not activated in the ex works state.

8.7.4.1 Outgoing

The **Applications**->**Call Data Records**->**Outgoing** menu contains information that permits the monitoring of outgoing activities.

The 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 called name.
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.

8.7.4.2 Incoming

The **Applications**->**Call Data Records**->**Incoming** menu contains information that permits the monitoring of incoming activities.

The 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 caller´s name.
External Number	Displays the caller's number.
Project Code	Displays the call project number, if any.

Field	Description
Interface	Displays the interface over which the connection from outside was routed.

8.7.4.3 General

In the **Applications**->**Call Data Records**->**General** menu, you can define how the connection data is saved in the system.

The menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Web Access Username	Enter a user name for the connection data administrator.
Web Access Password	Enter a password for the connection data administrator.
Save outgoing calls	Select which outgoing connections should be saved. Possible values: • *None* (default value) • *All* • *With Project Code only*
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. You can enter the number of hidden digits separately for **Outgoing Calls** and for **Incoming Calls**. The hiding of digits occurs from right to left. Possible values: • *No* (default value) • *All* • *1* to *9*

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**.

8.7.5 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**.

8.7.5.1 Incoming

The **Applications**->**Call List**->**Incoming** menu contains information that permits the monitoring of incoming activities.

The 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.

8.7.5.2 Outgoing

The **Applications**->**Call List**->**Outgoing** menu contains information that permits the monitoring of outgoing activities.

The 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

Field	Description
	routed.
Delete	You can use the **Select all** and **Deselect all** buttons for all the devices displayed.

8.7.5.3 General

In the **Applications**->**Call List**->**General** menu, you can define how the connection data is saved in the system.

The 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*
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 initated of accepted by a configured user) that are included in the list. The maximum number is *200*.

8.7.6 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.

8.7.6.1 Doorcom Units

In the **Applications**->**Doorcom Units**->**Doorcom Units** menu, select the internal analogue connection (FXS) to which a doorcom unit shall be connected. Then dial the internal number for the connection, and optionally the codes for call acceptance.

8.7.6.1.1 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 set up 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.

8.7.6.2 Doorcom Signalling

In the **Applications**->**Doorcom Units**->**Doorcom Signalling** you configure the signalling variants for receiving calls via a doorcom unit. 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.

8.7.6.2.1 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 each bell, you can create up to two doorcom signalling variants in the **Applications**->**Doorcom Units**->**Doorcom Signalling**->**New**->**Variant** menu. Possible values:

Field	Description
	• *No calendar,only manually* • *<Calendar>*
Active Doorcom Variant	Select which intercom call option shall be enabled by default for 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.

8.7.6.2.2 Doorcom Signalling Variant 1 and 2

In the **Doorcom Signalling Variant** area you configure the two doorcom call options for this signalling profile.

The menu **Applications**->**Doorcom Units**->**Doorcom Signalling**->**Doorcom Signalling 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.
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 the 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

Field	Description
	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).

8.7.7 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 individual voicemail boxes occurs via telephone.

Every subscriber can use her individual voicemail box by transferring calls to her voicemail box.

Note

Choose in the **Maintenance**->**Software &Configuration** menu the option *Import Voice Mail Wave Files*.

8.7.7.1 Voice Mail Boxes

The **Applications**->**Voice Mail System**->**Voice Mail Boxes** menu displays a list with the individual voicemail boxes of the individual subscribers, where voicemail boxes have been configured.

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 Voice Mail Boxes 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 voicemail box is configured.
Language	Displays the language of the announcement text on the voicemail box. *Default* means that the centrally-set language, defined for the entire voicemail system in the **Applications**->**Voice Mail System**->**General** menu, is used.

Field	Description
Notification	Indicates whether the subscriber is informed of missed calls.
Active Variant	Displays the current status of the voicemail box (`In the Office` 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.

8.7.7.1.1 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 Basic Setup menu

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.
Status	Select when incoming calls shall be forwarded to the specified internal number. Possible values: • `Off` • `Immediately` • `On Busy` • `On no reply` • `On busy / On no reply`
No Reply Time	Only for **Status** = `On no reply` and `On busy / On no reply` Define the maximum time a caller can remain on hold if they cannot get through to the target number. After expiration of this time, the caller shall be transferred to the defined redirect destination. The default value is `15` seconds.
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.

Field	Description
	• *Turkish*: The voicemail box uses Turkish 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.
E-Mail Address	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 email address is created 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. • *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**.
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 in the **Applications**->**Calendar** menu with the setting **Application** = *Voice Mail System* 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 User Settings menu

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 subscriber 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. The PIN for the personal Voice Mail Box you can change in the **Numbering**->**User Settings**->**Users**->**Authorizations** menu under **PIN for Phone Access**.
PIN	Only when setting up a Team Voice Mail Box. The PIN is required to set up the voice mail box. If the voice mailbox is being monitored over a telephone, this PIN must be entered.
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.

Fields in the Authorizations menu

Feld	Beschreibung
Login Name	Here you can change the permissions for external calls. The user selected here also receives user access to his personal voice mail box.

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 **Annoucement 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 **Annoucement 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.

8.7.7.2 Status

In the **Applications**->**Voice Mail**->**Status** menu, the status of the individual voicemail boxes for specific subscribers is indicated. You can see how many calls have gone into 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 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 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.

8.7.7.3 General

In this menu, you can configure the general settings for your voicemail system.

The menu **Applications**->**Voice Mail**->**General** consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Voice Mail System	Select whether to activate your voicemail system. The function is enabled with *Enabled*. The function is disabled 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. 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* • *Turkish*h 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 Mail Settings menu

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.
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 Advanced Settings menu

Field	Description
Lifetime	Voicemail messages are deleted after an adjustable period of time if the maximum number of messages has been reached for a voice mail box. If the maximum number of messages is reached before the specified time has expired, the next caller cannot leave a message and will be notified if

Field	Description
	applicable. Possible values are `10` to `60` days. The default value is `60`.
Non-standard SMTP Server port	Enter the port to be used for sending e-mails. The default value is `25`.

8.8 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.

8.8.1 Status Information

This menu displays current settings for terminals and team subscribers. This data is continuously read out.

8.8.1.1 Users

In the **Monitoring**->**Status Information**->**Users** menu the current settings for a user's internal number (MSN) are displayed.

8.8.1.1.1 Users - Details

By pressing the 🔍 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.
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.
IP Address	Displays the IP address.
Registration	Displays whether the user is registered.
Charges	Displays calculated charges for accrued connection units.

Values in the System Settings list

Field	Description
Parallel Ringing	Displays whether parallel call is set up for the user.
Call Forwarding	Displays current call forwarding for this user.
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.

8.8.1.2 Teams

In the **Monitoring**->**Status Information**->**Teams** menu, current team settings are displayed.

8.8.1.2.1 Teams - Details

By pressing the 🔍 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.
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.
Further Rerouting	Displays which of the redirect functions are enabled and which subscriber is the redirect destination.

Chapter 9 Telephony (Media Gateway)

9.1 Physical Interfaces

9.1.1 ISDN Ports (Media Gateway)

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

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

- Enter the settings for your ISDN connection: Here you set the most important parameters of your ISDN connection.
- MSN Configuration: Here you tell your device how to react to incoming calls from the WAN.

9.1.1.1 ISDN Configuration

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

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

9.1.1.1.1 Edit

Choose the ✎ icon to edit the configuration of the ISDN port.

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

Fields in the Basic Parameters menu

Field	Description
Port Name	Shows the name of the ISDN port.
Mode	Select the mode. Possible values: • *External* • *Internal*
Autoconfiguration on Bootup	Only if **Mode** = *External* Select whether the ISDN switch type (D channel detection for switched line) is to be automatically identified. The function is enabled with Enabled. The function is disabled by default.
Port Usage	Only if **Autoconfiguration on Bootup** is disabled. Select the protocol that you want to use for the ISDN port.

Field	Description
	Possible values: • *Not used*: The ISDN connection is not used. • *Dialup (Euro ISDN)* • *Q-SIG*
ISDN Configuration Type	Only if **Autoconfiguration on Bootup** is disabled and for **Port Usage** = *Dialup (Euro ISDN)* or *Q-SIG* Select the ISDN connection type. Possible values: • *Point-to-Multipoint* (default value): Point-to-multipoint connection • *Point-to-Point*: Point-to-point ISDN access.

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

Fields in the Advanced Settings menu

Field	Description
X.31 (X.25 in D Channel)	Select whether you want to use X.31 (X.25 in the D channel) e.g. for CAPI applications. The function is enabled with *Enabled*. The function is disabled by default.
X.31 TEI Value	Only if **X.31 (X.25 in D Channel)** is enabled With the ISDN autoconfiguration, the X.31-TEI is detected automatically. If the autoconfiguration has not detected TEI, you can manually enter the value assigned by the exchange. Possible values are *0* to *63*. The default value is *-1* (for automatic detection).
X.31 TEI Service	Only for **X.31 (X.25 in D Channel)** enabled Select the service for which you want to use X.31 TEI. Possible values: • *CAPI* • *CAPI Default* • *Packet Switch* (default value) *CAPI* and *CAPI Default* are only for the use of X.31 TEI for CAPI applications. For *CAPI*, the TEI value set in the CAPI application is used. For *CAPI Default*, the value of the CAPI application is ignored and the default value set here is always used. *Packet Switch* is set if you want to use X.31 TEI for the X.25 device.

9.1.1.2 MSN Configuration

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

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

The device supports the following services:

- PPP (Routing): The PPP (routing) service is your device's general routing service. This enables ISDN remote terminals to establish data connections with your LAN, among other things. This enables partners outside your own local network to access hosts within your LAN. It is also possible to establish outgoing data connections to ISDN remote terminals.
- ISDN Login: The ISDN login service enables both incoming data connections with access to the SNMP shell of your device, and outgoing data connections to other **be.IP smart** devices. As a result, your device can be remotely configured and administrated.
- IPSec: **be.IP smart** devices support the DynDNS service to enable hosts without fixed IP addresses to obtain a secure connection over the Internet. With the IPSec Callback function and using a direct ISDN call to an IPSec peer with a dynamic IP address you can signal to this IPSec peer that you are online and waiting for the setup of an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. The identification of the caller from his or her ISDN number is enough information to initiate setting up a tunnel.
- X.25 PAD: X.25 PAD is used to provide a protocol converter, which converts non-packet-oriented protocols to packet-oriented communication protocols and vice versa. Data terminal equipment sending or receiving data on a non-data-packet-oriented basis can this be adapted in line with Datex-P (public data packet network based on the principle of a packet switching exchange).

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

Note

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

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

9.1.1.2.1 New

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

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

Fields in the Basic Parameters menu

Field	Description
ISDN Port	Select the ISDN port for which the MSN is to be configured.
Service	Select the service to which a call is to be assigned on the **MSN** below. Possible values: • *ISDN Login* (default value): Enables login with *ISDN Login* • *PPP (Routing)*: Default setting for PPP routing. Contains automatic detection of the PPP connections stated below except *PPP DOVB*. • *IPSec*: Enables a number to be defined for IPSec callback. • *Other (PPP)*: Other services can be selected: *PPP 64k* (Allows 64 kpbs PPP data connections), *PPP 56k* (Allows 56 kpbs PPP data connections), *PPP V.110(9600) PPP V.110(14400)*, *PPP*

Field	Description
	V.110(19200), *PPP V.110(38400)* (Allows PPP connections with V.110 and bitrates of 9,600 bps, 14,400 bps, 19,200 bps, 38,400 bps), *PPP V.120* (Allows PPP connections with V.120).
MSN	Enter the number used to check the called party number. For the call to be accepted, it is sufficient for the individual numbers in the entry to agree, taking account of **MSN Recognition**.
MSN Recognition	Select the mode your device is to use for the number comparison for **MSN** with the called party number of the incoming call. Possible values: • *Right to Left* (default value) • *Left to Right (DDI)*: Always select if your device is connected to a point-to-point connection.
Bearer Service	Select the type of incoming call (service detection). Possible values: • *Data + Voice* (default value): Both data and voice calls. • *Data*: data call • *Voice*: Voice call (modem, voice, analog fax)

9.2 VoIP (Media Gateway)

Voice over IP (VoIP) uses the IP protocol for voice and video transmission.

The main difference compared with conventional telephony is that the voice information is not transmitted over a switched connection in a telephone network, but divided into data packets by the Internet protocol and these packets are then passed to the destination over undefined paths in a network. This technology uses the existing network infrastructure for voice transmission and shares this with other communication services.

The Session Initiation Protocol (SIP) is used to establish, clear and control a communication session.

9.2.1 Settings

9.2.1.1 Extensions

Here you can configure the numbers of the terminal devices (=Extensions) connected to the media gateway, i.e. the numbers of the SIP terminals and the numbers of the ISDN terminals, depending on the available interfaces.

A list of all existing subscribers is displayed in the **VoIP**->**Settings**->**Extensions** menu.

9.2.1.1.1 Edit or New

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

The **VoIP**->**Settings**->**Extensions**->✎->**New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the extension.
Extension / User Name	ISDN terminals: Enter the subscriber number the extension.

Field	Description
	SIP terminals: Enter the user name. A maximum of 40 characters can be entered.
Interface Type	Select the interface type to be used. The selection depends on the interfaces available. Possible values: • *SIP*: A SIP terminal device is used for the call. • *ISDN*: An ISDN terminal device is used for the call. Can only be selected if ISDN interfaces configured with Euro ISDN point-to-multipoint (NT mode) are available. • *Analogue*: An analogue terminal device is used for the call. Can only be selected if analogue interfaces are available.
Select analogue interface	Only for **Interface Type** = *Analogue* Select an analogue interface. Possible values: • fxs4-0 (default value) • fxs4-1
Select ISDN interface	Only for **Interface Type** = *ISDN* Select an ISDN interface. The ISDN interfaces you can select depends on the device used.
Registration	Only for **Interface Type** = *SIP* Specify whether the registration mechanism is to be used by SIP REGISTER. Normally, every SIP client (user) sends its current position to a REGISTRAR server by means of a REGISTER message. This information about the user and his current address is held by the REGISTRAR server and queried by other proxies to find the user. The function is enabled with *Enabled*. The function is enabled by default. Apart from this standard procedure, the relevant data can also be sent to a particular IP address that is already known to the correspondent. Registration and authentication are not then needed and the **Registration** function is disabled. An example of this method is Microsoft Exchange SIP.
Location	Set the location of the VoIP subscriber. Possible values: • *Not defined (Registration for Private Networks Only)* (default value): The VoIP subscriber is only registered if located within the private network. • *LAN*: The VoIP subscriber is only registered if located in the LAN.
Expire Time	Only if **Registration** is enabled. Enter the time in seconds after which the current registration becomes invalid and a new registration request is therefore sent.

Field	Description
	For clients, the external port is recognised automatically and should not be changed. Possible values are *0* to *3600*. The default value is *60*.
SIP Endpoint IP Address	Only if **Registration** is disabled. For configurations with no registration (e.g. connection to a Microsoft Exchange Communication Server) the connection can be set up as a static host. This requires you to specify the static IP address of the terminal.
Authentication ID	Only for **Interface Type** = *SIP* Enter a name that is to be used for authentication. A maximum of 20 characters can be entered. The name given here must also be entered on the SIP telephone. If you do not enter a name, the name in the **Extension / User Name** field is used.
Password	Only for **Interface Type** = *SIP* Enter a password here. A maximum of 20 characters can be entered. The password given here must also be entered on the SIP telephone.
Protocol	Select the protocol to be used for data transmission. Possible values: *UDP* (default value), *TCP* or *TLS*. If a protocol has been automatically recognised, it should not be changed.
Port	Enter the number of the UDP, TCP port or TLS ports to be used for the connection to the server or proxy. Possible values are *0* to *65535*. The default value is *5060*.

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

Fields in the Codec Settings menu

Field	Description
Codec Proposal Sequence	Choose the order in which the codecs are offered for use by the media gateway. If the first codec cannot be used, the second is tried and so on. Possible values: • *Default* (default value): the codec in the first position in the menu will be used if possible. • *Quality*: The codecs are sorted by quality. If possible, the codec with the best quality is used. • *Lowest*: The codecs are sorted by required bandwidth. If possible, the codec with the lowest bandwidth requirement is used. • *Highest*: The codecs are sorted by required bandwidth. If possible, the codec with the highest bandwidth requirement is used.

Fields in the Sort Order menu

Field	Description
Sort Order	Select the codecs to be proposed for the connection. The codecs chosen here are proposed in a certain order, depending on the setting in the **Codec Proposal Sequence** field. Possible values: • *G.711 uLaw*: ISDN codec according to US law • *G.711 aLaw*: ISDN codec according to EU law • *G.722*: G.722 passes audio signals in the range of 50-7000 Hz and samples them at the rate of 16,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,5. • *G.729*: Compressed from 31 to 8 kbps; good voice quality • *G.726-40*: Compressed from 63 to 40 kbps • *G.726-32*: Compressed from 55 to 32 kbps • *G.726-24*: Compressed from 47 to 24 kbps • *G.726-16*: Compressed from 39 to 16 kbps • *RFC 2833*: First the system attempts to use RFC 2833. If the remote terminal does not use this standard, SIP Info is used. • *SRTP*: SRTP is an encrypted variant of the Real-Time Transport Protocol (RTP). • *Data (RFC 4040)*: Enable the transport of 64 kbit/s channel data in RTP packets. • *SIP Info*: SIP Info is used for the transmision of DTMF events. • *T.38 Fax*: Allows the transmission of fax messages over data networks. By default *G.711 uLaw*, *G.711 aLaw* and *G.729* are enabled. The codecs actually used are the intersect of the codecs defined here and those signalled by the provider. For outgoing calls, any remaining codecs are dropped from the list that would require more than the available bandwidth.

Fields in the Voice Quality Settings menu

Field	Description
Echo Cancellation	Select whether echo cancellation should be used. Echo cancellation is a technique to suppress echo feedback in voice communication on full duplex lines. The function is enabled with *Enabled*. The function is enabled by default.
Comfort Noise Generation (CNG)	Specify whether Comfort Noise Generation should be used. For digital voice transmission, this function introduces a low level of background noise to avoid the impression that, during pauses at the other end, the connection is lost. The function is enabled with *Enabled*. The function is enabled by default.
Packet Size	Specify how many milliseconds of voice an RTP data packet should contain.

Field	Description
	Possible values are `5` to `500`. The default value is `20`.

9.2.1.2 SIP Accounts

If your want your device to connect to other SIP servers (e.g. servers of Internet SIP Service providers), you can configure the necessary entries here. In this case, the media gateway acts as a SIP client.

Furthermore, you can configure the entries for SIP trunking scenarios here. In this case, the media gateway acts as a SIP server for other SIP servers. An example for this is the connection of a SIP PBX (e.g. Asterisk) to the media gateway.

This means that not only all SIP provider accounts are configured here but also direct dial-in PBXs connected with the media gateway.

> **Note**
>
> In no case should you use this menu to configure SIP extensions, i.e. for SIP clients or PSTN clients such as SIP telephones, terminal adapters or ISDN telephones
>
> SIP extensions can be configured in the **VoIP**->**Extensions** menu.

The **VoIP**->**Settings**->**SIP Accounts** menu displays a list of all existing SIP accounts (SIP Client Mode and SIP Server Mode).

9.2.1.2.1 Edit or New

Select the **New** button to create new SIP accounts. Choose the ✎ icon to edit existing entries. In this menu SIP accounts are configured in SIP client mode as well as in SIP server mode.

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

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the SIP account.
Administrative Status	Select whether the SIP account should be enabled or disabled. The function is enabled with `Enabled`. The function is enabled by default.
Trunk Mode	Select whether and in which trunk mode the SIP account should be operated. Trunk mode (DDI, Direct Dial In) allows an incoming call to be assigned correctly to a terminal (DDI). For an outgoing call, the caller can be indicated to the called party. The setting that you can use depends on the provider. Possible values: • `Off` (default value): Trunk mode is not used. The SIP account has only one number. • `Client`: The media gateway is operated as DDI client. It is assigned a DDI. • `Server`: The media gateway is operated as a DDI server so that DDI clients can connect.

Field	Description
	• *Gateway*: The media gateway is operated as DDI client, but used as a trunk. This setting is used to connect a software-based IP PBX from Swyx.
Registrar	Only for **Trunk Mode** = *Off*, *Client* and *Gateway*Enter the IP address or domain name (FQDN) of the SIP registrar. The maximum number of characters is 40. Entries with spaces are not allowed.
SIP Endpoint IP Address	Only for **Trunk Mode** = *Server* and **Registration** deactivated Enter the IP address or domain name (FQDN) of the SIP proxy server.
Outbound Proxy	Only for **Trunk Mode** = *Off*, *Client* or *Gateway* Enter the name or IP address of the SIP outbound proxy server. A maximum of 32 characters can be entered. Here you must make an entry only if, for all SIP sessions, the communication is not to be direct but via a further proxy. In SIP client mode: Enter a name or IP address only if this is explicitly specified by the provider.
Domain / Realm	Enter a new domain name or a new IP address for the SIP proxy server. If you do not make an entry, the entry in the **Registrar** field is used. In SIP client mode: Enter a name or IP address only if this is explicitly specified by the provider.
Protocol	Select the protocol to be used for data transport. Possible values: • *UDP* (default value) • *TCP* • *TLS* • *Automatic* - With this setting, your device supports automatic negotiation of the protocol with your provider's servers. For this setting to work, this negotiation must also be supported by the provider. Enter the **Port**via which the data is to be transported. The default value is *5060*. In SIP client mode: The ports can be provider-specific. If you prefer a DNS SRV request instead of a DNS A record request for this provider, enter port *0* here. For connections offered by Deutsche Telekom this is a required setting because the SRV entry provides additional server addresses which may provide a better service quality. SIP provider that are created with the Initial Operation menu or with the Telephony assistant automatically use the correct port number.
User Name	In SIP client mode: Enter the username for authentication if your VoIP provider has assigned one for you. In SIP server mode: You must define the user name. A maximum of 40 characters can be entered.

Field	Description
Authentication ID	Enter a name that is to be used for authentication with the outbound proxy. If you do not enter a name, the name in the **User Name** field is used. In SIP client mode: Enter a name only if this is explicitly specified by the provider.
Password	In SIP client mode: The VoIP provider gives you a PIN or password for authentication. You must enter this value here. In SIP server mode: Define a PIN or a password. A maximum of 40 characters can be entered.
Registration type	Specify how registration and authentication at a provider are to be handled, or if they can omitted completely. In the latter case, the relevant data are sent to a particular IP address that is already known to the correspondent. Registration and authentication are not then needed and the Registration function is disabled. An example of this method is Microsoft Exchange SIP. If a registration is required, it can be carried out in either of two ways: • *Single*: With this option, a single MSN is registered with the SIP provider. • *Bulk (BNC)*: With this option, a SIP Trunk (DDI) is registered with the SIP provider, i.e. several numbers are registered under a single address.
Expire Time	Only if **Registration** is enabled. Enter the time in seconds after which the current registration becomes invalid and a new registration request is therefore sent. Possible values are *0* to *38400*. The default value is *600*. In answer to a REGISTER request, a server can set another Expire Time which overwrites the setting here.
Called Address	Determines from which parameter of the called address the number is extracted. Possible values: • *Standard* (default value): Extracts the number from the first part of the address. If this fails, the number is extracted from the second part of the address. • *Request URI*: In some applications (especially in DDI connections) the target address of a SIP call needs to be extracted from the Request URI. By activating this option the address is preferably read from this field of the invite.
Check Source IP	As a response to a DNS SRV request, your SIP provider transmits the addresses of valid registration servers. If you activate this option, each SIP invite has its source IP checked against these valid addresses. If it does not originate from one of them, the invite is ignored. The option is not active per default.
TLS certificate check	Only for DDI / SIP trunk connections. If a connection is encrypted using

Field	Description
	TLS (Transport Layer Security) a validity check on the server certificate of the remote station is performed. The option is not active per default.
Send RTP Dummy	This option is required if the **be.IP smart** is connected to a NAT device that provides internet access towards the SIP provider.

Fields in the Trunk Settings menu.

Field	Description
SIP Header Field: FROM Display	Not for **Trunk Mode** = *Off* The sender ID is placed in the "Display" field of the SIP header. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: FROM User	Not for **Trunk Mode** = *Off* The sender ID is sent in the "User" field of the SIP header. Possible values: • *Username* (default value): The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: P-Preferred	Not for **Trunk Mode** = *Off* The so-called "p-preferred-identity" field is added to the SIP header and contains the sender ID. Possible values: • *None* (default value): The sender ID is not sent. • *Username*: The user-configured user name is displayed. • *Caller Address*: The user-configured number the called party is displayed. • *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
SIP Header Field: P-Asserted	Not for **Trunk Mode** = *Off* The so-called "p-asserted-identity" field is added to the SIP 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.

Field	Description
	• *Billing Number*: The actual phone number from which the calls is initiated (e.g. for billing purposes) is displayed.
Subscribe Number	Only for **Trunk Mode** = *Client* or *Server* You can set a number that is added as a prefix for outgoing calls to the sender's number and is removed from the destination number for incoming calls. This corresponds to the trunk (exchange) number of an exchange.

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

Fields in the Codec Settings menu

Field	Description
Codec Proposal Sequence	Choose the order in which the codecs are offered for use by the media gateway. If the first codec cannot be used, the second is tried and so on. Possible values: • *Default* (default value): the codec in the first position in the menu will be used if possible. • *Quality*: The codecs are sorted by quality. If possible, the codec with the best quality is used. • *Low Bandwidth*: The codecs are sorted by required bandwidth. If possible, the codec with the lowest bandwidth requirement is used. • *High Bandwidth*: The codecs are sorted by required bandwidth. If possible, the codec with the highest bandwidth requirement is used.

Fields in the Codecs menu

Field	Description
Codecs	Select the codecs to be proposed for the connection. The codecs chosen here are proposed in a certain order, depending on the setting in the **Codec Proposal Sequence** field. Possible values: • *G.711 uLaw*: ISDN codec according to US law • *G.711 aLaw*: ISDN codec according to EU law • *G.722*: G.722 passes audio signals in the range of 50-7000 Hz and samples them at the rate of 16,000 samples per second. At 64 kbit/s bit rate the mean opinion score (MOS) is 4,5. • *G.729*: Compressed from 31 to 8 kbps; good voice quality • *G.726-40*: Compressed from 63 to 40 kbps • *G.726-32*: Compressed from 55 to 32 kbps • *G.726-24*: Compressed from 47 to 24 kbps • *G.726-16*: Compressed from 39 to 16 kbps By default *G.711 uLaw*, *G.711 aLaw* and *G.729* are enabled. The codecs actually used are the intersect of the codecs defined here and those signalled by the provider. For outgoing calls, any remaining codecs are dropped from the list that would require more than the available bandwidth.

Fields in the Options menu

Field	Description
Options	Select the option to be used for the connection. Possible values: • *RFC 2833*: First the system attempts to use RFC 2833 for the transmission of DTMF events. If the remote terminal does not use this standard, SIP Info is used. • *SRTP*: SRTP is an encrypted variant of the Real-Time Transport Protocol (RTP). • *Data (RFC 4040)*: Enable the transport of 64 kbit/s channel data in RTP packets. • *SIP Info*: SIP Infor is used for the transmission of DTMF events. • *T.38 Fax*: Allows the transmission of fax messages over data networks. • *SIP 302*: Select whether calls are to be redirected externally with the SIP provider. The call is forwarded using SIP status code 302. • *MediaSec*: MediaSec regulates the protection of SIP data between the SIP server and your system. The function is activated by selecting *Enabled*. The function is disabled by default. For seamless support, automatic negotiation of the transport protocol is mandatory. Fixed transport protocol settings (UDP and TCP) may cause problems during registration. Additionally, the use of SRTP must be allowed. Your VoIP provider must support MediaSec.

Fields in the Voice Quality Settings menu

Field	Description
Echo Cancellation	Select whether echo cancellation should be used. Echo cancellation is a technique to suppress echo feedback in voice communication on full duplex lines. The function is enabled with *Enabled*. The function is enabled by default.
Comfort Noise Generation (CNG)	Specify whether Comfort Noise Generation should be used. For digital voice transmission, this function introduces a low level of background noise to avoid the impression that, during pauses at the other end, the connection is lost. The function is enabled with *Enabled*. The function is enabled by default.
Packet Size	Specify how many milliseconds of voice an RTP data packet should contain. Possible values are *5* to *500*. The default value is *20*.

9.2.1.3 Locations

In the **VoIP**->**Settings**->**Locations** menu you configure the locations of the VoIP subscribers who have been configured on your system, and define the bandwidth management for the VoIP traffic.

Individual locations can be set up for using the bandwidth management. A location is identified from its fixed IP address or DynDNS address or from the interface to which the device is connected. The available VoIP bandwidth (up- and downstream) can be set up for each location.

Only for compact systems: A predefined entry with the parameters **Description** = *LAN*, **Parent Location** = *None*, **Type** = *Interfaces*, **Interfaces** = *LAN_EN1-0* is displayed.

Fields in the Registration behavior for VoIP subscribers without assigned location menu.

Field	Description
Default Behavior	Specify how the system is to proceed when registering VoIP subscribers for whom no location has been defined. Possible values: • *No Registration*: The VoIP subscriber is never registered. • *Registration for Private Networks Only* (default value): The VoIP subscriber is only registered if located within the private network. • *Unrestricted Registration*: The VoIP subscriber is always registered.

9.2.1.3.1 Edit or New

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

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

Fields in the Basic Settings menu.

Field	Description
Description	Enter the description of the entry.
Parent Location	You can cascade the SIP locations as you wish. Define here which SIP location that has been defined constitutes the high-level node for the SIP location to be configured here.
Type	Select whether the location is to be defined through IP addresses/DNS names or interfaces. Possible values: • *Addresses* (default value): The SIP location is defined via IP addresses or DNS names. • *Interfaces*: The SIP location is defined via the available interfaces.
Addresses	Only for **Type** = *Addresses* Enter the IP addresses of the devices at the SIP locations. Click **Add** to configure new addresses. Enter the IP address or DNS name that you want under **IP Address/DNS Name**. Also enter the required **Netmask**.
Interfaces	Only for **Type** = *Interfaces* Indicate the interfaces to which the devices of a SIP location are connected. Click **Add** to select a new interface.

Field	Description
	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 DSCP menu.

Field	Description
DSCP Settings for rtp Traffic	Select the Type of Service (TOS) for RTP data. Possible values: • *DSCP Binary Value* (default value): Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). The preconfigured value is *101110*. • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • *DSCP Hexadecimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • *TOS Binary Value*: The TOS value is specified in binary format, e.g. 00111111. • *TOS Decimal Value*: The TOS value is specified in decimal format, e.g. 63. • *TOS Hexadecimal Value*: The TOS value is specified in hexadecimal format, e.g. 3F.

9.2.1.4 ISDN Trunks

Your device must have at least two ISDN connections in point-to-point mode (BRI or PRI), which are configured as TE (party line) or NT for a configuration in the **ISDN Trunks** menu.

Note

Note that, for BRI connections, the connection mode (NT mode or TE mode) must be set by jumper in the device.

In this menu, the ISDN party lines (bundles) are defined.

9.2.1.4.1 Edit or New

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

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

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the party line. The maximum number of characters is 40.
ISDN Mode	Select the mode in which the party line is to be operated. Possible values: • *Extern* (default value): Point-to-Point TE connection (telecom party line) • *Trunk*: Point-to-Point NT connection (for connection of a PABX).
Members	Select the desired ISDN interfaces to be included with this party line. You can choose among the ISDN connections in point-to-point mode (BRI or PRI), which are configured as TE (party line) or NT.

9.2.1.5 Options

In the **VoIP**->**Settings**->**Options** menu you can perform global settings for the Media Gateway.

The menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Media Gateway Status	Select whether the media gateway function should be enabled. The function is enabled with *Enabled*. The function is disabled by default.
Session Border Controller Mode	Specify how the media gateway should behave in conjunction with a session border controller mode. Possible values: • *Auto* (default value): for all extensions that exactly agree with an existing SIP account, the call routing is handled by the session border controller, i.e. all SIP messages configured for the corresponding SIP account are forwarded to the session border controller. For all other extensions, the call routing is handled by the media gateway in accordance with the entries configured under **Call Routing**. Note that the call routing is handled by the media gateway if the provider is not available (backup). • *Off*: Call routing is handled exclusively by the media gateway in accordance with the entries configured under **Call Routing** and the local extensions. For calls that are to be routed via a particular provider (SIP account), you must configure a corresponding call routing entry. Internal calls (from internal extension to internal extension) that are only to be routed internally do not require an additional call routing entry. • *<SIP Trunk>*: Select a SIP trunk account configured under **VoIP**->**Media Gateway**->**SIP Accounts**. In this case, the call routing for all extensions is handled by the session border controller, all SIP

Field	Description
	messages are forwarded to the session border controller. Note that the call routing is handled by the media gateway if the provider is not available (backup). Please note: Entries in **Call Routing** have priority ahead of the session border controller configuration!
Call Routing for local Extensions	Determine if routing entries are to be preferred over extensions. *Enabled* activates this function. The function is enabled per default.
Media Stream Termination	Choose how RTP sessions are controlled by the system. If the function is enabled, RTP sessions are terminated on the media gateway, i.e. all RTP streams are controlled by the media gateway and routed via the media gateway. The participating terminal devices (e.g. SIP telephones) are not connected directly with one another. Note that, for VoIP to VoIP connections, there is no code translation for different VoIP terminal codecs. The codecs of media gateway and VoIP terminals must therefore agree. If the function is disabled, RTP sessions are not terminated on the media gateway, i.e. all RTP streams are routed by the media gateway without termination. The RTP data packets can be routed in complex networks and thus also via other gateways. The function is enabled with *Enabled*. The function is enabled by default.
Default Drop Extension	You can specify an extension to which incoming calls are forwarded if they cannot be assigned to an extension or connected PABX.
Dial Latency	Enter the maximum delay time before the system assumes the call number entered is complete and starts the SIP dialling process (sends the SIP INVITE message). This timeout is reset each time that a button is pressed. Possible values are *0* to *15*. The default value is *5*. If you terminate the number entered with #, dialling is immediate.

Fields in the VoIP Provider 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).

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.
SIP Port	Specify the port SIP data are to be transferred through. 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.

Fields in the Advanced Settings menu

Field	Description
ISDN Call Signalling	If you have connected a PABX to one of the internal ISDN connections, you can specify how to treat subscriber numbers of a DDI here. For some PABXs the type of number has to be identified, and the **International Prefix / Country Code** and/or the **National Prefix / Area Code** have to be removed from the subscriber number in order to correctly identify the subscriber. You can do this by selecting *Specific: international, national or subsriber number*. Possible values: • *Standard: always as unknown number*: The type of number is not detected. • *Specific: international, national or subscriber number*: The type of number is detected. If required, the **International Prefix / Country Code** and/or the **National Prefix / Area Code** are removed from the subscriber number
Speed Dialing	Define short sequences of numbers that can be dialled instead of the entire number. Click **Add** to configure new speeddial numbers. Enter the desired speeddial number for the user, e.g. *123* under **Shortcut**. Under **Replacement** enter the subscriber number to be dialled in place of the speed dial number, e.g. *09119673*. In the example above, if a user types in **123*, the device dials *09119673*. If the user wishes to call extension *111*, he types in **123111*. The device dials *09119673111*. A period at the end of the number indicates a complete number. This is dialled immediately the period is recognised. If you want to use a speeddial number from the list, you must dial * followed by the speeddial number.

Fields in the SIP dual Stack (IPv4/IPv6) menu

Field	Description
SIP dual Stack (IPv4/IPv6)	Enable this option if you want to support IPv6 for VoIP. Both, IPv4 as well as IPv6 are supported, and if a VoIP provider supports IPv6, IPv6 is preferred. If a VoIP provides does not support IPv6, IPv4 is used. With selection of *Activated* the option is anabled. The function is not enabled by default. This means that only IPv4 is used until you enable dual stack SIP.

9.2.2 Media Gateway

A media gateway serves as a translation instance between different telecommunications networks, e.g between the plain old phone network and the next generation networks (IP networks).

With the **be.IP** Media Gateway, a company equipped with an automatic PBX on a wired telephone network can be connected to a SIP Trunking Service Provider on the Internet in order to use IP telephony.

The **be.IP** Media Gateway supports the binding of several SIP Provider Accounts. With this gateway, you can set up extensions, create an extension number plan and configure exchange functions and optimise voice data transmission for low bandwidth of the upload connection.

9.2.2.1 Call Routing

Here you can define the conditions for the routing of calls. Define a list with rules or rule chains that are used to manipulate the indicated destination numbers.

A list of all existing entries is displayed in the **VoIP**->**Media Gateway**->**Call Routing** menu.

9.2.2.1.1 Edit or New

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

The **VoIP**->**Media Gateway**->**Call Routing**->✎->**New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the entry.
Administrative Status	Select whether the entry should be activated. The function is enabled with *Enable*. The function is enabled by default.
Type	Specify how calls are to be routed. Possible values: • *Accept Rule*: For calls forwarded by the media gateway to a PBX or an ISDN TE connector or a SIP DDI client. For this, the following can be used: PRI interfaces in NT mode, BRI interfaces in NT mode, SIP accounts in trunk mode (server mode). • *Deny*: For calls that are not to be routed (to be blocked).
Calling Line	You can restrict the application of the entry to the line on which the call comes in. The selection depends on the interfaces available and on the SIP accounts that have been created.

Field	Description
	Possible values: - *pri<Interface Index>*: restricts the routing entry to the selected PRI interface. - *bri<Interface Index>*: restricts the routing entry to the selected BRI interface. - *<SIP Account>*: restricts the routing entry to the selected SIP account. - *Any*: No restriction of the entry.
Calling Address	You can restrict the application of the entry to a particular caller. To do this, you must specify the subscriber number exactly (no wildcards).
Called Address	Enter the called address to which the rule is to be applied. To do this, enter an address numerically (e.g. a subscriber number) or alphanumerically (e.g. for a trunk) that is to be compared with a dialled address. The following wildcards can be used: - * means that at the end of a character string any number of characters may follow, - ? is a placeholder for an arbitrary character. If the configured address agrees with the signalled address, the entry is used.

In the **Routing Rules** menu you can define rules to determine how the subscriber number is manipulated before it is used for dialling.

Use **Add** to create more entries.

Fields in the Routing Rules menu (For Type = Accept Rule only)

Field	Description
Priority	Enter a whole number starting with 1 in ascending order to define the order of filter rules. The rules are worked through in the order given in the list. If a line or SIP account is not available, the next rule is automatically used.
Administrative Status	Select whether the rule should be activated. The rule is enabled with *Enable*. The rule is active by default.
Line	Choose the ISDN line (PRI, BRI) or SIP account used for the outgoing call.
Called Address Translation	Enter how the subscriber number is manipulated before it is used for dialling. Notation: <a:b>; i.e. a is replaced by b. Every rule must be ended with a semicolon. A number of rules can be chained together using semicolons as separators, e.g. <a:b>;<c:d>;<e:f>. After confirmation of entry, the rule chain is automatically sorted by the "best match" method. Numerical and alphanumerical values are permissible.

Field	Description
	? is a placeholder for an arbitrary character. **Example 9.1. Example of a rule** • Rule: <:+49911>; • number dialled: 96731234 • manipulated number: +4991196731234

9.2.2.2 CLID Translation

Here you define the processing of the calling party number for incoming calls. You can, for example, add a prefix to a received call number in order to route corresponding outgoing calls via a particular SIP account.

In the **VoIP**->**Media Gateway**->**CLID Translation** menu, a list of all existing entries is shown on which the received number is edited.

9.2.2.2.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create entries for CLID translation.

The **VoIP**->**Media Gateway**->**CLID Translation**->✎->**New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the entry.
Calling Line	Select the ISDN line or SIP account from which the call comes. The selection depends on the interfaces available and on the SIP accounts that have been created. Possible values: • *pri<Interface Index>*: Restricts the entry to the selected PRI interface. • *bri<Interface Index>*: Restricts the entry to the selected BRI interface. • *<SIP Account>*: Restricts the entry to the selected SIP account. • *Any*: No restriction of the entry.
Called Line	Here you have the option of entering the destination line of the call. Possible values: • *pri<Interface Index>*: Restricts the entry to the selected PRI interface. • *bri<Interface Index>*: Restricts the entry to the selected BRI interface. • *<SIP Account>*: Restricts the entry to the selected SIP account. • *Any*: No restriction of the entry. Enter either **Called Line** or **Called Address**. If a value other than *Any* is selected, **Called Address** should not be used. If **Called Line** = *Any* and **Called Address** is not used, all calls for **Called Line** are processed.

Field	Description
Called Address	Here you have the option of entering the destination address of the call. Enter either **Called Line** or **Called Address**. If **Called Address** is used, then **Called Line** = *Any* can be set .
Calling Address Translation	Enter the transformation rule applied to the call numbers. Notation: <a:b>; i.e. a is replaced by b. Every rule must be ended with a semicolon. A number of rules can be chained together using semicolons as separators, e.g. <a:b>;<c:d>;<e:f>;. After confirmation of entry, the rule chain is automatically sorted by the "best match" method. ? is a placeholder for an arbitrary digit. **Example 9.2. Example of a rule** • Rule: <:+49911>; • number dialled: 96731234 • manipulated number: +4991196731234

9.2.2.3 Call Translation

You can create a list for the translation of subscriber numbers, i.e. this list associates internal and external numbers.

> **Note**
>
> Which number (called party number or calling party number) is translated depends on the direction (incoming or outgoing) of the call in question. For incoming calls it is the called party number, for outgoing calls the calling party number that is translated.

For example, the internal number 340 can be shown externally as 09119673900 or a call from outside for the number 09119673200 can be routed internally to the number 340.

In the **VoIP**->**Media Gateway**->**Call Translation** menu, a list of existing transformations is displayed.

9.2.2.3.1 Edit or New

Choose the ✎ icon to edit existing entries. Select the **New** button to create entries for call translation.

The **VoIP**->**Media Gateway**->**Call Translation**->✎ ->**New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter the name of the call translation.
Direction	Select the direction for the entry. Possible values: • *Both* (default value): For incoming and outgoing calls (bidirectional). • *Incoming*: For incoming calls. • *Outgoing*: For outgoing calls.
Associated Line	Select the ISDN line or SIP account via which the calls are to be routed. Possible values:

Field	Description
	• *pri<Interface Index>*: Restricts the call to the selected PRI interface. • *bri<Interface Index>*: Restricts the call to the selected BRI interface. • *<SIP Account>*: restricts the call to the selected SIP account.
Local Address	Enter the internal number (e.g. extension or PABX number). For incoming calls, the signalled Called Party Number (corresponds in the menu to the **External Address**) is translated to **Local Address**. For outgoing calls, the signalled Calling Party Number (corresponds in the menu to the **Local Address** field) is translated to **External Address**. Numerical and alphanumerical characters are permissible. *?* is a placeholder for an arbitrary digit. See **Local Address** and **External Address** must contain the same number of wildcards.
External Address	Enter the external number (e.g. ISDN MSN or SIP account subscriber number). For incoming calls, the signalled Called Party Number (corresponds in the menu to the **External Address**) is translated to **Local Address**. For outgoing calls, the signalled Calling Party Number (corresponds in the menu to the **Local Address** field) is translated to **External Address**. The **External Address** is not shown if the field **Associated Line** = *<SIP Account>* is set. In this case, the **User Name** of the selected SIP Account is used as **External Address**..

9.2.2.4 Special Numbers

At a DDI connection, the called number of an outgoing call is automatically converted to the international E.164 format. This conversion is undesirable for certain numbers. Exceptions from the conversion can be configured here.

9.2.2.4.1 Edit or New

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

The **Call Routing**->**Outgoing Services**->**Special Numbers**->**New** menu consists of the following fields:

Fields in the Basic Settings menu

Field	Description
Description	Enter a description for the entry.
Special Number	Specify the number that is to be excepted from E.164 conversion.

Chapter 10 WLAN

10.1 Wireless LAN

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

Network functions

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

Currently applicable standard: IEEE 802.11. Information on the modi contained in the standard and the correspondingly supported transmission speeds are, e.g., avilable at *Wikipedia*.

10.1.1 WLAN

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

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

10.1.1.1 Radio Settings

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

10.1.1.1.1 Radio Settings-> ✎

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

Select the ✎ icon to edit the configuration.

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

Fields in the menu Wireless Settings

Field	Description
Operation Mode	Define the mode in which the wireless module of your device is to operate. Possible values: • *Off* (default value): The wireless module is not active. • *Access-Point*: Your device is used as an access point in your network.
Operation Band	Select the operation band and, where applicable, the usage area of the wireless module. For **Operation Mode** = *Access-Point* 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 runs in 5 GHz inside buildings.

Field	Description
	• *5 GHz Outdoor*: Your device runs in 5 GHz outside buildings. • *5 GHz In/Outdoor*: Your device is run with 5 GHz inside or outside buildings.
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 clients actually support these channels. Possible values: • For **Operation Band** = *2.4 GHz In/Outdoor* Possible values are *1* to *13* and *Auto* (default value). *Auto* is not possible in bridge mode. • For **Operation Band** = *5 GHz Indoor* Possible values are *36*, *40*, *44*, *48* and *Auto* (default value) • For **Operation Band** = *5 GHz In/Outdoor* and *5 GHz Outdoor* Only the *Auto* option is possible here.
Transmit Power	Select the maximum value for the radiated antenna power. The actually radiated antenna power may be lower than the maximum value set, depending on the data rate transmitted. The maximum value for Transmit Power is country-dependent. Possible values: • *Max.* (default value): The maximum antenna power is used. • *5 dBm* • *8 dBm* • *11 dBm* • *14 dBm* • *16 dBm* • *17 dBm*

Fields in the menu Performance Settings

Field	Description
Wireless Mode	Select the wireless technology that the access point is to use. Only for **Operation Mode** = *Access Point* and **Operation Band** = *2.4 GHz In/Outdoor* Possible values: • *802.11g*: The device operates only in accordance with 802.11g.

Field	Description
	802.11b clients have no access. • *802.11b*: Your device operates only in accordance with 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 Mode** = *Access-Point* and **Operation Band** = *5 GHz Indoor*, *5 GHz Outdoor*, *5 GHz In/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.
Bandwidth	For **Operation Mode** = *Access-Point* Not for **Operation Band** = *2.4 GHz In/Outdoor* Select how many channels are to be used. Possible values: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channels and the other as an expansion channel.
Number of Spatial Streams	Not for **Wireless Mode** = *802.11a* Select how many traffic flows are to be used in parallel. Possible values: • *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*.

Field	Description
	The function is disabled by default. This fuction is only applied to unprioritized frames of the WMM Classe "Background".

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

Fields in the Advanced Settings menu for Operation Mode = Access Point

Field	Description
Channel Plan	Only for **Operation Mode** = `Access-Point` and **Channel** = `Auto` 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`: Select the desired channels.
Selected Channels	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 delete entries with the 🗑 icon.
RTS Threshold	Here, you select how the RTS/CTS mechanism is to be switched on/off. If you choose `User-defined`, you can specify in the input field the data packet length threshold in bytes (1 - 2346) as of which the RTS/CTS mechanism is to be used. This makes sense if several clients that are not in each other's wireless range are run in one access point. The mechanism can also be switched on/off independently of the data packet length by selecting the value `Always on` or `Always off` (default value).
Short Guard Interval	Enable this function to reduce the guard interval (= time between transmission of two data symbols) from 800 ns to 400 ns.
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` bytes.

10.1.1.2 Wireless Networks (VSS)

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

Note

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

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

Setting network names

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

Protection of wireless networks

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

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

WEP

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

IEEE 802.11i

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

WPA

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

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

WPA 2

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

Access control

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

Security measures

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

- Change the access passwords for your device.
- Change the default SSID, **Network Name (SSID)** = *default*, of your access point. Set **Visible** = *Enabled*. This will exclude all WLAN clients that attempt to establish a connection with the general value for **Network Name (SSID)** *Any* and do not know the SSID settings.
- Use the available encryption methods. To do this, select **Security Mode** = *WEP 40*, *WEP 104*, *WPA-PSK* or *WPA Enterprise* and enter the relevant key in the access point under **WEP Key 1 - 4** or **Preshared Key** and in the WLAN clients.
- The WEP key should be changed regularly. To do this, change the **Transmit Key**. Select the longer 104 Bit WEP key.
- For transmission of information with very high security relevance, configure **Security Mode** = *WPA Enterprise*with **WPA Mode** = *WPA 2*. This method contains hardware-based encryption and RADIUS authentication of the client. In special cases, combination with IPSec is possible.
- Restrict WLAN access to permitted clients. Enter the MAC addresses of the wireless network cards for these clients in the **Allowed Addresses** list in the **MAC-Filter** menu (see *Fields in the menu MAC-Filter* on page 193).

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

10.1.1.2.1 Edit or New

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

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

Fields in the menu Service Set Parameters

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

Field	Description
	The function is enabled by default. Users of the guest WLAN should normally have access to the Internet but no access to the company's intranet. To prevent this, the option must be disabled.
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.

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*: 802.11i/TKIP
Transmit Key	Only for **Security Mode** = *WEP 40* or *WEP 104* Select one of the keys configured in **WEP Key** <1 - 4> as a default 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 applied. • *WPA*: Only **WPA** is applied. • *WPA 2*: Only **WPA 2** is applied.
WPA Cipher	Only for **Security Mode** = *WPA-PSK* and *WPA Enterprise* and for **WPA Mode** = *WPA* and *WPA and WPA 2* Select the type of encryption with which to apply **WPA**. Possible values: • *AES* : AES is used. • *TKIP*: TKIP is used.

Field	Description
	• *AES and TKIP* (default value): 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 with which to apply **WPA 2**. Possible values: • *AES* : AES is used. • *AES and TKIP* (default value): 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!
EAP Preauthentification	Only for **Security Mode** = *WPA Enterprise* Select whether the EAP preauthentification function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This maximum is 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

Field	Description
	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 wireless 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.

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. 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 Advanced Settings

Field	Description
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*.
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.

10.1.2 Administration

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

10.1.2.1 Basic Settings

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

Fields in the WLAN Administration menu.

Field	Description
Region	Select the country in which the access point is to be run. Possible values are all the countries configured on the device's wireless module. The range of channels available for selection (**Channel** in the **Wireless LAN**->**WLAN**->**Radio Settings** menu) changes depending on the country setting. The default value is *Germany*.

10.2 Wireless LAN Controller

By using the wireless LAN controller, you can set up and manage a WLAN infrastructure with an access point (AP). **be.IP smart** assumes the master role, the AP operates as a slave.

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.

Provided the controller has "located" your AP in its system, it receives a new passport and configuration in succession, i.e. they are managed via the WLAN controller and can no longer be manipulated "externally".

With the **WLAN controller** you can

- automatically detect your access point (AP) and connect to a WLAN network

- Load the system software into the AP
- Load the configuration into the AP
- Monitor and manage the AP

For information about the AP number you can manage with the wireless LAN controller of your gateway and the necessary licenses, please consult the data sheet of your device.

10.2.1 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.

10.2.1.1 Wireless LAN Controller Wizard

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

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

IP Address Range

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

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

10.2.1.1.2 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.

10.2.1.1.3 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.

10.2.1.1.3.1 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, 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 enabled by default.

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.

10.2.1.1.4 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 displayed you will see how far the installation has progressed. The display is continuously updated.

Provided that non-overlapping wireless channels are located for all access points, the configuration that is set in the Wizard is transferred to the access points.

When the installation is complete, you will see a list of the **Managed** access points.

Under **Configure the Alert Service for WLAN surveillance**, click **Start** to monitor your managed APs. You are taken to the **External Reporting**->**Alert Service**->**Alert Recipient** menu with the default setting **Event** = *Managed AP offline*. You can specify that you wish to be notified by e-mail if the *Managed AP offline* event occurs.

Click under **New Neighborscan** on **Start**, to rescan adjacent AP's. You will receive a warning that the wireless modules of the access points must also be disabled for a certain period of time. When you start the process with **OK**, a progress bar is displayed. The located AP display is updated every ten seconds.

10.2.1.2 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.

10.2.1.2.1 Edit or New

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	Dscription
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**.

10.2.2 Controller Configuration

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

10.2.2.1 General

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

Fields in the Basic Settings menu

Field	Description
Status	Activate the function to set the basic settings for the wireless LAN controller.
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 **be.IP** 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 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.

Field	Description
	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): Only the status LED flashes once per second. • *Flashing*: All LEDs show their standard behavior. • *Off*: All LEDs are deactivated.

10.2.2.2 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.

10.2.2.2.1 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 menu

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*

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

10.2.3 Slave AP configuration

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

10.2.3.1 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 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.

10.2.3.1.1 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*

Field	Description
	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)
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.

10.2.3.2 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**).

10.2.3.2.1 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 Radio Profile Definition menu

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:

Field	Description
	• *2.4 GHz In/Outdoor* (default value): Your device is operated at 2.4 GHz (mode 802.11b, mode 802.11g and mode 802.11n), inside or outside buildings. • *5 GHz Indoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) inside buildings. • *5 GHz Outdoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) outside buildings. • *5 GHz In/Outdoor*: Your device is operated at 5 GHz (mode 802.11a/h and mode 802.11n) 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 Performance Settings menu

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 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. • *802.11ac/a/n*: (if supported by your device) Your device operates only according to either 802.11ac, a or n. • *802.11ac/n*: (if supported by your device) Your device operates ac-

Field	Description
	cording 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: • *20 MHz* (default value): One channel with 20 MHz bandwidth is used. • *40 MHz*: Two channels each with 20 MHz bandwidth are used. In the case one channel acts as a control channel and the other as an expansion channel. • *80 MHz*: In mode 802.11ac you can also use a bandwidth of 80 MHz.
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. 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 Advanced Settings menu

Field	Description
Channel Plan	Select the desired channel plan.

Field	Description
	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*. 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.

Field	Description
	Possible values are *1* to *255*. The default value is *7*.
Long Retry Limit	Enter the maximum number of attempts to send a data packet of length greater than the value defined in **RTS Threshold**. After this many failed attempts, the packet is discarded. Possible values are *1* to *255*. The default value is *4*.
Fragmentation Threshold	Enter the maximum size as of which the data packets are to be fragmented (i.e. split into smaller units). Low values are recommended for this field in areas with poor reception and in the event of radio interference. Possible values are *256* to *2346*. The default value is *2346*.

10.2.3.3 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.

10.2.3.3.1 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 Service Set Parameters menu

Field	Description
Network Name (SSID)	Enter the name of the wireless network (SSID). Enter an ASCII string with a maximum of 32 characters. Also select whether the **Network Name (SSID)** is to be transmitted. The network name is displayed by selecting *Visible*. It is visible by default.
Intra-cell Repeating	Select whether communication between the WLAN clients is to be permitted within a radio cell. The function is activated by selecting *Enabled*. The function is enabled by default. Users of the guest WLAN should normally have access to the Internet but no access to the company's intranet. To prevent this, the option must be disabled.
U-APSD	Select whether the Unscheduled Automatic Power Save Delivery

Field	Description
	(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 Security Settings menu

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* Select the type of encryption you want to apply to WPA. Possible values:

Field	Description
	- *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	You can control access to a wireless network via a RADIUS server. With **Add**, you can create new entries. Enter the IP address and the password of the RADIUS server.
EAP Preauthentification	Only for **Security Mode** = *WPA Enterprise* Select whether the EAP preauthentification function is to be activated. This function tells your device that WLAN clients, which are already connected to another access point, can first carry out 802.1x authentication as soon as they are within range. Such WLAN clients can then simply connect over the existing network connection with your device. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the menu Client load balancing

Field	Description
Max. number of clients - hard limit	Enter the maximum number of clients that can be connected to this wireless network (SSID) The maximum number of clients that can register with a wireless module depends on the specifications of the respective WLAN module. This maximum is 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

Field	Description
	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 wireless 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 Controller**->**Monitoring**->**Rogue Clients** menu. The function is activated by selecting *Enabled*. The function is activated by default.

Field	Description
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 VLAN menu

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) • *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. Possible values are • *No limit* (default value) • *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*.

10.2.4 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.

10.2.4.1 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.

Status	Meaning
AP offline	Displays the number of access points not connected to the Wireless LAN Controller.
AP managed	Displays the number of managed access points.
WLAN Controller: VSS throughput	Displays the data traffic in receive and transmit direction in bytes per second.
CPU usage [%]	Displays the percentaged CPU load over time.
Memory usage [%]	Displays the percentaged memory consumption over time.
Connected clients/VSS	Displays the number of connected clients per wireless network (VSS) over time.

10.2.4.2 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 🔍 icon, you can open an summary with additional details about the **Slave Access Points**.

10.2.4.2.1 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.

10.2.4.2.2 Radio 1

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

Values in the Radio list

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

10.2.4.3 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 🔍 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.

10.2.4.4 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**).

10.2.4.5 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.

10.2.5 Neighbor Monitoring

This menu serves the monitoring of remote access points.

10.2.5.1 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.

10.2.5.2 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.

10.2.5.3 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.
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.

10.2.5.3.1 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.

10.2.6 Maintenance

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

10.2.6.1 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.

10.3 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.

10.3.1 WLAN

10.3.1.1 WLANx

In the **Monitoring**->**WLAN**->**WLAN** menu, current values and activities of the WLAN interface are displayed. The values for wireless mode 802.11n are listed separately.

Values in the WLANx Statistics list

Field	Description
mbps	Displays the possible data rates on this wireless module.
Tx Packets	Shows the total number of packets sent for the data rate shown in **mbps**.
Rx Packets	Shows the total number of received packets for the data rate shown in **mbps**.

You can choose the **Advanced** button to go to an overview of more details.

Values in the Advanced list

Field	Description
Description	Displays the description of the displayed value.
Value	Displays the statistical value.

Meaning of the list entries

Description	Meaning
Unicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to unicast addresses since the last reset. An acknowledgement was received for each of these packets.
Multicast MSDUs transmitted successfully	Displays the number of MSDUs successfully sent to multicast addresses (including the broadcast MAC address).
Transmitted MPDUs	Displays the number of MPDUs received successfully.
Multicast MSDUs received successfully	Displays the number of successfully received MSDUs that were sent with a multicast address.
Unicast MPDUs received successfully	Displays the number of successfully received MSDUs that were sent with a unicast address.
MSDUs that could not be transmitted	Displays the number of MSDUs that could not be sent.
Frame transmissions without ACK received	Displays the number of sent framesfor which an acknowledgement frame was not received.
Duplicate received MSDUs	Displays the number of MSDUs received in duplicate.
CTS frames received in response to an RTS	Displays the number of received CTS (clear to send) frames that were received as a response to RTS (request to send).
Received MPDUs that couldn't be decrypted	Displays the number of received MSDUs that could not be encrypted. One reason for this could be that a suitable key was not entered.
RTS frames with no CTS received	Displays the number of RTS frames for which no CTS was received.
Corrupt Frames Received	Displays the number of frames received incompletely or with errors.

10.3.1.2 VSS

In the **Monitoring**->**WLAN**->**VSS** menu, current values and activities of the configured wireless networks are displayed.

Values in the Client Node Table list

Field	Description
MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the client is logged in.
Tx Packets	Shows the total number of packets sent.
Rx Packets	Shows the total number of packets received.
Signal dBm (RSSI1, RSSI2,	Shows the received signal strength in dBm.

Field	Description
RSSI3)	
Noise dBm	Shows the received noise strength in dBm.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24, 18, 12, 9, 6 mbps. If the 5 GHz frequency band is used, the indication of 11, 5.5, 2 and 1 mbps is suppressed for IEEE 802.11b.
Rx Discards	Displays the number of received data packets that have been discarded if the bandwidth for receive traffic has been limited in the **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**-> ✎ menu using the field **Rx Shaping**
Tx Discards	Displays the number of data packets that were queued for transmission and have been discarded if the bandwidth for transmit traffic has been limited in the **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**-> ✎ menu using the field **Rx Shaping**.

VSS - Details for Connected Clients

In the **Monitoring**->**WLAN**->**VSS**-><**Connected Client**> -> 🔍 menu, the current values and activities of a connected client are shown. The values for wireless mode 802.11n are listed separately.

Values in the list <Connected Client>

Field	Description
Client MAC Address	Shows the MAC address of the associated client.
IP Address	Shows the IP address of the client.
Uptime	Shows the time in hours, minutes and seconds for which the client is logged in.
Signal dBm(RSSI1, RSSI2, RSSI3)	Shows the received signal strength in dBm.
Noise dBm	Shows the received noise strength in dBm.
SNR dB	Signal-to-Noise Ratio in dB is an indicator of the quality of the wireless connection. Values: • > 25 dB excellent • 15 – 25 dB good • 2 – 15 dB borderline • 0 – 2 dB bad.
Data Rate mbps	Shows the current transmission rate of data received by this client in mbps. The following clock rates are possible: IEEE 802.11b: 11, 5.5, 2 and 1 mbps; IEEE 802.11g/a: 54, 48, 36, 24, 18, 12, 9.6 Mbps. If the 5-GHz frequency band is used, the indication of 11, 5.5, 2 and 1 Mbps is suppressed for IEEE 802.11b.
Rate	Displays the possible data rates on the wireless module.
Tx Packets	Shows the number of sent packets for the data rate.
Rx Packets	Shows the number of received packets for the data rate.

10.3.1.3 Client Management

The **Monitoring**->**WLAN**->**Client Management** menu displays an overview of the **Client Management**. For each VSS you can see such information as the number of clients connected, the number of clients that are affected by the **2,4/5 GHz changeover**, and the number of rejected clients.

Values in the list Client Management

Field	Description
VSS Description	Displays the unique description of the wireless network (VSS).
Network Name (SSID)	Displays the name of the wireless network (SSID).
MAC Address	Displays the MAC address being used for this VSS.
Active Clients	Displays the number of active clients.
2,4/5 GHz changeover	Displays the number of clients who have been moved to a different frequency band by the **2,4/5 GHz changeover** function.
Denied Clients soft/hard	Displays the number of rejected clients after the absolute number of permitted clients has been reached.

Chapter 11 Internet & Network

11.1 Physical Interfaces

11.1.1 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 preconfigured with **IP Address** *192.168.2.1* and **Netmask** *255.255.255.0* .

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

☞ **Note**

To ensure your 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 port being 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 a completely independent configuration of the interface is made possible.

VLANs for Routing Interfaces

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

11.1.1.1 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 Port Configuration, 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.

Field	Description
Ethernet Interface Selection	Assign a logical Ethernet interface to the switch port. You can select from five interfaces, *en1-0* to *en1-2*. In the basic setting, switch ports **1**-**4** are assigned the *en1-0* interface.
Configured Speed / Mode	Select the mode in which the interface is to run. Possible values: • *Full Autonegotiation* (default value) • *Auto 1000 mbps only* • *Auto 100 mbps only* • *Auto 10 mbps only* • *Auto 100 mbps / Full Duplex* • *Auto 100 mbps / Half Duplex* • *Auto 10 mbps / Full Duplex* • *Auto 10 mbps / Half Duplex* • *Fixed 1000 mbps / Full Duplex* • *Fixed 100 mbps / Full Duplex* • *Fixed 100 mbps / Half Duplex* • *Fixed 10 mbps / Full Duplex* • *Fixed 10 mbps / Half Duplex* • *None* : The interface is created but remains inactive.
Current Speed / Mode	Shows the actual mode and actual speed of the interface. Possible values: • *1000 mbps / Full Duplex* • *100 mbps / Full Duplex* • *100 mbps / Half Duplex* • *10 mbps / Full Duplex* • *10 mbps / Half Duplex* • *Down*
Flow Control	Select whether a flow control should be conducted on the corresponding interface. Possible values: • *Disabled* (default value): No flow control is performed. • *Enabled*. Flow control is performed. • *Auto*: Automatic flow control is performed.

11.1.2 DSL Modem

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

11.1.2.1 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
Physical Connection	Shows the current ADSL operation mode. The value cannot be changed. Possible values: • *Unknown*: The ADSL link is not active. • *ADSL1*: ADSL classic, G.DMT, ITU-T G.992.1 • *ADSL2*: G.DMT.Bis, ITU-T G.992.3 • *ADSL2 Plus*: ADSL2 Plus, ITU-T G.992.5 • *ADSL2+ Annex J*: ITU-T G.992.5 • *VDSL2*: ITU-T G.993.2
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.
DSL Chipset	Shows the key of the installed chipset.

Fields in the DSL Parameter menu

Field	Description
DSL Mode	Displays the selected DSL operating mode Possible values: • *Inactive*: The link is not active. • *ETSI T1.413*: ETSI T1.413 • *ADSL1*: ADSL classic, G.DMT, ITU-T G.992.1 • *ADSL Automode* (default value if the device is operated as a PBX): Automatic detection of ADSL mode *ADSL1*, *ADSL2* or *ADSL2 Plus* • *ADSL2*: G.DMT.Bis, ITU-T G.992.3 • *ADSL2 Plus*: ADSL2 Plus, ITU-T G.992.5 • *VDSL*: VDSL2 (ITU-T G.993.2) • *VDSL/ADSL Multimode* (default value if the device is operated as a Media Gateway): Automatic detection of DSL mode *ADSL1*, *ADSL2* , *ADSL2 Plus* or *VDSL*
Transmit Shaping	Select whether the data rate in the send direction is to be reduced. This is only needed in a few cases for special DSLAMs. Possible values: • *Default (Line Speed)* (default value): The data rate in the send direction is not reduced. • *128,000 bps* to *2,048,000 bps*: The data rate in the send direction is reduced to a maximum of 128,000 bps to 2,048,000 bps in defined steps. • *User-defined*:The data rate is reduced to the value entered in **Maximum Upstream Bandwidth**.
Maximum Upstream Band-	Only for **Transmit Shaping** = *User-defined*

Field	Description
width	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 Profiles menu

Field	Description
DSL 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.

11.2 LAN

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

11.2.1 IP Configuration

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

11.2.1.1 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

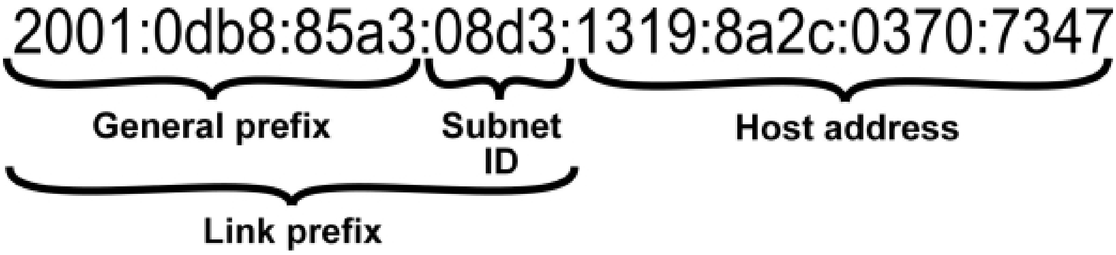
If your device is connected to a LAN that consists of two subnets, you should enter a second **IP Address / Netmask**.

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.

Configuring IPv6 addresses

In addition to IPv4 addresses, you can also used IPv6 addresses.

The following shows an example for an IPv6 address:



Your device can operate either as a router or as a host on an interface. In general, it operates on LAN interfaces as a router, and on WAN interfaces and PPP connections as a host.

If your device operates as a router, you can form its own IPv6 addresses as follows: a link prefix can be derived from a general prefix, or you can enter a static value. A host address can be generated from *Auto eui-64*; for additional host addresses you can enter the static values.

If your device operates as a router, it generally distributes the configured link prefix to the hosts by router advertisement. Over a DHCP server, additional information such as the address of a time server is transmitted to the hosts. The client can generates its host address either by stateless address autoconfiguration (SLAAC) or be assigned the address by a DHCP server.

For the router mode described above, in the menu **LAN**->**IP Configuration**->**Interfaces**->**New** choose the settings **IPv6 Mode** = *Router*, **Transmit Router Advertisement** *Enabled* **DHCP Server** *Enabled* and **IPv6 Addresses Add**.

If your device operates as a host, it is assigned a link prefix from another router by router advertisement. The host address is then generated automatically by SLAAC. Additional information, such as the general prefix of the provider or the address of a time server, can be obtained by DHCP. To do this, go to the **LAN**->**IP Configuration**->**Interfaces**->**New** menu and choose the settings **IPv6 Mode** = *Client*, **Accept Router Advertisement** *Enabled* and **DHCP Client** = *Enabled*.

11.2.1.1.1 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.

Field	Description
	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 module.
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, if you enable **Use built-in**. The VLAN IDs must be different however. You can also allocate a virtual MAC address. The first 6 characters of the MAC are preset (but can be changed). If **Use built-in** is activated, the default MAC address of the underlying physical interface is used. **Use built-in**is active by default.

Fields in the Basic IPv4 Parameters menu

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted*: All IP packets are allowed through except for those which are explicitly prohibited. • *Untrusted*: Only IP packets that can be assigned to a connection established from a trustworthy zone are allowed through. You can configure exceptions for the selected setting in the *Firewall* on page 318 menu.
Address Mode	Select how an IP address is assigned to the interface. Possible values: • *Static* (default value): The interface is assigned a static IP address in **IP Address / Netmask**. • *DHCP*: An IP address is assigned to the interface dynamically via DHCP.
DHCP Metric	It is possible to assign a metric for gateway route received by an interface via DHCP. This may be necessary when configuring backup connections to ensure a clean switch to the backup and back again. The default value is *1*. In case of a backup solution, this option should be set to a higher value so the backup route does not receive a too high priority.

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

Fields in the Basic IPv6 Parameters menu

Field	Description
IPv6	Select whether the selected 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	Here 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 IP packets that can be assigned to a connection established from a trustworthy zone are allowed through. 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 318 menu.
IPv6 Mode	Only for **IPv6** = *Enabled* Choose whether the interface is only operated in host mode or in router mode. Depending on the selection made, different parameters are displayed that must be configured. Possible values: • *Router (Transmit Router Advertisement)* (default value): The interface is operated in router mode. • *Host*: The interface is operated in host mode.
DHCP Server	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Router* Define whether your device should operate as a DHCP server, i.e. whether DHCP options should be sent, to forward information on the DNS servers to the clients, for example. Enable this option if hosts are to generate IPv6 addresses by SLAAC. The function is activated by selecting *Enabled*. The function is enabled by default.
Accept Router Advertisement	Only for **IPv6** = *Enabled* and **IPv6 Mode** = *Host* Select whether router advertisements are to be received via the selected interface. The prefix list, for example, is created using router advertisements.

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* Define whether your device should operate as a DHCP client, i.e. whether DHCP options should be received, to receive information on the DNS servers, for example. The function is activated by selecting *Enabled*. The function is enabled by default.
IPv6 Addresses	Only for **IPv6** = *Enabled* You can assign the selected interface **IPv6 Addresses**. With **Add** you can create one or more address entries. An additional window opens in which you can define an IPv6 address consisting of a link prefix and a host part. If your device operates in host mode (**IPv6 Mode** = *Host*, **Accept Router Advertisement** *Enabled* and **DHCP Client** *Enabled*), its IPv6 addresses are defined by SLAAC. You do not need to configure any IPv6 address manually, but can enter additional addresses on request. If your device operates in router mode (**IPv6 Mode** = *Router*, and **DHCP Server** *Enabled*), you must configure its IPv6 addresses here.

Use **Add** to create more entries.

Fields in the Basic Parameters menu

Field	Description
Advertise	Only for **IPv6 Mode** = *Router* Here you can define whether this prefix is sent by router advertisement via the selected interface, based on the link prefix defined in the current window. The function is activated by selecting *Enabled*. The function is enabled by default.

Fields in the Link Prefix menu

Field	Description
Setup Mode	Select the way in which the link prefix is defined. 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 from which the link prefix is to be derived. You may choose from the general prefixes created under **Network**->**IPv6 General Prefixes**->**General Prefix Configuration**->**New**.

Field	Description
Auto Subnet Configuration	Only if **Setup Mode** = *From General Prefix* and if **General Prefix** is selected. Select whether the subnet is to be created automatically. When generating the subnet automatically, the ID *0* is used for the first subnet the subnet ID *1* for the second subnet, and so on. Possible values for **Subnet ID** are *0* to *255*. The subnet ID describes the fourth of the four 16 bit fields of a link prefix. When generating the subnet, the decimal ID value is converted into a hexadecimal value. The function is activated by selecting *Enabled*. The function is enabled by default. If the function is not active, you can define a subnet by entering the subnet ID.
Subnet ID	Only if **Auto Subnet Configuration** is not enabled. Enter a subnet ID to define a subnet. The subnet ID describes the fourth and four 16 bit fields of a link prefix. Possible values are *0* to *255*. When generating the subnet, the entered decimal ID value is converted into a hexadecimal value.
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	Define whether the host part of the IPv6 address is to be generated automatically by EUI-64 from the MAC address. The function is activated by selecting *Enabled*. The function is enabled by default. EUI-64 initiates the following process: • The hexadecimal 48 bit MAC address is divided into 2 x 24 bits. • *FFFE* is inserted into the gap created to obtain 64 bits. • The hexadecimal format of the 64 bits is converted into the dual format. • Bit 7 is set to *1* in the first 8 bit field.
Static Addresses	Irrespective of automatic generation defined under **Generation Mode**, you can manually enter the host part of an IPv6 address or multiple IPv6 addresses with **Add**. Its length is set to *64*. Start your entry with *::* .

Fields in the **Advanced** menu are part of the prefix information, which is sent in the router advertisement if **Advertise** is active. 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.

Field	Description
	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 a host to use the prefix and an 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, the addresses that have been generated using the prefix over SLAAC are given preference. 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.

Field	Description
	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. 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**.
Router Preference	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router* and **Transmit Router Advertisement** = *Enabled*. Select your router's preference for choice of default router. This is useful for cases where a node receives advertisements from multiple routers, or for back-up scenarios. Possible values: • *High* • *Medium* (default value) • *Low*
DHCP Mode	Only for **IPv6** = *Enabled*, **IPv6 Mode** = *Router* and **Transmit Router**

Field	Description
	Advertisement = *Enabled*. Select the information to be forwarded to the DHCP client. **Note** To achieve this, your router must not be set up as a DHCP server. By selecting *Other - DNS Servers, SIP Servers* (default value), no address-related information, such as i.e. DNS, VoIP, etc., is passed through. Enable this option if hosts in the network are to form their IP addresses automatically over SLAAC. In this case, the router sends only non address-related data over DHCP. By selecting *Managed - IPv6 Address Management* IPv6 addresses and all non address-related data is obtained from the host over DHCP.
DNS Propagation	Only for **IPv6 Mode** = *Router* and **Transmit Router Advertisement** = *Enabled* Choose whether DNS server addresses are to be propagated via router advertisements and if yes, in which way. A maximum of two DNS server addresses are to be propagated. Possible values: • *Off*: No DNS server address is propagated. • *Self*: An own IP address is propagated as the DNS server address. For multiple addresses, the addresses are propagated in the following order: • Global addresses • ULA (Unique Local Addresses) • Link local addresses • *Other*: Statically configured and dynamically learned DNS server entries are propagated according to priority. If no entries exist, no addresses are propagated.

11.2.2 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-aware 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**.

11.2.2.1 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.

11.2.2.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to configure other 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 default 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).

11.2.2.2 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.
Drop non-members	If this option is enabled, all tagged frames that are tagged with a VLAN ID to which the selected port does not belong are discarded.

11.2.2.3 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-Gruppe br<ID> VLAN-Optionen 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.

11.3 Networking

11.3.1 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**.

11.3.1.1 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.

11.3.1.1.1 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.

Field	Description
	• *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. **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.

Field	Description
	When **Route Type** = *Network Route via Interface* Also enter the relevant netmask in the second field.
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. • *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.

Field	Description
	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 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

Field	Description
	routing until the interface is "up".

11.3.1.2 IPv6 Route Configuration

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

11.3.1.2.1 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 when no other suitable route is available. • *Default Route via Gateway*: Route via a specific gateway, which is used when no other suitable 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	ISelect the IPv6 interface to be used for this route. You may choose from the interfaces created under **LAN**->**IP Configuration**->**Interfaces**->**New** and for which use of IPv6 is activated.
Source Address / Length	Enter the IPv6 source address along with the corresponding prefix length. The entry *::* describes an unspecific address. By default the prefix length *64* is predefined.
Destination Address / Length	Enter the IPv6 destination address along with the corresponding prefix length. The entry *::* describes an unspecific address. By default the prefix length *64* is predefined.

Field	Description
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 *255*. The default value is *1*.

11.3.1.3 IPv4 Routing Table

A list of all active IPv4 routes is displayed in the **Network**->**Routes**->**IPv4 Routing Table** 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*, **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 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.

11.3.1.4 IPv6 Routing Table

A list of all active 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.

11.3.1.5 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*. By default, the function is deactivated for all interfaces.

11.3.2 IPv6 General Prefixes

IPv6 General Prefixes are generally assigned by IPv6 providers. These can be statically assigned or obtained via DHCP. Generally these are /48 or /56 networks. From these general prefixes you can generate /64 subnets and distributes these within your network.

The concept of general prefixes has two decisive advantages:

- A single route between provider and customer is sufficient.
- If the provider assigns a new general prefix via DHCP or a statically assigned general prefix has to be modified, you as the customer have little or no configuration work to carry out: Via DHCP you automatically receive the new general prefix. In the case of a statically assigned general prefix, you must do these once in your system. All of the subnets and IPv6 addresses derived from this general prefix change automatically when updating the general prefix.

To use IPv6, you must configure how you want to define and distribute subnets and IPv6 addresses (see "Configure IPv6 addresses under *Interfaces* on page 223 and the parameters relevant for IPv6 in the **LAN**->**IP Configuration**->**Interfaces** menu.

11.3.2.1 General Prefix Configuration

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

11.3.2.1.1 Edit or New

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

Options in the menu Basic Parameters

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. By default, the prefix is enabled.
Name	Enter a name for the general prefix. A meaningful name allows the general prefix to be selected easily 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 will be predefined, e.g. by a provider.
From Interface	Only if **Type** = *Dynamic* Select the IPv6 interface from which a **General Prefix** is to be obtained. You may choose from the interfaces created under **LAN**->**IP Configuration**->**Interfaces**->**New** and that satisfy the following conditions: • **IPv6** is *Enabled*. • **IPv6 Mode** = *Host* • **DHCP Client** is *Enabled*.
Used Prefix / Length	Only if **Type** = *Static* Enter the prefix to be used. Enter the corresponding length. This prefix must end with ::. By default the length *48* is predifined.

11.3.3 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 241).

11.3.3.1 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 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**.

11.3.3.2 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.

11.3.3.2.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to set up NAT.

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

Fields in the Basic Parameters menu

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.

Field	Description
	• *excluding (Without NAT)*: Data traffic excluded from NAT.
NAT method	Only for **Type of traffic** = *outgoing (Source NAT)* Select the NAT method for outgoing data traffic. The starting point for choosing the NAT method is a NAT scenario in which an "internal" source host has initiated an IP connection to an "external" destination host over the NAT interface, and in which an internally valid source address and internally valid source port are translated to an externally valid source address and an externally valid source port. 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* (default 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 Specify original traffic menu

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 data packets to be excluded from NAT. Possible values: • *Exclude* (default value): All data packets will be excluded from NAT if they match the subsequently specified parameters (Protocol, Source IP Address/Netmask, Destination IP Address/Netmask, ect.). • *Do not exclude*: All data packets will be excluded from NAT if they do not match the subsequently specified parameters (Protocol, Source IP Address/Netmask, Destination IP Address/Netmask, ect.).
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.

Field	Description
	Possible values: • *Any* (default value) • *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP* • *ISO-IP* • *Kryptolan* • *L2TP* • *OSPF* • *PUP* • *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP* • *VRRP* • *XNS-IDP*
Source IP Address/Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* or *exclusive (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

Field	Description
	data packets, as the case arises.
Original Source Port/ Range	Only for **Type of traffic** = *outgoing (Source NAT)*, **NAT method** = *symmetric*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Enter the source port of the original data packets. The default setting *-All-* means that the port remains unspecified. If you select *Specify port* you can specify a single port, if you select *Specify port range* you can specify a 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 is not specified.

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 Replacement Values menu

Field	Description
New Destination IP Address/Netmask	Only for **Type of traffic** = *incoming (Destination NAT)* Enter the destination IP address to which the original source IP address is to be translated, with corresponding netmask, as the case arises.
New Destination Port	Only for **Type of traffic** = *incoming (Destination NAT)*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* Leave the destination port as it appears or enter the destination port to which the original destination port is to be translated. Selecting *Original* leaves the original destination port. If you disable *Original*, an input field appears in which 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.

Field	Description
New Source Port	Only for **Type of traffic** = *incoming (Destination NAT)*, **NAT method** = *symmetrical*, **Service** = *user-defined* and **Protocol** = *TCP*, *UDP*, *TCP/UDP* 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 follwing 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.

11.3.4 Load Balancing

The increasing amount of data traffic over the Internet means it is necessary to send data over different interfaces to increase the total bandwidth available. IP load balancing enables the distribution of data traffic within a certain group of interfaces to be controlled.

11.3.4.1 Load Balancing Groups

If interfaces are combined to form groups, the data traffic within a group is divided according to the following principles:

- In contrast to Multilink PPP-based solutions, load balancing also functions with accounts with different providers.
- Session-based load balancing is achieved.
- Related (dependent) sessions are always routed over the same interface.
- A decision on distribution is only made for outgoing sessions.

A list of all configured load balancing groups is displayed in the **Networking**->**Load Balancing**->**Load Balancing Groups** menu. You can click the 🔍 icon next to any list entry to go to an overview of the basic parameters that affect this group.

Note

Note that the interfaces that are combined into a load balancing group must have routes with the same metric. If necessary, go to the **Networking**->**Routes** menu and check the entries there.

11.3.4.1.1 New

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

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

Fields in the Basic Parameters menu

Field	Description
Group Description	Enter the desired description of the interface group.

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

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

Use **Add** to create more entries.

Fields in the Basic Parameters menu.

Field	Description
Group Description	Shows the description of the interface group.
Distribution Policy	Displays the type of data traffic selected.

Fields in the Interface Selection for Distribution menu

Field	Description
Interface	Select the interfaces that are to belong to the group from the available interfaces.
Distribution Ratio	Enter the percentage of the data traffic to be assigned to an interface. The meaning differs according to the **Distribution Ratio** employed: • For *Session-Round-Robin* is based on the number of distributed sessions. • For *Load-dependent Bandwidth*, the data rate is the decisive factor.

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

Fields in the Advanced Settings menu

Field	Description
Route Selector	The **Route Selector** parameter is an additional criterion to help define a load balancing group more precisely. Here, routing information is added to the "interface" entry within a load balancing group. The route selector is required in certain scenarios to enable the IP sessions managed by the router to be balanced uniquely for each load balancing group. The following rules apply when using the parameter: • If an interface is only assigned to one load balancing group, it is not necessary to configure the route selector. • If an interface is assigned to multiple load balancing groups, configuration of the route selector is essential. • The route selector must be configured identically for all interface entries within a load balancing group. Select the **Destination IP Address** of the desired route. You can choose between all routes and all extended routes.
Tracking IP Address	You can use the **Tracking IP Address** parameter to have a particular route monitored. The load balancing status of the interface and the status of the routes connected to the interface can be influenced using this parameter. This means that routes can be enabled or disabled irrespective of the interface's operation status. The connection is monitored using the gateway's host surveillance function here. Host surveillance entries must be configured in order to use this function. These can be configured in the **Local Services**->**Surveillance**->**Hosts** menu. Here, it is important that only the host surveillance entries with the action **Monitor** are taken into account in the context of load balancing. Links between the load balancing function and the host surveillance function are made through the configuration of the **Tracking IP Address** in the **Load Balancing**->**Load Balancing Groups**->**Advanced Settings** menu. The interface's load balancing status now varies according to the status of the assigned host surveillance entry. Select the IP address for the route to be monitored. You can choose from the IP addresses you have entered in the **Local Services**->**Surveillance**->**Hosts**->**New** menu under **Monitored IP Address** and which are monitored with the aid of the **Action to be executed** field (**Action** = `Monitor`).

11.3.4.2 Special Session Handling

Special Session Handling enables you to route part of the data traffic to your device via a particular interface. This data traffic is excluded from the **Load Balancing** function.

You can use the **Special Session Handling** function with online banking, for example, to ensure that the HTTPS data traffic is sent to a particular link. Since a check is run in online banking to see whether all the data traffic comes from the same source, data transmission using **Load Balancing** might be terminated at times without **Special Session Handling**.

The **Networking**->**Load Balancing**->**Special Session Handling** menu displays a list of entries. If you have not configured any entries, the list is empty.

Every entry contains parameters which describe the properties of a data packet in more or less detail. The first data packet which the properties configured here match specifies the route for particular subsequent data packets.

Which data packets are subsequently routed via this route is configured in the **Networking**->**Load Balancing**->**Special Session Handling**->**New**->**Advanced Settings** menu.

If in the **Networking**->**Load Balancing**->**Special Session Handling**->**New** menu, for example, you select the parameter **Service** = *http (SSL)* (and leave the default value for all the other parameters), the first HTTPS packet specifies the **Destination Address** and the **Destination Port** (i. e. Port 443 with HTTPS) for data packets sent subsequently.

If, under**Frozen Parameters**, for the two parameters **Destination Address** and **Destination Port** you leave the default setting *enabled*, the HTTPS packets with the same source IP address as the first HTTPS packet are routed via port 443 to the same **Destination Address** via the same interface as the first HTTPS packet.

11.3.4.2.1 Edit or New

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

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

Fields in the Basic Parameters menu

Field	Description
Admin Status	Select whether the Special Session Handling should be activated. The function is activated by selecting *Enabled*. The function is enabled by default.
Description	Enter a name for the entry.
Service	Select one of the preconfigured services, if required. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth* • *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.
Protocol	Select a protocol, if required. The *Any* option (default value) matches any protocol.
Destination IP Address/ Netmask	Enter, if required, the destination IP address and netmask of the data packets. Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host. • *Network*: Enter the network address and the related netmask.
Destination Port/Range	Enter, if required, a destination port number or a range of destination port numbers.

Field	Description
	Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Source Interface	If required, select your device's source interface.
Source IP Address/Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: • *Any* (default value) • *Host*: Enter the IP address of the host. • *Network*: Enter the network address and the related netmask.
Source Port/Range	Enter, if required, a source port number or a range of source port numbers. Possible values: • *-All-* (default value): The destination port is not specified. • *Specify port*: Enter a destination port. • *Specify port range*: Enter a destination port range.
Special Handling Timer	Enter the time period during which the specified data packets are to be routed via the route that has been defined. The default value is *900* seconds.

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

Fields in the Advanced Settings menu.

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

11.3.5 QoS

QoS (Quality of Service) makes it possible to distribute the available bandwidths effectively and intelligently. Certain applications can be given preference and bandwidth reserved for them. This is an advantage, especially for time-critical applications such as VoIP.

The QoS configuration consists of three parts:

- Creating IP filters
- Classifying data
- Prioritising data.

11.3.5.1 IPv4/IPv6 Filter

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

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

11.3.5.1.1 New

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

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

Fields in the Basic Parameters menu.

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

Field	Description
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. 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.

Field	Description
	• *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*.

11.3.5.2 QoS Classification

The data traffic is classified in the **Networking**->**QoS**->**QoS Classification** menu, i.e. the data traffic is associated using class IDs of various classes. To do this, create class plans for classifying IP packets based on pre-defined IP filters. Each class plan is associated to at least one interface via its first filter.

11.3.5.2.1 New

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

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

Fields in the Basic Parameters menu

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

Field	Description
Direction	Select the direction of the data packets to be classified. Possible values: • *Incoming*: Incoming data packets are assigned to the class (**Class ID**) that is then to be defined. • *Outgoing* (default value): Outgoing data packets are assigned to the class (**Class ID**) that is then to be defined. • *Both*: Incoming and outgoing data packets are assigned to the class (**Class ID**) that is then to be defined.
High Priority Class	Enable or disable the high priority class. If the high priority class is active, the data packets are associated with the class with the highest priority and priority 0 is set automatically. The function is enabled with *Enabled*. The function is disabled by default.
Class ID	Only for **High Priority Class** not active. Choose a number which assigns the data packets to a class. **Note** The class ID is a label to assign data packets to specific classes. (The class ID defines the priority.) Possible values are whole numbers between *1* and *254*.
Set DSCP/Traffic Class Filter (Layer 3)	Here you can set or change the DSCP/TOS value of the IP data packets, based on the class (**Class ID**) that has been defined. Possible values: • *Preserve* (default value): The DSCP/TOS value of the IP data packets remains unchanged. • *DSCP Binary Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format). • *DSCP Decimal Value*: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP 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*.

Field	Description
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.

11.3.5.3 QoS Interfaces/Policies

In the **Networking**->**QoS**->**QoS Interfaces/Policies** menu, you set prioritisation of data.

Note

Data can only be prioritized in the outgoing direction.

Packets in the high-priority class always take priority over data with class IDs 1.. 254.

It is possible to assign or guarantee each queue and thus each data class a certain part of the total bandwidth of the interface. In addition, you can optimise the transmission of voice data (real time data).

Depending on the respective interface, a queue is created automatically for each class, but only for data traffic classified as outgoing and for data traffic classified in both directions. A priority is assigned to these automatic queues. The value of the priority is equal to the value of the class ID. You can change the default priority of a queue. If you add new queues, you can also use classes in other class plans via the class ID.

11.3.5.3.1 New

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

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

Fields in the Basic Parameters menu

Field	Description
Interface	Select the interface for which QoS is to be configured.
Prioritisation Algorithm	Select the algorithm according to which the queues are to be processed. This activates and deactivates QoS on the selected interface. Possible values: • *Priority Queueing* (default value): QoS is activated on the interface. The available bandwidth is distributed strictly according to the queue priority. • *Weighted Round Robin*: QoS is activated on the interface. The available bandwidth is distributed according to the weighting (weight) of the queue. Exception: High-priority packets are always handled with priority. • *Weighted Fair Queueing*: QoS is activated on the interface. The available bandwidth is distributed as “fairly” as possible among the (automatically detected) traffic flows in a queue. Exception: High-priority packets are always handled with priority. • *Disabled* : 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.

Field	Description
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	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 bytes; possible values are *0* to *100*.) • Undefined (Protocol Header Offset=0) (default value) Can only be selected for Ethernet interfaces • *Ethernet* • *Ethernet and VLAN* • *PPP over Ethernet* • *PPP over Ethernet and VLAN* Can only be selected for IPSec interfaces: • *IPSec over Ethernet* • *IPSec over Ethernet and VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE and VLAN*
Encryption Method	Only if an IPSec Peers is selected as **Interface**, **Traffic shaping** is *Active* and **Protocol Header Size below Layer 3** is not *Undefiniert (Protocol Header Offset=0).* Select the encryption method used for the IPSec connection. The encryption algorithm determines the length of the block cipher which is taken into account during bandwidth calculation. Possible values: • *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.

Field	Description
	Select the mode for optimising voice transmission. Possible values: • *All RTP Streams*: All RTP streams are optimised. The function activates the RTP stream detection mechanism for the automatic detection of RTP streams. In this mode, the Real Time Jitter Control is activated as soon as an RTP stream has been detected. • *Inactive*: Voice data transmission is not optimised. • *Controlled RTP Streams only*: This mode is used if either the VoIP Application Layer Gateway (ALG) or the VoIP Media Gateway (MGW) is active. Real Time Jitter Control is activated by the control instances ALG or MGW. • *Always*: Real Time Jitter Control is always active, even if no real time data is routed.

Fields in the Queues/Policies menu

Field	Description
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”.
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*.

Field	Description
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 Speed	Only for **Traffic Shaping** = enabled. Enter a maximum data rate for the queue in kbits. Possible values are *0* to *1000000*. The default value is *0*.
Overbooking allowed	Only for **Traffic Shaping** = enabled. Enable or disable the function. The function controls the bandwidth limit. If **Overbooking allowed** is activated, the bandwidth limit set for this queue can be exceeded, as long as free bandwidth exists on the interface. If **Overbooking allowed** is deactivated, the queue can never occupy bandwidth beyond the bandwidth limit that has been set. The function is enabled with *Enabled*. The function is disabled by default.
Burst size	Only for **Traffic Shaping** = enabled. Enter the maximum number of bytes that may still be transmitted temporarily when the data rate permitted for this queue has been reached. Possible values are *0* to *64000*. The default value is *0*.

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

Fields in the Advanced Settings menu

Field	Description
Dropping Algorithm	Choose the procedure for rejecting packets in the QoS queue, if the maximum size of the queue is exceeded. Possible values: • *Tail Drop* (default value): The newest packet received is dropped. • *Head Drop*: The oldest packet in the queue is dropped. • *Random Drop*: A randomly selected packet is dropped from the queue.
Congestion Avoidance (RED)	Enable or disable preventative deletion of data packets. Packets which have a data size of between **Min. queue size** and **Max. queue size** are preventively dropped to prevent queue overflow (RED=Random Early Detection). This procedure ensures a smaller long-term queue size for TCP-based data traffic, so that traffic bursts can also usually be transmitted without large packet losses. The function is activated with *Enabled*. The function is disabled by default.
Min. queue size	Enter the lower threshold value for the process **prevention of data congestion (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 **prevention of data congestion (RED)** in bytes. Possible values are *0* to *262143*. The default value is *16384*.

11.3.6 Access Rules

Accesses to data and functions are restricted with access lists (which user gets to use which services and files).

You define filters for IP packets in order to allow or block access from or to the various hosts in connected networks. This enables you to prevent undesired connections being set up via the gateway. Access lists define the type of IP traffic the gateway is to accept or deny. The access decision is based on information contained in the IP packets, e.g.:

- source and/or destination IP address
- packet protocol
- source and/or destination port (port ranges are supported)

Access lists are an effective means if, for example, sites with LANs interconnected over a **be.IP** 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 use in the access lists to tell the gateway what to do with the filtered data packets, i.e. whether it should allow or deny them. You can also define several rules, which you arrange in the form of a chain to obtain a certain sequence.

There are various approaches for the definition of rules and rule chains:

Allow all packets that are not explicitly denied, i.e.:

- Deny all packets that match Filter 1.
- Deny all packets that match Filter 2.
- ...
- Allow the rest.

or

- Allow all packets that are explicitly allowed, i.e.:
- Allow all packets that match Filter 1.
- Allow all packets that match Filter 2.
- ...
- Deny the rest.

or

- Combination of the two possibilities described above.

A number of separate rule chains can be created. The same filter can also be used in different rule chains.

You can also assign a rule chain individually to each interface.

⚠ **Caution**

Make sure you don’t lock yourself out when configuring filters:

If possible, access your gateway for filter configuration over the serial console interface or ISDN Login.

11.3.6.1 Access Filter

This menu is for configuration of access filter Each filter describes a certain part of the IP traffic and defines, for example, the IP addresses, the protocol, the source port or the destination port.

A list of all access filters is displayed in the **Networking**->**Access Rules**->**Access Filter** menu.

11.3.6.1.1 Edit or New

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

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

Fields in the Basic Parameters menu.

Field	Description
Description	Enter a description for the filter.
Service	Select one of the preconfigured services. The extensive range of services configured ex works includes the following: • *activity* • *apple-qt* • *auth*

Field	Description
	• *charge* • *clients_1* • *daytime* • *dhcp* • *discard* The default value is *User defined*.
Protocol	Select a protocol. The *Any* option (default value) matches any protocol.
Type	Only if **Protocol** = *ICMP* Possible values: • *Any* • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time exceeded* • *Timestamp* • *Timestamp reply* The default value is *Any*. See RFC 792.
Connection State	Only if **Protocol** = *TCP* You can define a filter that takes the status of the TCP connections into account. Possible values: • *Any* (default value): All TCP packets match the filter. • *Established*: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter.
Destination IPv4 Address/ Netmask	Enter the destination IPv4 address of the data packets and the corresponding netmask. Possible values: • *Any* (default value): The destination IP address/netmask are not specified. • *Host*: Enter the destination IP address of the host. • *Network*: Enter the destination network address and the corresponding netmask.
Destination IPv6 Address/ Length	Enter the destination IPv6 address of the data packets and the prefix length. Possible values: • *Any* (default value): The destination IP address/length are not specified. • *Host*: Enter the destination IP address of the host.

Field	Description
	• *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* 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.

Field	Description
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*.

11.3.6.2 Rule Chains

Rules for IP filters are configured in the access list 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.

11.3.6.2.1 Edit or New

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

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

Fields in the Basic Parameters menu

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

To set the rules of a rule chain in a different order select the ⇅ button in the list menu for the entry to be shifted. A dialog 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.

11.3.6.3 Interface Assignment

In this menu, the configured rule chains are assigned to the individual interfaces and the gateway's behavior is defined for denying IP packets.

A list of all configured interface assignments is displayed in the **Networking**->**Access Rules**->**Interface Assignment** menu.

11.3.6.3.1 Edit or New

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

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

Fields in the Basic Parameters menu

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

11.4 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.

11.4.1 General

11.4.1.1 General

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

The menu consists of the following fields:

Fields in the Basic Settings menu

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

11.4.2 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.

11.4.2.1 IGMP

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

11.4.2.1.1 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.

Field	Description
	Possible values are `0,0` to `25,0`. The default value is `1,0`.
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** .

11.4.2.2 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.

Field	Description
	- *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.
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.
IGMP State Limit	Enter the maximum permitted total number of incoming queries and messages per second. The default value is *0*, i.e. the number of IGMP status messages is not limited.

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.

11.4.3 Forwarding

11.4.3.1 Forwarding

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

11.4.3.1.1 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, set the checkmark for **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.

11.5 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.

11.5.1 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 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.

11.5.1.1 PPPoE

A list of all PPPoE 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.

11.5.1.1.1 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.
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.

Field	Description
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 flatrate 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: • `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 318 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.

Field	Description
Route Entries	Only if **IP Address Mode** = *Static* Define other routing entries for this connection partner. Add new entries with **Add**. • *Remote IP Address*: IP address of the destination host or network. • *Netmask*: Netmask for **Remote IP Address** If no entry is made, your device uses a default netmask. • *Metric*: The lower the value, the higher the priority of the route (range of values *0*... *15*). The default value is *1*.

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 318 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. 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*

Field	Description
	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* 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

Field	Description
	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. • *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

Field	Description
	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 **DNS Server** primary domain name server **Primary** and **DNS Server** secondary domain name server **Secondary** 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	Check whether the reachability 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) 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*.

11.5.1.2 PPPoA

A list of all PPTP 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**.

11.5.1.2.1 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 flatrate 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: • *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 318 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*.

Field	Description
	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 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 318 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* Wählen Sie, ob Router-Advertisements über das ATM-Profil empfangen werden sollen. Mithilfe der Router-Advertisements wird die Default Router List sowie die Prefix List erstellt.

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.
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*.

Field	Description
	The function is enabled by default. If the function is disabled, you can define a subnet by entering a Subnet ID.
Subnet ID	Only if **Auto Subnet Configuration** is not active. Enter a Subnet ID in order to define a subnet. The subnet ID describes the fourth of the four 16 bit fields of a Link Prefix. Possible values are *0* - *65535*. Upon subnet creation the decimal ID value is converted to a hexadecimal one.
Link Prefix	Only for **Setup Mode** = *Static* You can specify the Link Prefix of an IPv6 address. This prefix must end with *::*. Its predetermined length is *64*.

Fields in the Host Address menu.

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

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

Fields in the Advanced Settings menu.

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

Field	Description
	• *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.
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.

11.5.1.3 ISDN

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

In this menu, you configure the following ISDN connections:

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

11.5.1.3.1 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.

Field	Description
	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 Dialin 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 flatrate charge.
Connection Idle Timeout	Only if **Always on** is disabled. Enter the idle interval in seconds. This determines how many seconds should pass between sending the last traffic data packet and clearing the connection. Possible values are *0* to *3600* (seconds). *0* deactivates the timeout. The default value is *20*.

Fields in the IP Mode and Routes menu

Field	Description
IP Address Mode	Select whether your device is to be assigned a static IP address or whether it should be assigned this dynamically. Possible values: • *Static* (default value): You enter a static IP address. • *Provide IP Address*: Your device dynamically assigns an IP address to the remote terminal. • *Get IP Address*: Your device is dynamically assigned an IP address.
Default Route	Only for **IP Address Mode** = *Static* and *Get IP Address* Select whether the route to this connection partner is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Create NAT Policy	Only for **IP Address Mode** = *Static* and *Get IP Address*

Field	Description
	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.
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 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.

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.
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. • *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 num-

Field	Description
	ber 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 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.
Port Usage	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

Field	Description
	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.

11.5.1.4 IP Pools

> **Note**
>
> Note that the menu **IP Pools** is only available if a port in the menu **Physical Interfaces**->**ISDN Ports**-> **ISDN Configuration** is set to external operation (TE mode). A corresponding adapter which is available seperately needs to be connected for external operation.

In the **IP Pools** a list of all IP pools is displayed.

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 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.

11.5.1.4.1 Edit or New

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

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

Fields in the Basic Parameters menu

Field	Description
IP Pool Name	Enter the name of the IP pool.
IP Address Range	In the first field, enter the first IP address of the range. In the second field, enter the last IP address of the range.
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.

11.5.2 ATM

ATM (Asynchronous Transfer Mode) is a data transmission procedure that was originally designed for broadband ISDN.

ATM is currently used in high-speed networks. You will need ATM, for example, if you want high-speed access to the Internet via the integrated ADSL or SHDSL modem.

In an ATM network, different applications such as speech, video and data, can be transmitted side-by-side in the asynchronous time multiplex procedure. Each transmitter is provided with time sections for transmitting data. With asynchronous transmission, unused time sections of a transmitter are used by another transmitter.

With ATM, the packet switching procedure is connected-based. A virtual connection is used for data transmission that negotiates between the transmitter and recipient or is configured on both sides. This determines the route that the data should take, for example. Multiple virtual connections can be set up over a single physical interface.

The data is transmitted in so-called cells or slots of constant size. Each cell consists of 48 bytes of usage data and 5 bytes of control information. The control information contains, amongst other things, the ATM address which is similar to the Internet address. The ATM address is made up of the Virtual Path Identifier (VPI) and the Virtual Connection Identifier (VCI); this identifies the virtual connection.

Various types of traffic flows are transported over ATM. To take account of the various demands of these traffic flows on the networks, e.g. in terms of cell loss and delay time, suitable values can be defined using the service categories. Uncompressed video data, for example, requires different parameters to time-uncritical data.

In ATM networks Quality of Service (QoS) is available, i.e. the size of various network parameters, such as bit rate, delay and jitter can be guaranteed.

OAM (Operation, Administration and Maintenance) is used to monitor the data transmission in ATM. OAM includes configuration management, error management and performance measurement.

11.5.2.1 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*).

11.5.2.1.1 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 identification number of the virtual channel. A virtual channel is the logical connection for the transport of ATM cells between two or more points. Note your provider's instructions. Possible values are *32* to *65535*. The default value is 32.
Encapsulation	Only for **Provider** = `-- User-defined --` Select the encapsulation to be used. Note your provider's instructions. Possible values (in accordance with RFC 2684): • *LLC Bridged no FCS* (Default value for Ethernet over ATM : Is only displayed for **Type** = *Ethernet over ATM*. Bridged Ethernet with LLC/SNAP encapsulation without Frame Check Sequence (checksums).

Field	Description
	- *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 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** (standard 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*.

Field	Description
DHCP Hostname	Only for **Address Mode** = `DHCP`. If necessary, enter the host name registered with the provider to be used by your device for DHCP requests. The maximum length of the entry is 45 characters.

Fields in menu Routed Protocols over ATM Settings (appears only for Type = Routed Protocols over ATM)

Field	Description
IP Address/Netmask	Enter the IP addresses (**IP Address**) and the corresponding netmasks (**Netmask**) of the ATM interface. Add new entries with **Add**.
Prioritize TCP ACK Packets	Select whether the TCP download is to be optimised in the event of intensive TCP upload. This function can be specially applied for asymmetrical bandwidths (ADSL). The function is enabled with `Enabled`. The function is disabled by default.

Field in menu PPP over ATM Settings (appears only for Type = PPP over ATM)

Field	Description
Client Type	Select whether the PPPoA connection is to be set up permanently or on demand. Possible values: • `On Demand` (default value): The PPPoA is only set up on demand, e.g. for Internet access. You'll find additional information on PPP over ATM under *PPPoA* on page 275.

11.5.2.2 Service Categories

In the **WAN**->**ATM**->**Service Categories** menu is displayed a list of already configured ATM connections (PVC, Permanent Virtual Circuit) to which specific data traffic parameters were assigned.

Your device supports QoS (Quality of Service) for ATM interfaces.

Caution

ATM QoS should only be used if your provider specifies a list of data traffic parameters (traffic contract).

The configuration of ATM QoS requires extensive knowledge of ATM technology and the way the **be.IP** devices function. An incorrect configuration can cause considerable disruption during operation. If applicable, save the original configuration on your PC.

11.5.2.2.1 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. When you select the ATM service category a priority is implicitly assigned: from CBR (highest priority) through VBR.1 /VBR.3 to VBR (lowest priority). Possible settings: • *Unspecified Bit Rate (UBR)* (default value): (Unspecified Bit Rate) A particular data rate is not 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)* : (Variable Bit Rate) The connection is assigned a guaranteed data rate (**Sustained Cell Rate (SCR)** This may be exceeded by the volume configured in **Maximum Burst Size (MBS)**. Any additional ATM traffic is discarded. The **Peak Cell Rate (PCR)** constitutes the maximum possible data rate. This category is suitable for non-critical applications with burst data traffic. • *Variable Bit Rate V.3 (VBR.3)* : (Variable Bit Rate) The connection is assigned a guaranteed data rate (**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*.

11.5.2.3 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 **be.IP** 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.

11.5.2.3.1 New

Choose the **New** button to set up monitoring for other flow levels.

The menu **WAN**->**ATM**->**OAM Controlling**->**New** consists of the following fields:

Fields in the OAM Flow Configuration menu

Field	Description
OAM Flow Level	Select the OAM flow level to be monitored. Possible values: • *F5*: (virtual channel level) The OAM settings are used for the virtual channel (default value). • *F4* : (virtual path level) The OAM settings are used on the virtual path.
Virtual Channel Connection (VCC)	Only for **OAM Flow Level** = *F5* Select the already configured ATM connection to be monitored (displayed by the combination of VPI and VCI).
Virtual Path Connection (VPC)	Only for **OAM Flow Level** = *F4* Select the already configured virtual path connection to be monitored (displayed by the VPI).

Fields in the Loopback menu

Field	Description
Loopback End-to-End	Select whether you activate the loopback test for the connection between the endpoints of the VCC or VPC. The function is enabled with *Enabled*. The function is disabled by default.

Field	Description
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 *999*. The default value is *5*.
Loopback Segment	Select whether you want to activate the loopback test for the segment connection (segment = connection of the local endpoint to the next connection point) of the VCC or VPC. The function is enabled with *Enabled*. The function is disabled by default.
Segment Send Interval	Only if **Loopback Segment** is enabled. Enter the time in seconds after which a loopback cell is sent. Possible values are *0* to *999*. The default value is *5*.
Segment Pending Requests	Only if **Loopback Segment** is enabled. Enter the number of directly consecutive loopback cells that may fail to materialise before the connection is regarded as interrupted ("down"). Possible values are *1* to *999*. 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.

11.5.3 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.

11.5.3.1 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.

11.5.3.1.1 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.

Field	Description
	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 kbps for the selected interface.

11.6 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.

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.

11.6.1 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 38). The IPSec implementation in your device achieves this firstly by using the Authentication Header (AH) protocol and Encapsulated Security Payload (ESP) protocol, and secondly through the use of cryptographic key administration mechanisms like the Internet Key Exchange (IKE) protocol.

Additional Traffic Filter

be.IP 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 doe simplify many configurations, problems may also be caused by competing routes or the "coarser" filtering of data traffic.

The **Additional Traffic Filter** parameter fixes this problem. You can apply a "finer" filter, i.e. you can enter the source IP address or the source port. If a **Additional Traffic Filter** is configured, this is used to negotiate the IPSec phase 2 SAs; the route now only determines which data traffic is to be routed.

If an IP packet does not match the defined **Additional Traffic Filter** , it is rejected.

If an IP packet meets the requirements in an **Additional Traffic Filter** , IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

> **Note**
>
> The parameter **Additional Traffic Filter** is exclusively relevant for the initiator of the IPSec connection, it is only used for outgoing traffic.

> **Note**
>
> Please note that the phase 2 policies must be configured identically on both of the IPSec tunnel endpoints.

11.6.1.1 IPSec Peers

An endpoint of a communication is defined as peer in a computer network. Each peer offers its services and uses the services of other peers.

A list of all configured IPSec Peers is displayed in the **VPN**->**IPSec**->**IPSec Peers** menu.

Peer Monitoring

The menu for monitoring a peer is called by selecting the 🔍 button for the peer in the peer list.

11.6.1.1.1 New

Choose the **New** button to set up more IPSec peers.

The menu **VPN**->**IPSec**->**IPSec Peers**->**New** consists of the following fields:

Fields in the menu Peer Parameters

Field	Description
Administrative Status	Select the status to which you wish to set the peer after saving the peer configuration. Possible values: • *Up* (default value): The peer is available for setting up a tunnel immediately after saving the configuration. • *Down*: The peer is initially not available after the configuration has been saved.
Description	Enter a description of the peer that identifies it. The maximum length of the entry is 255 characters.
Peer Address	Select the **IP Version**. You can choose if IPv4 or IPv6 is to be preferred or if only one IP version is to be permitted. **Note** This selection is only relevant if an IP address is entered as host name. Possible values: • *IPv4 Preferred* • *IPv6 Preferred* • *IPv4 Only*

Field	Description
	• *IPv6 Only* Enter the public IP address of the peer or a resolvable host name. This entry can be omitted in certain configurations, but in that case your device cannot initiate an IPSec connection.
Peer ID	Select the ID type and enter the peer ID. This entry is not necessary in certain configurations. The maximum length of the entry is 255 characters. Possible ID types: • *Fully Qualified Domain Name (FQDN)*: Any string • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *Key ID*: Any string On the peer device, this ID corresponds to the **Local ID Value**.
Internet Key Exchange	Select the version of the Internet Exchange Protocol to be used. Possible values: • *IKEv1* (default value): Internet Key Exchange Protocol Version 1 • *IKEv2*: Internet Kex Exchange Protocol Version 2
Authentication Method	Only for **Internet Key Exchange** = *IKEv2* Select the authentication method. Possible values: • *Preshared Keys* (default value): If you do not use certificates for the authentication, you can select Preshared Keys. These are configured during peer configuration in the **IPSec Peers**. The preshared key is the shared password. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm.
Local ID Type	Only for **Internet Key Exchange** = *IKEv2* Select the local ID type. Possible ID types: • *Fully Qualified Domain Name (FQDN)* • *E-mail Address* • *IPV4 Address* • *ASN.1-DN (Distinguished Name)* • *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.

Field	Description
	When you enable the option **Use Subject Name from certificate**, the subject name indicated in the certificate is used.
Preshared Key	Enter the password agreed with the peer. The maximum length of the entry is 50 characters. All characters are possible except for *0x* at the start of the entry.
IP Version of the tunneled Networks	Select if IPv4, IPv6 or both versions are allowed for the VPN tunnel. Possible values: • *IPv4* • *IPv6* • *IPv4 and IPv6*

Fields in the menu IPv4 Interface Routes

Field	Description
Security Policy	Select the security settings to be used with the interface. Possible values: • *Trusted* : All IP packets are allowed through except for those which are explicitly prohibited. • *Untrusted* (default value): Only those packets are transmitted that can be attributed to a connection that has been initiated from a trusted zone. You can configure exceptions for the selected setting in the *Firewall* on page 318 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.

Field	Description
Default Route	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Client* Select whether the route to this IPSec peer is to be defined as the default route. The function is enabled with *Enabled*. The function is disabled by default.
Local IP Address	Only for **IP Address Assignment** = *Static* or *IKE Config Mode Server* Enter the WAN IP address of your IPSec tunnel. This can be the 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 318 menu.

Field	Description
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

be.IP 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 doe simplify many configurations, problems may also be caused by competing routes or the "coarser" filtering of data traffic.

The **Additional Traffic Filter** parameter fixes this problem. You can apply a "finer" filter, i.e. you can enter the source IP address or the source port.

If an IP packet does not match the defined **Additional Traffic Filter** , it is rejected. If an IP packet meets the requirements in an **Additional Traffic Filter** , IPSec phase 2 negotiation begins and data traffic is transferred over the tunnel.

Note

The parameter **Additional Traffic Filter** is exclusively relevant for the initiator of the IPSec connection, it is only used for outgoing traffic.

Note

Please note that the phase 2 policies must match on both of the IPSec tunnel endpoints.

Add new entries with **Add**.

Fields in the Basic Parameters menu

Field	Description
Description	Enter a description for the filter.
Protocol	Select a protocol. The *Any* option (default value) matches any protocol.
Source IP Address/Netmask	Enter, if required, the source IP address and netmask of the data packets. Possible values: • *Any* • *Host*: Enter the IP address of the host. • *Network* (default value): Enter the network address and the related

Field	Description
	netmask.
Source Port	Only for **Protocol** = *TCP* or *UDP* Enter the source port of the data packets. The default setting *-All-* 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-* means that the port is not specified.

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

Fields in the Advanced IPSec Options menu

Field	Description
Phase-1 Profile	Select a profile for Phase 1. Besides user-defined profiles, predefined profiles are available. Possible values: • *None (use default profile)*: Uses the profile marked as standard in **Phase-1 Profiles** • **PSK Multiproposal*: 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 **Phase-1 Profiles**. • *<Profilname>*: Uses a profile configured in menu **Phase-1 Profiles** for Phase 1.
Phase-2 Profile	Select a profile for Phase 2. Besides user-defined profiles, predefined profiles are available. Possible values: • *None (use default profile)*: Uses the profile marked as standard in **Phase-2 Profiles** • *Multi-Proposal*: Uses a special profile which contains the proposals for Phase 2 3DES/MD5, AES-128/MD5 and Blowfish/MD5 regardless of the proposal selection in menu **Phase-2 Profiles**. • *<Profilname>*: Uses a profile configured in menu **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.

Field	Description
	The configuration of the dynamic peer must not have a Peer ID or a Per IP Address. Clients connecting to the gateway, however, must have a **Local ID** configured, since this ID is used to distinguish the IPSec tunnels created by dynamic peers. Find information on how to configure this ID type for your IPSec client in its respective documentation. The resulting peer would not apply to all incoming tunnel requests and needs to be moved to the end of the IPSec peer list. Otherwise, all subsequent peers in the list would inactive.
Start Mode	Select how the peer is to be switched to the active state. Possible values: • *On Demand* (default value): The peer is switched to the active state by a trigger. • *Always up*: The peer is always active.
Backup Peer	Only for peers using IKEv2. If a peer has been configured for the **Start Mode** *Always up*, you can select another, already configured peer as a backup option. If the current peer becomes inactive, e.g. because of an outage of the central VPN dial-in node, the backup peer can initiate a connection to a backup VPN dial-in node. If the primary dial-in node becomes available again, the connection is seamlessly switched back. This solution requires that the routing for the peers has to be configured in a way that a connection to the remote site is actually possible via either of them. Moreover, the routing metric for the backup peer should be lesser than for the primary peer. This ensures that the tunnel is switched back to the primary peer as soon as its connection is available again.
Delay until returning to primary peer	If in a fallback case the primary peer is coming up again, it may be desirable to delay the use of the primary peer and thus the reset of the secondary peer. This option defines the intended delay time.

Fields in the menu Advanced IP Options

Field	Description
Public Interface	Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select *Choosen by Routing*, the decision as to via which interface the data traffic is routed is made based on the current routing table. If you select an interface, the interface is used taking into consideration the setting under **Public Interface Mode**.
Public Interface Mode	Only when under **Public Interface** an interface is selected. Specify how strictly the setting is handled. Possible values: • *Force*: Only the selected interface is used, whatever 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 ad-

Field	Description
	dress for the peer's data traffic. Select whether the **Public Source IPv4 Address** is to be enabled. The function is enabled with *Enabled*. In the input field, enter the public IP address that is to be used as the sender address. The function is disabled by default.
Public Source IPv6 Address	Public Source IPv6 Address The function is enabled with *Enabled*. In the input field, enter the public IP address that is to be used as the sender address. The function is disabled by default.
IPv4 Back Route Verify	Select whether a check on the back route should be activated for the interface to the connection partner. The function is enabled with *Enabled*. The function is disabled by default.
MobIKE	Only for peers with IKEv2. **MobIKE** In cases of changing public IP addresses, enables only these addresses to be updated in the SAs without the SAs themselves having to be renegotiated. The function is enabled by default. Note that MobIKE requires a current IPSec client, e. g. the current Windows 7 or Windows 8 client or the latest version of the bintec elmeg IPSec client.
IPv4 Proxy ARP	Select whether your device is to respond to ARP requests from its own LAN on behalf of the specific connection partner. Possible values: • *Inactive* (default value): Deactivates Proxy ARP for this IPSec peer. • *Up or Dormant*: Your device only responds to an ARP request if the status of the connection to the IPSec peer is *Up* (active) or *Dormant* (dormant). In the case of *Dormant*, your device only responds to the ARP request; the connection is not set up until someone actually wants to use the route. • *Up only*: Your device responds to an ARP request only if the status of the connection to the IPSec peer is *Up* (active), i.e. a connection already exists to the IPSec peer.
CA Certificates	Only available if certificates are in use on the device. If you enable the **Trust the following CA certificates** option, you can select CA certificates that are accepted for this profile. This option can only be configured if certificates are loaded.

IPSec Callback

bintec elmeg devices support the DynDNS service to enable hosts without fixed IP addresses to obtain a secure connection over the Internet. This service enables a peer to be identified using a host name that can be resolved by DNS. You do not need to configure the IP address of the peer.

The DynDNS service does not signal whether a peer is actually online and cannot cause a peer to set up an Internet connection to enable an IPSec tunnel over the Internet. This possibility is created with IPSec callback: Using a direct ISDN call to a peer, you can signal that you are online and waiting for the peer to set up an IPSec tunnel over the Internet. If the called peer currently has no connection to the Internet, the ISDN call causes a connection to be set up. This ISDN call costs nothing (depending on country), as it does not have to be accepted by your device. The identification of the caller from his or her ISDN number is enough information to initiate setting up a tunnel.

To set up this service, you must first configure a call number for IPSec callback on the passive side in the **Physical Interfaces**->**ISDN Ports**->**MSN Configuration**->**New** menu. The value *IPSec* is available for this purpose in the field **Service**. This entry ensures that incoming calls for this number are routed to the IPSec service.

If callback is active, the peer is caused to initiate setting up an IPSec tunnel by an ISDN call as soon as this tunnel is required. If callback is set to passive, setting up a tunnel to the peer is always initiated if an ISDN call is received on the relevant number (**MSN** in menu **Physical Interfaces**->**ISDN Ports**->**MSN Configuration**->**New** for **Service** *IPSec*). This ensures that both peers are reachable and that the connection can be set up over the Internet. The only case in which callback is not executed is if SAs (Security Associations) already exist, i.e. the tunnel to the peer already exists.

Note

If a tunnel is to be set up to a peer, the interface over which the tunnel is to be implemented is activated first by the IPSec Daemon. If IPSec with DynDNS is configured on the local device, the own IP address is propagated first and then the ISDN call is sent to the remote device. This ensures that the remote device can actually reach the local device if it initiates the tunnel setup.

Transfer of IP Address over ISDN

Transferring the IP address of a device over ISDN (in the D channel and/or B channel) opens up new possibilities for the configuration of IPSec VPNs. This enables restrictions that occur in IPSec configuration with dynamic IP addresses to be avoided.

Note

To be able to use IP address transmission via ISDN, you will need a free additional license.

You can obtain this license from your sales partner or from our support.

Before System Software Release 7.1.4, IPSec ISDN callback only supported tunnel setup if the current IP address of the initiator could be determined by indirect means (e.g. via DynDNS). However, DynDNS has serious disadvantages, such as the latency until the IP address is actually updated in the database. This can mean that the IP address propagated via DynDNS is not correct. This problem is avoided by transferring the IP address over ISDN. This type of transfer of dynamic IP addresses also enables the more secure ID Protect mode (main mode) to be used for tunnel setup.

Method of operation: Various modes are available for transferring your own IP address to the peer: The address can be transferred free in the D channel or in the B channel, but here the call must be accepted by the remote station and therefore incurs costs. If a peer whose IP address has been assigned dynamically wants to arrange for another peer to set up an IPSec tunnel, it can transfer its own IP address as per the settings described in *Fields in the menu IPv4 IPSec Callback* on page 304. 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).

Field	Description
Incoming Phone Number	Only for **Mode** = *Passive* or *Both* Enter the ISDN number from which the remote device calls the local device (calling party number). Wildcards may also be used.
Outgoing Phone Number	Only for **Mode** = *Active* or *Both* Enter the ISDN number with which the local device calls the remote device calls (called party number). Wildcards may also be used.
Transfer own IP address over ISDN/GSM	Select whether the IP address of your own device is to be transferred over ISDN for IPSec callback. The function is enabled with *Enabled*. The function is disabled by default.
Transfer Mode	Only for **Transfer own IP address over ISDN/GSM** = enabled Select the mode in which your device is to attempt to transfer its IP address to the peer. Possible values: • *Autodetect best mode*: Your device automatically determines the most favourable mode. It first tries all D channel modes before switching to the B channel. (Costs are incurred for using the B channel.) • *Autodetect only D Channel Modes*: Your device automatically determines the most favourable D channel mode. The use of the B channel is excluded. • *Use specific D Channel Mode*: Your device tries to transfer the IP address in the mode set in the **Mode** field. • *Try specific D Channel Mode, fall back to B Channel*: Your device tries to transfer the IP address in the 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".

11.6.1.2 Phase-1 Profiles

In the **VPN**->**IPSec**->**Phase-1 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.

11.6.1.2.1 New

Choose the **New** button with **Create new IKEv1 Profile** to create additional profiles.

The menu **VPN**->**IPSec**->**Phase-1 Profiles**->**New** consists of the following fields:

Fields in the Phase-1 (IKE) Parameters menu

Field	Description
Description	Enter a description that uniquely defines the type of rule.
Proposals	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 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

Field	Description
	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	Only for **Phase-1 (IKE) Parameters** The Diffie-Hellman group defines the parameter set used as the basis for the key calculation during phase 1. "MODP" as supported by **be.IP** devices stands for "modular exponentiation". Possible values: • *1(768 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 768bits is used to create the encryption material. • *2(1024 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • *5(1536 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
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 **IPSec Peers**. The preshared key is the shared password. • *DSA Signature*: Phase 1 key calculations are authenticated using the DSA algorithm. • *RSA Signature*: Phase 1 key calculations are authenticated using the RSA algorithm. • *RSA Encryption*: In RSA encryption the ID payload is also encrypted for additional security.
Local Certificate	Only for **Phase-1 (IKE) Parameters** Only for **Authentication Method** = *DSA Signature* , *RSA Signature* or *RSA Encryption* This field enables you to select one of your own certificates for authentic-

Field	Description
	ation. 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 for configuring 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)*
Local ID Value	Only for **Phase-1 (IKE) Parameters** Enter the ID of your device. For **Authentication Method** = *DSA Signature* or *RSA Signature* the option **Use Subject Name from certificate** is displayed. When you enable the option **Use Subject Name from certificate**, the subject name indicated in the certificate is used.

Alive Check

During communication between two IPSec peers, one of the peers may become unavailable, e.g. due to routing problems or a reboot. However, this can only be detected when the end of the lifetime of the security connection is reached. Up until this point the data packets are lost. These are various methods of performing an alive check to prevent this happening. In the **Alive Check** field you can specify whether a method should be used to check the availability of a peer.

Two methods are available: Heartbeats and Dead Peer Detection.

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

Fields in the Advanced Settings menu

Field	Description
Alive Check	Only for **Phase-1 (IKE) Parameters** Select the method to be used to check the functionality of the IPSec con-

Field	Description
	nection. In addition to the default method Dead Peer Detection (DPD), the (proprietary) Heartbeat method is implemented. This sends and receives signals every 5 seconds, depending on the configuration. If these signals are not received after 20 seconds, the SA is discarded as invalid. Possible values: • *Autodetect* (default value): Your device detects and uses the mode supported by the remote terminal. • *Inactive*: Your device sends and expects no heartbeat. Set this option if you use devices from other manufacturers. • *Heartbeats (Expect only)*: Your device expects a heartbeat from the peer but does not send one itself. • *Send*: 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. **Note** As the two methods of accessibility testing use different procedures, it is not recommended to use them in combination in Phase 1 and Phase 2. In Phase 2 only heartbeats are supported, so they should be deactivated if Dead Peer Detection is required in Phase 1. Only for **Phase-1 (IKEv2) Parameters** Enable or disable alive check. The function is enabled by default.
Block Time	Define how long a peer is blocked for tunnel setups after a phase 1 tunnel setup has failed. This only affects locally initiated setup attempts. Possible values are *-1* to *86400* (seconds); *-1* means the value in the default profile is used and *0* means that the peer is never blocked. The default value is *30*. If a peer has been configured in "always up" mode, there is an implicit minimum block time of 15 seconds which is applied 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 tun-

Field	Description
	nel 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. 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. 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 CA certificates that are accepted for this profile. This option can only be configured if certificates are loaded.

11.6.1.3 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.

11.6.1.3.1 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

Field	Description
	and general speed. Here, it is used with a key length of 128 bits. • *AES-192*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 192 bits. • *AES-256*: Rijndael has been nominated as AES due to its fast key setup, low memory requirements, high level of security against attacks and general speed. Here, it is used with a key length of 256 bits. • *Twofish*: Twofish was a final candidate for the AES (Advanced Encryption Standard). It is rated as just as secure as Rijndael (AES), but is slower. • *Blowfish*: Blowfish is a very secure and fast algorithm. Twofish can be regarded as the successor to Blowfish. • *CAST*: CAST is also a very secure algorithm, marginally slower than Blowfish, but faster than 3DES. • *DES*: DES is an older encryption algorithm, which is rated as weak due to its small effective length of 56 bits. 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 activate PFS (*Enabled*) , the options are the same as for the configuration in **Phase-1 Profiles**, **DH Group**. PFS is used to protect the keys of a renewed phase 2 SA, even if the keys of the phase 1 SA have become known. The field has the following options: • *1(768 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 768bits is used to create the encryption material. • *2(1024 Bit)* (default value): During the Diffie-Hellman key calculation, modular exponentiation at 1024 bits is used to create the encryption material. • *5(1536 Bit)*: During the Diffie-Hellman key calculation, modular exponentiation at 1536 bits is used to create the encryption material.
Lifetime	Define how the lifetime is defined that will expire before phase 2 SAs need to be renewed.

Field	Description
	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 **be.IP** 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 **be.IP** device. If it is, *Heartbeats (Send &Expect)* (for a remote terminal with **be.IP**) or *Inactive* (for a remote terminal without **be.IP**) 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.

Field	Description
	Note In Phase 1 and Phase 2, your device supports different methods of accessibility testing: In Phase 1, dead peer detection and heartbeats, in Phase 2 only heartbeats. Since the two methods of accessibility testing use different procedures, it is not recommended to combine them in Phase 1 and Phase 2. Heartbeats should therefore be deactivated in Phase 2 if Dead Peer Detection is required in Phase 1.
Propagate PMTU	Select whether the PMTU (Path Maximum Transfer Unit) is to be propagated during phase 2. The function is enabled with *Enabled*. The function is enabled by default.

11.6.1.4 XAUTH Profiles

In the **XAUTH Profiles** menu a list of all XAUTH profiles is displayed.

Extended Authentication for IPSec (XAuth) is an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or as a client:

- As a server the gateway requires a proof of authorisation.
- As a client the gateway provides proof of authorisation.

In server mode, multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Multiple users can dial-in either one after another or simultaneously via a so-called multi peer. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server.

If a company's headquarters is connected to several branches via IPSec, several peers can be configured, for example, one peer for each branch. A password is assigned to each peer, i.e. each branch. Besides this authentication method per branch, XAuth offers an additional method for logging in individually and independently from a user's location via a private password. A specific user can then use the IPSec tunnel across various peers. This is useful, for example, if an employee works alternately in different branches and if he needs to have individual access to the tunnel.

All users are assigned the same password in a so-called multi peer, i.e. a group password. Here, XAuth offers an individual authentication method to the user, too. If in a branch, for example, multiple users have access to a tunnel via a multi peer, it may have an adventage for users with different tasks that each of them uses a private password.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

11.6.1.4.1 New

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

The **VPN**->**IPSec**->**XAUTH Profiles**->**New** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Description	Enter a description for this XAuth profile. You can create up to 10 XAuth profiles with **Role** = *Server* and **Mode** = *Local* or **Role** = *Client* settings (see below).
Role	Select the role of the gateway for XAuth authentication. Possible values: • *Server* (default value): The gateway requires a proof of authorisation. • *Client*: The gateway provides proof of authorisation.
Mode	Only for **Role** = *Server* Select how authentication is carried out. Possible values: • *RADIUS* (default value): Authentication is carried out via a Radius server. It is configured in the **System Management**->**Remote Authentication**->**RADIUS** menu and selected in the **RADIUS Server Group ID** field. • *Local*: Authentication is carried out via a local list.
Name	Only for **Role** = *Client* Enter the authentication name of the client.
Password	Only for **Role** = *Client* Enter the authentication password.
RADIUS Server Group ID	Only for **Role** = *Server* Select the desired list in **System Management**->**Remote Authentication**->**RADIUS** configured RADIUS group.
Users	Only for **Role** = *Server* and **Mode** = *Local* If your gateway is configured as an XAuth server, the clients can be authenticated via a locally configured user list. Define the members of the user group of this XAUTH profile here by entering the authentication name of the client (**Name**) and the authentication password (**Password**). Add new members with **Add**. There is no limitation for users per XAuth profile.

11.6.1.5 IP Pools

Note

Note that the menu **IP Pools** is only available if a port in the menu **Physical interfaces**->**ISDN ports**-> **ISDN configuration** is set to external operation (TE mode). An adapter must be connected for this (which is available as an accessory).

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.

11.6.1.5.1 Edit or New

Choose the **Add** button to set up new IP pools. Select the ✎ icon to edit existing entries.

The **VPN**->**IPSec**->**IP Pools**->**Add** menu consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
IP Pool Name	Enter the name of the IP pool.
IP Address Range	In the first field, enter the first IP address of the range. In the second field, enter the last IP address of the range.
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.

11.6.1.6 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** is not activated.
IPSec Debug Level	Select the priority of the syslog messages of the IPSec subsystem to be recorded internally. Possible values: • *Emergency* (highest priority) • *Alert* • *Critical* • *Error* • *Warning* • *Notice* • *Information* • *Debug* (default value, lowest priority) Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level *Debug*.

The **Advanced Settings** menu is for adapting certain functions and features to the special requirements of your environment, i.e. mostly interoperability flags are set. The default values are globally valid and enable your system to work correctly to other **be.IP** devices, so that you only need to change these values if the remote terminal is a third-party product or you know special settings are necessary. These may be needed, for example, if the remote end operates with older IPSec implementations.

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

Fields in the Advanced Settings menu

Field	Description
IPSec over TCP	Determine whether IPSec over TCP is to be used. IPSec over TCP is based on NCP pathfinder technology. This technology insures that data traffic (IKE, ESP, AH) between peers is integrated into a pseudo HTTPS session. The function is enabled with *Enabled*. The function is disabled by default.
Send Initial Contact Message	Select whether IKE Initial Contact messages are to be sent during IKE (phase 1) if no SAs with a peer exist. The function is enabled with *Enabled*. The function is enabled by default.
Sync SAs with ISP interface state	Select whether all SAs are to be deleted whose data traffic was routed via an interface on which the status has changed from *Up* to *Down*, *Dormant* or *Blocked*. The function is enabled with *Enabled*. The function is disabled by default.
Use Zero Cookies	Select whether zeroed ISAKMP Cookies are to be sent. These are equivalent to the SPI (Security Parameter Index) in IKE proposals; as they are redundant, they are normally set to the value of the negotiation currently in progress. Alternatively, your device can use zeroes for all values of the cookie. In this case, select *Enabled*.
Zero Cookie Size	Only for **Use Zero Cookies** = enabled. Enter the length in bytes of the zeroed SPI used in IKE proposals. The default value is *32*.
Dynamic RADIUS Authentication	Select whether RADIUS authentication is to be activated via IPSec. The function is enabled with *Enabled*. 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.

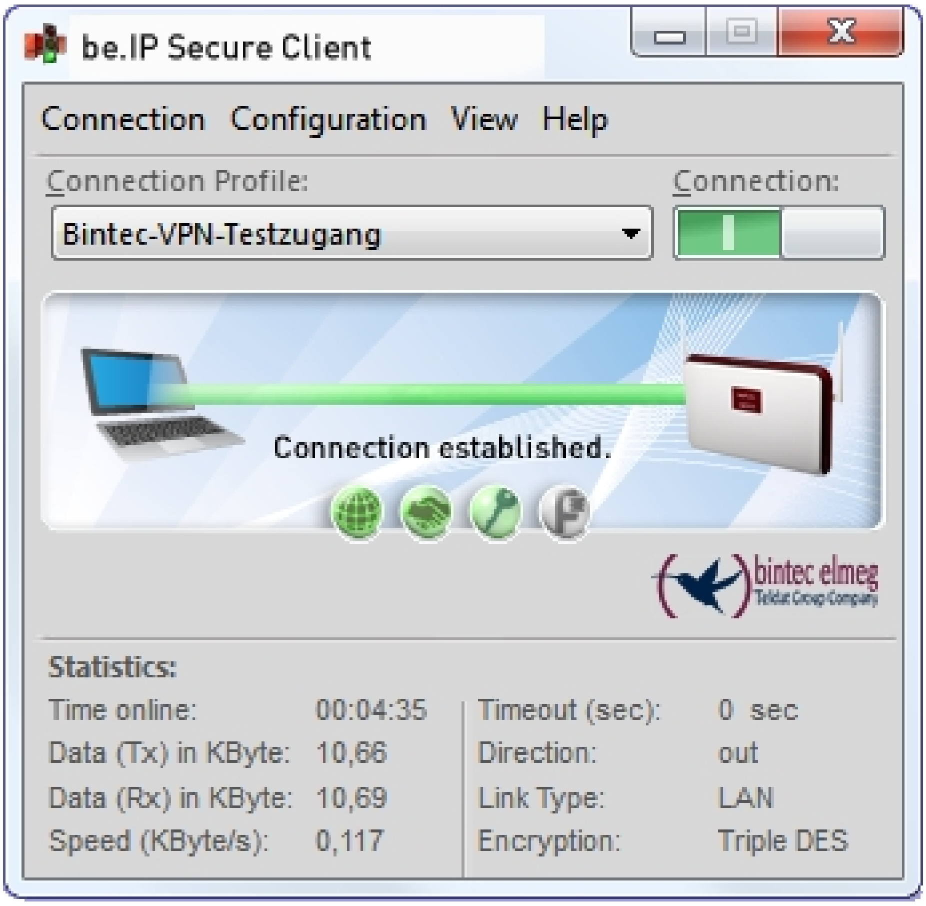
Field	Description
Send Certificate Request Payloads	Select whether certificate requests are to be sent during IKE (phase 1). The function is enabled with *Enabled*. The function is enabled by default.
Send Certificate Chains	Select whether complete certificate chains are to be sent during IKE (phase 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.

11.6.2 be.IP Secure Client

Here you can download the current Secure IPsec Client software for free.

⚠ **Important**

Note that the client is only available for Windows!



Connection Profile: Bintec-VPN-Testzugang

Connection:

Statistics:

Time online:	00:04:35	Timeout (sec):	0 sec
Data (Tx) in KByte:	10,66	Direction:	out
Data (Rx) in KByte:	10,69	Link Type:	LAN
Speed (KByte/s):	0,117	Encryption:	Triple DES

11.7 Firewall

The Stateful Inspection Firewall (SIF) provided for **be.IP** 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

be.IP's Stateful Inspection Firewall fits into the existing security architecture of **be.IP** device very well due to its simple configuration. 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 rejected without sending an error message to the sender of the packet; if a reject rule matches, the packet is rejected 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).

11.7.1 Policies

11.7.1.1 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 the infrastructure is made up of trustworthy and non-trustworthy areas. Both security policies *Trusted* and *Untrusted* describe this assumption. These define the two 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 now define additional filter rules, to discard certain packets. In the same way you can release selected data packets for the

Untrusted setting.

A list of all configured IPv4 filter rules is displayed in the **Firewall**->**Policies**->**IPv4 Filter Rules** menu.

You can use the ✎ button in row **Trusted Interfaces** to define which interfaces are **Trusted**. This opens a new window containing a list of interfaces. You can mark the individual interfaces as trustworthy.

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.

11.7.1.1.1 New

Note

Informationen on the selection of Trusted Interfaces can be found here: *IPv4 Filter Rules* on page 319.

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.

11.7.1.2 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 the infrastructure is made up of trustworthy and non-trustworthy areas. Both security policies *Trusted* and *Untrusted* describe this assumption. These define the two 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 now define additional filter rules, to discard certain packets. In the same way you can release selected data packets for the *Untrusted* setting.

Data packets which use Neighbour Discovery Protocol are allowed in principle, even for the *Untrusted* filter rule.

A list of all configured IPv6 filter rules is displayed in the **Firewall**->**Policies**->**IPv6 Filter Rules** menu.

You can use the ✎ button in row **Trusted Interfaces** to define which interfaces are **Trusted**. This opens a new window containing a list of interfaces. You can mark the individual interfaces as trustworthy.

Note

Note that the interface list for IPv6 is empty until an interface has been enabled for IPv6.

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.

11.7.1.2.1 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**), addresses (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**), addresses (see **Firewall**->**Addresses**->**Address List**) and address groups (see **Firewall**->**Addresses**->**Groups**) are available for selection for IPv6.
Service	Select one of the preconfigured services to which the packet to be filtered must be assigned. The extensive range of services configured ex works includes the following: • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* Additional services are created in **Firewall**->**Services**->**Service List**. 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.

11.7.1.3 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*

Field	Description
	The function is enabled by default.
Logged Actions	Select the firewall syslog level. The messages are output together with messages from other subsystems. Possible values: • *All* (default value): All firewall activities are displayed. • *Deny*: Only reject and deny events are shown, see "Action". • *Accept*: Only accept events are shown. • *None*: Syslog messages are not generated.
IPv4 Full Filtering	With TCP sessions, the SIF first verifies if a session has been established completely and correctly. Incomplete sessions will be blocked. The filtering itself is carried out in a second step. The default setting **IPv4 Full Filtering** has been designed to meet this "standard" case. If - in a two-way communication - one traffic direction is sent through the router, but the counter direction takes a different route, the session is interpreted as "incomplete" by the SIF, and the data traffic of this connection will be blocked by the router. In order to allow the data traffic of such "incomplete" sessions in the special case of identical source and destination interface you have to disable **IPv4 Full Filtering**. SIF rules for this data traffic will be ignored.
STUN Handler	Enable this option if you intend to allow network devices (esp. SIP clients) to use STUN in order to identify the network address translation mode and the public IP address. The firewall creates temporary rules that allow RTP data traffic for SIP phone calls.
Port STUN server	Only for **STUN Handler**= Enabled Enter the number of the port to be used for the connection to the STUN server. The default value is 3478. A 5 digit sequence isd possible.

Fields in the Session Timer menu

Field	Description
UDP Inactivity	Enter the inactivity time after which a UDP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. The default value is *180*.
TCP Inactivity	Enter the inactivity time after which a TCP session is to be regarded as expired (in seconds). Possible values are *30* to *86400*. 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*.

Field	Description
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.

11.7.2 Interfaces

11.7.2.1 IPv4 Groups

A list of all configured 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.

11.7.2.1.1 New

Choose the **New** button to set up new 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 interface group.
Members	Select the members of the group from the available interfaces. To do this, activate the field in the **Members** column.

11.7.2.2 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.

11.7.2.2.1 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.

11.7.3 Addresses

11.7.3.1 Address List

A list of all configured addresses is displayed in the **Firewall**->**Addresses**->**Address List** menu.

11.7.3.1.1 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 fpr **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*.
Address Range	Only for **IPv4** = *Enabled* and **Address Type** = *Address Range* Enter the first and the last IP address of the range.
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.

11.7.3.2 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.

11.7.3.2.1 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 field in the **Selection** column.

11.7.4 Services

11.7.4.1 Service List

In the **Firewall**->**Services**->**Service List** menu, a list of all available services is displayed.

11.7.4.1.1 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.

Field	Description
	Possible values are *1* to *65535*.
Type	Only for **Protocol** = *ICMP* The **Type** field shows the class of ICMP messages, the **Code** field specifies the type of message in greater detail. Possible values: • *Any* (default value) • *Echo reply* • *Destination unreachable* • *Source quench* • *Redirect* • *Echo* • *Time Exceeded* • *Parameter Problem* • *Timestamp* • *Timestamp reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	Only for **Protocol** = *ICMP* and for **Type** = *Destination unreachable* are selection options available for the ICMP code. 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*

11.7.4.2 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.

11.7.4.2.1 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 field in the **Members** column.

11.8 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)

11.8.1 DNS

Each device in a TCP/IP network is usually located by its IP address. Because host names are often used in networks to reach different devices, it is necessary for the associated IP address to be known. This task can be performed by a DNS server, which resolves the host names into IP addresses. Alternatively, name resolution can also take place over the HOSTS file, which is available on all PCs.

Your device offers the following options for name resolution:

- DNS Proxy, for forwarding DNS requests sent to your device to a suitable DNS server. This also includes specific forwarding of defined domains (Forwarded Domains).
- DNS cache, for saving the positive and negative results of DNS requests.
- Static entries (static hosts), to manually define or prevent assignments of IP addresses to names.
- DNS monitoring (statistics), to provide an overview of DNS requests on your device.

Name server

Under **Local Services**->**DNS**->**DNS Servers**->**New** you enter the IP addresses of name servers that are queried if your device cannot answer requests itself or by forwarding entries. Global name servers and name servers that are attached to an interface can both be entered.

Your device can also receive the name servers attached to an interface dynamically via PPP or DHCP and transfer them dynamically if necessary.

Strategy for name resolution on your device

A DNS request is handled by your device as follows:

(1) If possible, the request is answered directly from the static or dynamic cache with IP address or negative response.

(2) Otherwise, if a suitable forwarding entry exists, the relevant DNS server is asked, depending on the configuration of the Internet or dialin connections, if necessary by setting up a WAN connection at extra cost. If the DNS server can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(3) Otherwise, if name servers have been entered, taking into account the priority configured and if the relevant interface status is "up", the primary DNS server is queried and then the secondary DNS server. If one of the DNS servers can resolve the name, the information is forwarded and a dynamic entry created in the cache.

(4) Otherwise, if a suitable Internet or dialin connection is selected as the standard interface, the relev-

ant 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, they 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.

11.8.1.1 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.

11.8.1.2 DNS Servers

A list of all configured DNS servers is displayed in the **Local Services**->**DNS**->**DNS Servers** menu.

11.8.1.2.1 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*.

Field	Description
	The function is enabled by default.
Description	Enter a description for DNS server.
Priority	Assign a priority to the DNS server. You can assign more than one pair of DNS servers (**Primary DNS Server** and **Secondary DNS Server**) to an interface (i. e. for example, to an Ethernet port or a PPPoE WAN partner) or to multiple interfaces. The pair with the highest priority is used if the interface is "up". Possible values from *0* (highest priority) to *9* (lowest priority). The default value is *5*.
Interface Mode	Select whether the IP addresses of name servers for resolving the names of Internet addresses are to be obtained automatically or whether up to two fixed DNS server addresses are to be entered, depending on the priority. Possible values: • *Static* • *Dynamic* (default value)
Interface	Select the interface to which the DNS server pair is to be assigned. The selected interface is relevant for outgoing DNS requests. This interface is used for DNS requests directed at the router or generated by the router itself. For **Interface Mode** = *Static* A DNS server is configured for all interfaces with the *Any* setting.
IP Version	Select the IP version used. Possible values: • *IPv4* • *IPv6* *IPv4* is selected by default.
Primary IPv4 DNS Server	Only if **Interface Mode** = *Static* Enter the IPv4 address of the first name server for Internet address name resolution.
Secondary IPv4 DNS Server	Only if **Interface Mode** = *Static* Optionally, enter the IPv4 address of an alternative name server.
Primary IPv6 DNS 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* Optionally, enter the IPv6 address of an alternative name server.

11.8.1.3 Static Hosts

A list of all configured static hosts is displayed in the **Local Services**->**DNS**->**Static Hosts** menu.

11.8.1.3.1 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 received to a DNS request. If a negative response is received to 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.
Response	In this entry, select the type of response to DNS requests. Possible values: • *Negative*: A DNS request for **DNS Hostname** gets a negative response. • *Positive* (default value): A DNS request for **DNS Hostname** is answered with the related **IP Address**. • *None*: A DNS request is ignored; no answer is given.
IPv4 Address	Only if **Response** = *Positive* Enter the IPv4 address assigned to **DNS Hostname**.
IPv6 Address	Only if **Response** = *Positive* Enter the IPv6 address assigned to **DNS Hostname**.

11.8.1.4 Domain Forwarding

In the **Local Services**->**DNS**->**Domain Forwarding** menu, a list of all configured forwardings for defined domains is displayed.

11.8.1.4.1 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:

Field	Description
	- *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 the name supplied by the value specified in **Local Services**->**DNS**->**Global Settings** for **Domain Name** as soon as you confirm with **OK**.
Domain	Only for **Forward** = *Domain* Enter the name of the domain for which requests are to be forwarded. The entry can start with the wildcard "*", e.g. "*.bintec-elmeg.com". If you enter a name without a leading wildcard "*" a leading wildcard "*" is supplemented as soon as you confirm with **OK**.
Forward to	Select if matching DNS requests are to be forwarded to the DNS server of an **Interface** or to a manually specified **DNS Server**. Possible values: - *Interface* (default value): Requests are forwarded to the DNS server assigned to either an automatically selected or to a user-selected interface. - *DNS Server*: Requests are forwarded to the specified **DNS Server**.
Destination Interface	Only for **Forward to** = *Interface* Select the interface that has the DNS server assinged which is to receive the DNS requests.
Source Interface	Here you can select the DNS request source interface for domain forwarding. This option is available for forwarding to an interface as well as to specific DNS servers. It allows you to send DNS requests from different network segments to different DNS servers. For example, you can forwards the requests from your guest network to a webfilter DNS and deny access to undesired content.
Primary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the primary DNS server.
Secondary DNS Server (IPv4/IPv6)	Only for **Forward to** = *DNS Server* Enter the IPv4/IPv6 address of the secondary DNS server.

11.8.1.5 Dynamic Hosts

In the menu **Local Services**->**DNS**->**Dynamic Hosts**, you can find relevant information on dynamic DNS entries.

11.8.1.6 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**

. This entry then disappears from the list and is thus included in the list in the **Static Hosts** menu. The TTL is transferred in this operation.

11.8.1.7 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** per **DNS Requests** 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).

11.8.2 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.

11.8.2.1 HTTPS Server

In the **Local Services**->**HTTPS**->**HTTPS Server** menu, configure the parameters of the backed up configuration connection via HTTPS.

The menu consists of the following fields:

Fields in the HTTPS Parameters menu

Field	Description
HTTPS TCP Port	Enter the port via which the HTTPS connection is to be established. Possible values are *0* to *65535*. The default value is *443*.
Local Certificate	Select a certificate that you want to use for the HTTPS connection. Possible values: • *Internal* (default value): Select this option if you want to use the certificate built into the device.

Field	Description
	• *<Certificate name>*: Under **System Management**->**Certificates**->**Certificate List** entered certificate.

11.8.3 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.

11.8.3.1 DynDNS Update

In the **Local Services**->**DynDNS Client**->**DynDNS Update** menu, a list of all configured DynDNS registrations for updating is displayed

11.8.3.1.1 New

Choose the **New** button to set up further DynDNS registrations to be updated.

The menu **Local Services**->**DynDNS Client**->**DynDNS Update**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Host Name	Enter the complete host name exactly as registered with the DynDNS provider.
Interface	Select the WAN interface the IP address of which is to be propagated over the DynDNS service (e.g. the interface of the Internet Service Provider).
User Name	Enter the user name as registered with the DynDNS provider.
Password	Enter the password as registered with the DynDNS provider.
Provider	Select the DynDNS provider with which the specified data are registered. A choice of DynDNS providers is already available. and the protocols they use are supported. Other DynDNS providers can be configured in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu. The default value is *DynDNS*.
Enable update	Select whether the DynDNS entry configured here is to be activated and

Field	Description
	the current IP address of the selected interface is to be sent to the provider . The function is activated by selecting *Enabled*. The function is disabled by default.
HTTPS/SSL	This option is only available if the selected DynDNS provider supports SSL. If required, you can create a new provider supporting this option in the menu **Local Services**->**DynDNS Client**->**DynDNS Provider**. Enable this option in order to create an SSL-encrypted connection between your device and your DynDNS provider. Choosing *Enabled* activates the option. It is not enabled per default.
Certificate checking	Enable this fucntion in order verify the SSL certificate of the sever.
IP Version	This option is only available if your selected DynDNS provider provides server addresses for both IP versions. Select the IP version of the address you intend to update with your DynDNS provider. Possible values: IPv4 IPv6. In order to update the IPv4 as well as the Pv6 address of an interface, create two entries with otherwise identical settings. Inquire with your service provider if they support multiple updates!

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

Fields in the Advanced Settings menu.

Field	Description
Mail Exchanger (MX)	Enter the full host name of a mail server to which e-mails are to be forwarded if the host currently configured is not to receive mail. Ask your provider about this forwarding service and make sure e-mails can be received from the host entered as MX.
Wildcard	Select whether forwarding of all subdomains of the **Host Name** is to be enabled for the current IP address of the **Interface** (advanced name resolution). The function is activated by selecting *Enabled*. The function is disabled by default.

11.8.3.2 DynDNS Provider

A list of all configured DynDNS providers is displayed in the **Local Services**->**DynDNS Client**->**DynDNS Provider** menu.

11.8.3.2.1 New

Choose the **New** button to set up new DynDNS providers.

The menu **Local Services**->**DynDNS Client**->**DynDNS Provider**->**New** consists of the following fields:

Fields in the Basic Parameters menu.

Field	Description
Provider Name	Enter a name for this entry.
Server	Enter the host name or IP address of the server on which the provider's DynDNS service runs.
Update Path	Enter the path on the provider's server that contains the script for managing the IP address of your device. Ask your provider for the path to be used.
Port	Enter the port at which your device is to reach your provider's server. Ask your provider for the relevant port. The default value is *80*.
Protocol	Select one of the protocols implemented. Information on which protocol to use can be found in your provider's documentation. Possible values: • *DynDNS* (default value) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS* • *DnsExit* • *dyndnss* • *dyndns2*
Update Interval	Enter the minimum time (in seconds) that your device must wait before it is allowed to propagate its current IP address to the DynDNS provider again. The default value is *300* seconds.
IPv6 server	Specify the host name or IPv6 address of the DynDNS provider if you intend to update an IPv6 address.
Supports SSL	Enable support of SSL for securing data traffic between your device and the DnyDNS provider. The option is disabled per default.
Homepage	Here you can specify a web address that will take you to the page of the provider.

11.8.4 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 (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.

11.8.4.1 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.

11.8.4.1.1 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.

11.8.4.2 DHCP Configuration

To activate your device as a DHCP server, you must first define IP address pools from which the IP addresses are distributed to the requesting clients.

A list of all configured IP address pools is displayed in the **Local Services**->**DHCP Server**->**DHCP Configuration** menu.

In the list, for each entry, you have the possibility under **Status** of enabling or disabling the configured DHCP pools.

Note

In the ex works state the DHCP pool is preconfigured with the IP addresses 192.168.0.10 to 192.168.0.30 and is used if there is no other DHCP server available in the network.

11.8.4.2.1 Edit or New

Choose the **New** button to set up new IP address 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 Address Range** 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	Specify whether the IP pool is used for DHCP requests in the same subnet or for DHCP requests that have been forwarded to your device from another subnet. In this case it is possible to define IP addresses from another network. Possible values: • *`Local`* (default value): The DHCP pool is only used for DHCP requests in the same subnet. • *`Relay`*: The DHCP pool is only used for DHCP requests forwarded from other subnets. • *`Local/Relay`*: The DHCP pool is used for DHCP requests in the same subnet and from other subnets.
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 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.

Field	Description
	• *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*. • *Vendor Group* (Vendor Specific Information): This enables you to send the client any manufacturer-specific information in any text string. Several entries are possible. Add additional entries with the **Add** button.

Vendor Specific Information (DHCP Option 43)

The options for a **Vendor String** or a vendor-specific group of DHCP options (**Vendor Group**) enable you to transmit any manufacturer-specific information or configuration parameters to DHCP clients. You can also define entire groups of DHCP options to be transmitted.

Note

For some products settings have already been predefined in this section. These are required for the seamless integration of telephones or LTE access routers and should not be changed or deleted.

Choose the ✎ icon to edit an existing entry or one of the **Add** buttons to add an entry. In the popup menu, you configure manufacturer-specific settings in the DHCP server for specific telephones, for example.

Fields in the Basic Parameters menu for vendor strings

Field	Description
Select vendor	Here, you can select for which manufacturer specific values shall be transmitted for the DHCP server. Possible values: • *Other* (default value) • *-bintec-*
APN	Only für **Select vendor** = *-bintec-* Enter the Access Point Namen (APN) of the SIM card.
PIN	Only für **Select vendor** = *-bintec-* Enter the PIN of the SIM card.
Vendor Description	Only für **Select vendor** = *Other* Type in the name of the manufacturer for which you want to transfer specific DHCP server settings.
Vendor ID	Only für **Select vendor** = *Other* To identify the device, enter the manufacturer ID.
Vendor Specific Information	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 (code 3)	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.

11.8.4.3 IP/MAC Binding

The **Local Services**->**DHCP Server**->**IP/MAC Binding** menu displays a list of all clients that received an IP address from your device via DHCP.

You can allocate an IP address from a defined IP address pool to specific MAC addresses. You can do this by selecting the **Static Binding** option in the list to convert a list entry as a fixed binding, or you manually create a fixed IP/MAC binding by configuring this in the **New** sub-menu.

Note

You can only create new static IP/MAC bindings if IP address ranges were configured in **Local Services**->**DHCP Server**->**IP Pool Configuration**, and in the **Local Services**->**DHCP Server**->**DHCP Configuration** menu a valid IP Pool is assigned to the DHCP server.

11.8.4.3.1 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.

Field	Description
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.

11.8.4.4 DHCP Relay Settings

If your device for the local network does not distribute any IP addresses to the clients by DHCP, it can still forward the DHCP requests on behalf of the local network to a remote DHCP server. The DHCP server then assigns the your device an IP address from its pool, which in turn sends this to the client in the local network.

The menu **Local Services**->**DHCP Server**->**DHCP Relay Settings** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Primary DHCP Server	Enter the IP address of a server to which BootP or DHCP requests are to be forwarded. The default value is `0.0.0.0`.
Secondary DHCP Server	Enter the IP address of an alternative BootP or DHCP server. The default value is `0.0.0.0`.

11.8.5 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 **Hinzufügen** 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**

11.8.5.1 DHCPv6 Server

Here you can create interface-related address pools and define DHCP options inside of an DHCP Option Set.

11.8.5.1.1 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

Field	Description
	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.

11.8.5.2 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, Server Fallback 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 domain name (e.g. dev.bintec.de.) mast end with a dot (.).

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

Fields in the Advanced Parameter menu

Field	Description
Server preference	The DHCPv6 advertisements sent by the DHCPv6 server to the clients may contain the DHCPv6 option 7 "Preference". Possible values are `0...255`. In a network with multiple DHCPv6 servers this option controls which server takes the highest priority. If a client receives DHCPv6 advertisements with different priorities from different servers, it will usually accept the parameters from the highest priority server. The client can, however, also accept DHCPv6 advertisements with a lower priority if the set of parameters in the advertisement provides more of the options requested by the client. A value of `0` means "not specified" (lowest priority), `255` denotes the highest priority.

Fields in the menu Advanced Server Fallback Options

Field	Description
DNS Server	Here you can configure the DNS servers that are propagated by DHCPv6. (DHCPv6 Option 23 "DNS Recursive Name Server"). Per default, the global DNS server of the system are propagated. (Global DNS servers are configured by the field **DNS Propagation** in the menu **LAN**->**IP Configuration**->**Interfaces**-> ✎ ->**Advanced Settings** if **IPv6** = *Enabled* .) You can also manually specify DNS servers and have them propagated to the clients. To do this disable the option **Use RA or Global Fallback DNS Server** and create the desired DNS server entries using **Add**.
SNTP Server	Here you can configure the time servers to be propagated by DHCPv6 (DHCPv6 Option 31 "Simple Network Time Protocol Server"). Use **Add** to create the desired time server entries.

11.8.5.3 Stateful Clients

Here you see an entry for each Stateful Client that has contacted the server and has been assigned an IPv6 address.

11.8.5.4 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.

11.8.5.4.1 Edit or New

Use **New** to create entries for Stateful Clients. Normally, you do not have to create any entries.Use ✎ in order to edit existing entries. You should check each automatically created entry once to verify the settings and adjust them if required.

The menu consists of the following fields.

Fields in the menu Basic Parameters

Field	Description
DUID	Clients use the **DUID field** (DHCP Unique Identifier) in order to identify themselves and request an IP address from the DHCPv6 server. If you create an entry using **New** you can specify the **DUID** as a 16 - 20 digit HEX number. You can enter them using a "-" (minus) as separator (Windows style), or you can enter them in a single block (Linux style).
Accept Client FQDN	If **Accept Client FQDN** is enabled, the client is entered into the cache of the Domain Name Server with the parameter FQDN (Fully Qualified Domain Name).
Administrative FQDNs	With **Add**, you can specify an FQDN (Fully Qualified Domain Name) - even for automatically created entries.
Static Interface Identifier	The field **Static Interface Identifier** is the host portion of the IPv6 address, i.e., the last 64 Bit of the IP address. This prefix must start with ::.

11.8.6 Surveillance

In this menu, you can configure an automatic availability check for hosts or interfaces and automatic ping tests.

☞ **Note**

This function cannot be configured on your device for connections that are authenticated via a RADIUS server.

11.8.6.1 Hosts

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Hosts** menu.

11.8.6.1.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to create additional monitoring tasks.

The menu **Local Services**->**Surveillance**->**Hosts**->**New** consists of the following fields:

Fields in the Host Parameters menu

Field	Description
Group ID	If the availability of a group of hosts or the default gateway is to be monitored by your device, select an ID for the group or the default gateway. The group IDs are automatically created from *0* to *255*. If an entry has not yet been created, a new group is created using the *New ID* option. If entries have been created, you can select one from the list of created groups. Each host to be monitored must be assigned to a group. The operation configured for the select **Interface** is only executed if no group member can be reached.

Fields in the Trigger menu

Field	Description
Monitored IP Address	Enter the IP address of the host to be monitored. Possible values: • *Default Gateway* (default value): The default gateway is monitored. • *Specific*: Enter the IP address of the host to be monitored manually in the adjacent input field.
Source IP Address	Select how the IP address is to be determined that your device uses as the source address of the packet sent to the host to be monitored. Possible values: • *Automatic* (default value): The IP address is determined automatically. • *Specific*: Enter the IP address in the adjacent input field.
Interval	Enter the time interval (in seconds) to be used for checking the availability of hosts. Possible values are *1* to *65536*. 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

Field	Description
	as accessible. You can use this setting to specify, for example, when a host is deemed to be accessible once more, and used again, instead of a backup device. Possible values are *1* to *65536*. The default value is *3*.
Unsuccessful Trials	Specify how many pings need to be unanswered for the host to be regarded as inaccessible. You can use this setting to specify, for example, when a host is deemed to be inaccessible, and that a backup device should be used. Possible values are *1* to *65536*. The default value is *3*.
Action to be performed	Not for **Action** = *Monitor*. Select which **Action** should be execude, when the Host is regarded as inaccessible. For most actions, you select an **Interface** to which the **Action** relates. All IP interfaces can be selected. For each interface, select whether it is to be enabled (*Enable*), disabled (*Disable* default value), reset (*Reset*), or the connection established (*Redial*). The **Actions** *Enable* and *Disable* also canceled when 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.

11.8.6.2 Interfaces

A list of all monitored hosts is displayed in the **Local Services**->**Surveillance**->**Interfaces** menu.

11.8.6.2.1 Edit or New

Choose the ✎ icon to edit existing entries. Choose the **New** button to set up monitoring of 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

Field	Description
	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 switch all physical and virtual interfaces as well as options `All PPP Interfaces` and `All IPSec Interfaces`.

11.8.6.3 Ping Generator

In the **Local Services**->**Surveillance**->**Ping Generator** menu, a list of all configured, automatically generated pings is displayed.

11.8.6.3.1 Edit or New

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

The menu **Local Services**->**Surveillance**->**Ping Generator**->**New** consists of the following fields:

Fields in the Basic Parameters menu

Field	Description
Destination IP Address	Enter the IP address to which the ping is automatically sent.
Source IP Address	Enter the source IP address of the outgoing ICMP echo request packets. Possible values: • `Automatic`: The IP address is determined automatically. • `Specific` (default value): Enter the IP address in the adjacent input field e.g. to test a particular extended route.
Interval	Enter the interval in seconds during which the ping is sent to the address specified in **Remote IP Address**. Possible values are `1` to `65536`. The default value is `10`.
Trials	Enter the number of ping tests to be performed. The default value is `3`.

11.8.7 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* .

11.8.7.1 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 enabled by default.

11.8.7.2 General

In this menu, you make the basic UPnP settings.

The **Local Services**->**UPnP**->**General** menu consists of the following fields:

Fields in the Basic Parameters 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 re-

Field	Description
	quests. The possible values are *1* to *65535*, the default value is *5678*.

11.8.8 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**.

11.8.8.1 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.

11.8.8.1.1 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* • *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*.

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. 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:

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*.

11.8.8.2 WOL Rules

The menu **Local Services**->**Wake-On-LAN**->**WOL Rules** displays a list of all the WOL rules that have been configured.

11.8.8.2.1 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.

Field	Description
	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. • *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.

11.8.8.3 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.

11.8.8.3.1 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.

Field	Description
Rule Chain	Select a rule chain.

11.9 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.

11.9.1 IPSec

11.9.1.1 IPSec Tunnels

A list of all configured IPSec tunnels 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 Address	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 pressing the ⌃ button or ⌄ button in the **Action** column.

By pressing 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** / **Lifetime remaining** / **Status**	The parameters of the IKE (Phase 1) SAs are displayed here.
IPSec (Phase-2) SAs (x) **Role** / **Algorithm** / **Lifetime remaining** / **Status**	Shows the parameters of the IPSec (Phase 2) SAs.
Messages	The system messages for this IPSec tunnel are displayed here.

11.9.1.2 IPSec Statistics

In the **Monitoring**->**IPSec**->**IPSec Statistics** menu, statistical values for all IPSec connections are displayed.

The menu consists of the following fields:

Field 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**).

Field in the Peers menu

Field	Description
Status	Displays the number of IPSec tunnels by their current status. • **Up**: Currently active IPSec tunnels. • **Going up**: IPSec tunnels currently in the tunnel setup phase. • **Blocked**: IPSec tunnels that are blocked. • **Dormant**: Currently inactive IPSec tunnels. • **Configured**: Configured IPSec tunnels.

Fields in the SAs menu

Field	Description
IKE (Phase-1)	Shows the number of active phase 1 SAs (**Established**) from the total number of phase 1 SAs **Total**).
IPSec (Phase-2)	Shows the number of active phase 2 SAs (**Established**) from the total number of phase 2 SAs **Total**).

Fields in the Packet Statistics menu

Field	Description
Total	Shows the number of all processed incoming (**In**) or outgoing (**Out**) packets.

Field	Description
Passed	Shows the number of incoming (**In** or outgoing (**Out**) packets forwarded in plain text.
Dropped	Shows the number of all rejected incoming (**In**) or outgoing (**Out**) packets.
Encrypted	Shows the number of all incoming (**In**) or outgoing (**Out**) packets protected by IPSec.
Errors	Shows the number of incoming (**In**) or outgoing (**Out**) packets for which processing led to errors.

11.9.2 ISDN/Modem (Media Gateway)

11.9.2.1 Current Calls

In the **Monitoring**->**ISDN/Modem**->**Current Calls** menu, a list of the existing ISDN connections (incoming and outgoing) is displayed.

Values in the Current Calls list

Field	Description
Service	Displays the service to or from which the call is connected: *PPP*, *IPSec*, *X.25*, *POTS*.
Remote Number	Displays the number that was dialled (in the case of outgoing calls) or from which the call was made (in the case of incoming calls).
Interface	Displays additional information for PPP connections.
Direction	Displays the send direction: *Incoming*, *Outgoing*.
Charge	Displays the costs of the current connection.
Duration	Displays the duration of the current connection.
Stack	Displays the related ISDN port (STACK).
Channel	Displays the number of the ISDN B channel.
Status	Displays the state of the connection: *null*, *c-initiated*, *ovl-send*, *oc-procd*, *c-deliverd*, *c-present*, *c-recvd*, *ic-procd*, *up*, *discon-req*, *discon-ind*, *suspd-req*, *resum-req*, *ovl-recv*.

11.9.2.2 Call History

In the **Monitoring**->**ISDN/Modem**->**Call History** menu, a list of the last 20 ISDN calls (incoming and outgoing) completed since the last system start is displayed.

Values in the Call History list

Field	Description
Service	Displays the service to or from which the call was connected: *PPP*, *IPSec*, *X.25*, *POTS*.
Remote Number	Displays the number that was dialled (in the case of outgoing calls) or from which the call was made (in the case of incoming calls).
Interface	Displays additional information for PPP connections.
Direction	Displays the send direction: *Incoming*, *Outgoing*.
Charge	Displays the costs of the connection.
Start Time	Displays the time at which the call was made or received.
Duration	Displays the duration of the connection.

11.9.3 Interfaces

11.9.3.1 Statistics

In the **Monitoring**->**Interfaces**->**Statistics** menu, current values and activities of all device interfaces are displayed.

Change the status of the interface by pressing the ⌃ button or ⌄ button in the **Action** column.

Values in the Statistics list

Field	Description
No.	Shows the serial number of the interface.
Description	Displays the name of the interface.
Type	Displays the interface text.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Tx Errors	Shows the total number of errors sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.
Rx Errors	Shows the total number of errors received.
Status	Shows the operating status of the selected interface.
Unchanged for	Shows the length of time for which the operating status of the interface has not changed.
Action	Enables you to change the status of the interface as displayed.

Press the 🔍 button to display the statistical data for the individual interfaces in detail.

Values in the Statistics list

Field	Description
Description	Displays the name of the interface.
MAC Address	Displays the MAC address.
IP Address / Netmask	Shows the IP address and the netmask.
NAT	Indicates if NAT is activated for this interface.
Tx Packets	Shows the total number of packets sent.
Tx Bytes	Displays the total number of octets sent.
Rx Packets	Shows the total number of packets received.
Rx Bytes	Displays the total number of bytes received.

Fields in the TCP Connections menu

Field	Description
Status	Displays the status of an active TCP connection.
Local Address	Displays the local IP address of the interface for an active TCP connection.
Local Port	Displays the local port of the IP address for an active TCP connection.
Remote Address	Displays the IP address to which an active TCP connection exists.
Remote Port	Displays the port to which an active TCP connection exists.

11.9.3.2 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.

11.9.4 Bridges

11.9.4.1 br<x>

In the **Monitoring**->**Bridges**-> **br<x>** menu, current values pertaining to the configured bridges are displayed.

Values in the br<x> list

Field	Description
MAC Address	Displays the MAC addresses of the associated bridges.
Port	Displays the port, the bridge is active at.

11.9.5 QoS

In the **Monitoring**->**QoS** menu, statistics are displayed for interfaces on which QoS has been configured.

11.9.5.1 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 12 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 **System Phone** assigned to you, and modify these to your needs.

12.1 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.

12.1.1 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.

12.1.1.1 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 *`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.

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 tele-

Field	Description
	phone. 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.

12.1.1.2 Log on / Log off

With system telephones, it is 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 Log on / Log off menu

Field	Description
Description	Indicates the teams the user belongs to.
Status	Select whether the team member shall be logged in or out of the team. The function is activates by selecting *Logged on*. The function is enabled by default.

12.2 Status

The **User Access**->**Status** menu displays the most important settings performed for you by the system administrator.

The 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.
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

Field	Description
	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. 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.
Pick-up Group	Displays the number of the group in which calls may be picked up.

12.3 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**.

12.3.1 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.
Call Through	Indicates whether the telephone number for the **Call Through** function is activated.

12.3.2 User Phonebook

In the **User Phonebook**, your user entries are displayed. You can add, edit or delete entries.

12.3.2.1 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).

12.4 Call Data Records

The **Call Data Records** menu displays your user's incoming and outgoing connections recorded to date.

12.4.1 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.
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.

Field	Description
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.

12.4.2 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.

12.5 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**.

12.5.1 Incoming

The **Applications**->**Call List**->**Incoming** menu contains information that permits the monitoring of incoming activities.

The 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.

Field	Description
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.

12.5.2 Outgoing

The **Applications**->**Call List**->**Outgoing** menu contains information that permits the monitoring of outgoing activities.

The 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.

12.6 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.

12.6.1 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 phone's configuration interface.

Select the ✎ symbol to select the display language and the key settings of the phone.

12.6.1.1 Settings

The **Settings** menu allows you to select the desired display language from a drop-down menu.

12.6.1.2 Keys

The menu **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 functions 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 **Media-Pool** 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 selected 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. The keys can be used for the following features:
  - User defined: freely configurable
  - Night mode: switch between day and night modes
  - CFU; CFNR; CFB; CFB/CFNR: Call Forwarding (immediately, delayed, on Busy)
  - Team Signalization: log in to our of a team

> **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 Keys

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*

Field	Description
	• *Macro Function* • *XML-Content* • *Next call anonymous* • *Menu - Call Forwarding* • *Menu - Resource Directory* • *Menu - Internet Radio* • *Macro Function* • *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.
Macro Function	Only for **Key Type** = *Macro Function* The keys can be used for the following features: • *User defined*: Freely configurable • *Night mode*: Switch between day and night modes • *CFU; CFNR; CFB; CFB/CFNR*: Call Forwarding (immediately, delayed, on Busy) • *Team Signalization*: You can log in to a team or log out of a team.
On Code	Only for**Macro Function** = *User defined* Define an arbitrary code to be executed when the key is switched on.
Off Code	Only for**Macro Function** = *User defined* Define an arbitrary code to be executed when the key is switched off.
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 ↑↓ icon to move configured function keys.

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.

Index